New York J. Math. 30 (2024) 828-843.

Polynomials with integral Mahler measures

Artūras Dubickas

ABSTRACT. For each $m \in \mathbb{N}$ and each sufficiently large $d \in \mathbb{N}$, we give an upper bound for the number of integer polynomials of degree d and Mahler's measure m. We show that there are at most $\exp\left(11(md)^{2/3}\left(\log(md)\right)^{4/3}\right)$ of such polynomials. For 'small' m, i.e. $m < d^{1/2-\varepsilon}$, this estimate is better than the estimate $m^{d(1+\varepsilon)}$ that comes from a corresponding upper bound on the number of integer polynomials of degree d and Mahler's measure at most m. By the results of Zaitseva and Protasov, our estimate has applications in the theory of self-affine 2-attractors. We also show that for each integer $m \geq 3$ there is a constant c = c(m) > 0 such that the number of monic integer irreducible expanding polynomials of sufficiently degree d and constant coefficient m (and hence with Mahler's measure equal to m) is at least cd^{m-1} .

CONTENTS

1.	Introduction	828
2.	Auxiliary results	831
3.	Proof of Theorem 1.4 and Proposition 1.5	835
4.	Proof of Theorem 1.1	837
References		842

1. Introduction

For a degree *d* polynomial

we define its Mahler measure by

$$M(f) = |a_d| \prod_{i=1}^d \max\{1, |\alpha_j|\}.$$

The Mahler measure is multiplicative, namely,

$$M(fg) = M(f)M(g) \tag{1}$$

Received April 2, 2024.

²⁰¹⁰ Mathematics Subject Classification. 11R06, 11R09, 11C08, 12D10.

Key words and phrases. Mahler's measure, integer expanding polynomial, self-affine 2 attractor.

for any $f, g \in \mathbb{C}[x]$, and satisfies

$$M(f) = M(f^*), \tag{2}$$

where $f^*(x) = x^d f(1/x)$ for $f \in \mathbb{C}[x]$ of degree d. Throughout, we say that the polynomial f^* defined as above is *reciprocal* to the polynomial f of degree d. The Mahler measure of an algebraic number $\alpha \in \overline{\mathbb{Q}}$ with minimal polynomial $f \in \mathbb{Z}[x]$ is defined by $M(\alpha) = M(f)$.

In [7], Chern and Vaaler gave an asymptotic formula for the number of integer polynomials of degree at most d and Mahler's measure at most T as $T \to \infty$. It turns out to be asymptotic to $\kappa_d T^{d+1}$ with some $\kappa_d > 0$ as $T \to \infty$. The situation is much more complicated when T is bounded and d is large. The case T=2 has been first considered by Mignotte [19]. Later, Mignotte's bound was improved by the author and Konyagin. In [13], it was shown that for any real T>1 the number of integer polynomials of degree at most d and Mahler's measure at most T is bounded above by

$$\min\{T^{(1+\varepsilon)d}, T^{d+1} \exp(d^2/2)\}\tag{3}$$

for any $\varepsilon > 0$ and any sufficiently large d. (Throughout the paper, $\exp(x)$ stands for e^x .) For T=2, this gives the upper bound $2^{(1+\varepsilon)d}$. On the other hand, the best available lower bound for the number of monic integer irreducible polynomials of degree at most d and of Mahler's measure less than 2 is only κd^5 with some absolute constant $\kappa > 0$, see [11], [12].

As in [1], we say that a polynomial in $\mathbb{Z}[x]$ (or even in $\mathbb{C}[x]$) whose roots are all in |z| > 1 is *expanding*. Expanding polynomials also appear, for instance, in the papers of Akiyama and Zaimi [3], Brunotte [6]. Note that if $f \in \mathbb{C}[x]$ is expanding then

$$M(f) = |f(0)|. \tag{4}$$

In [23], Zaitseva and Protasov considered various questions related to socalled self-affine 2-attractors and reduced one of the problems to estimating the number of monic integer expanding polynomials of degree d with constant term ± 2 . They showed that for d sufficiently large there are at least $0.06d^2$ and at most $\exp(0.7d)$ of such polynomials, the upper bound being taken from (3) with T=2. Of course, such polynomials have Mahler's measure not at most 2, but exactly 2. This raises a natural question of finding a better upper bound for the number of degree d integer polynomials with Mahler's measure 2 and, more generally, with Mahler's measure m, where $m \ge 2$ is an integer.

In the case when d is fixed and $m \to \infty$ this problem has already been addressed in [2], [8], [17]. In [2, Theorem 5.2], Akiyama and Pethő proved a result which implies that the number of monic integer irreducible expanding polynomials of degree d with constant term m is asymptotic to $v_d m^{d-1}$ with some $v_d > 0$ as $m \to \infty$. By (4), such polynomials have Mahler's measure equal to m. Similar asymptotical results when the degree d is fixed and Mahler's measure tends to infinity were recently obtained by Dill [8, Section 8].

However, as in the case of the problem of estimating the number of integer polynomials with bounded Mahler's measure which we discussed above, this problem, where Mahler's measure $m \in \mathbb{N}$ of polynomials is fixed and their degree d is large, turns out to be more difficult. In this paper, we will evaluate the number of integer polynomials of degree d and Mahler's measure equal to a positive integer m. Our main result is the following upper bound which improves the bound (3) in case we count only polynomials with Mahler's measure exactly m:

Theorem 1.1. For each positive integer m and each sufficiently large integer d there are at most

$$\exp\left(11(md)^{2/3}\left(\log(md)\right)^{4/3}\right) \tag{5}$$

integer polynomials of degree d and Mahler's measure m.

We remark that m=1 is the only case when a better result is known. By Kronecker's theorem (see, e.g., [20, Theorem 4.5.4]), integer polynomials with Mahler's measure 1 are products of $\pm x^k$, $k \in \mathbb{N} \cup \{0\}$, and cyclotomic polynomials. The next proposition is the main result of Boyd and Montgomery [5]:

Proposition 1.2. The number of degree d monic integer polynomials with all roots on |z|=1 is asymptototic to $\frac{c_1}{d\sqrt{\log d}}\exp(c_2\sqrt{d})$ as $d\to\infty$, with $c_1=\sqrt{105\zeta(3)}/(4\pi^2e^{\gamma/2})$, where γ is Euler's constant, and $c_2=\sqrt{105\zeta(3)}/\pi$.

Proposition 1.2 immediately implies the upper bound of the form $\exp(c_3\sqrt{d})$, where $c_3 > c_2$, on the number of integer polynomials of sufficiently large degree d and Mahler's measure m=1. This is better than (5) gives for m=1. Of course, the example (x-m)f(x), where f runs through all monic degree d-1 polynomials in $\mathbb{Z}[x]$ with all roots on |z|=1, shows that the exponent 2/3 for d in (5) cannot be improved to a constant smaller than 1/2.

On the other hand, for $m \ge 2$ fixed, and, more generally, for m in the range $2 \le m < d^{1/2-\varepsilon}$, Theorem 1.1 gives a better bound than that $m^{(1+\varepsilon)d}$ coming from (3). In particular, for m=2, Theorem 1.1 improves the upper bound in [23, Theorem 10]. Since $10.5 \cdot 2^{2/3} < 17$, Theorem 1.1, which we will prove with the better constant 10.5 (instead of 11) in (5) (see (32)), combined with [23, Corollary 6] yields the following:

Corollary 1.3. The total number of not affinely similar 2-attractors in dimension d is less than $\exp(17d^{2/3}(\log d)^{4/3})$ for d sufficiently large.

We remark that in [23, Theorem 10], the bound corresponding to that of Corollary 1.3 was $\exp(0.7d)$.

It seems very likely that the main contribution in Theorem 1.1 comes from reducible polynomials, while the number of irreducible polynomials of degree d and Mahler's measure m should be much smaller. In the next theorem we will construct many monic integer irreducible polynomials with Mahler's measure $m \in \mathbb{N} \setminus \{1\}$.

Theorem 1.4. The number of monic integer irreducible expanding polynomials of degree d with constant coefficient 2 is at least c_0d^2 , where $c_0 > 0$ is an absolute constant. Furthermore, for each $m \ge 3$ there is a constant c(m) > 0 such that for each sufficiently large $d \in \mathbb{N}$ the number of monic integer irreducible expanding polynomials of degree d with constant coefficient m is at least $c(m)d^{m-1}$.

Note that the gap between the bounds in Theorems 1.1 and 1.4 is large. Since we consider the situation with m small and d large, the bound in Theorem 1.4 is far from that given in the asymptotic formula $v_d m^{d-1}$ as $d \to \infty$ [2] and closer to that in [12]. For $m \ge 3$, the proof of Theorem 1.4 is based on an explicit construction. For m = 2, the construction is different and taken from [23]. However, for the sake of completeness, we will give a full proof of Theorem 1.4 in the case m = 2 too.

Earlier, somewhat unrelated results on the properties of the Mahler measure have been obtained by the author in [10]. Some of those results were recently extended by Fili, Pottmeyer and Zhang in [14], [15], but now, in the present context, a very useful result seems to be also [10, Theorem 2]. Here, in the same fashion, we will derive a result that completely characterizes all integer polynomials with integral Mahler measure. This will be a useful tool in completing the proof of Theorem 1.1:

Proposition 1.5. Let m and d be two positive integers and let $f \in \mathbb{Z}[x]$ be a polynomial of degree d with Mahler measure equal to m. Write

$$f(x) = ax^{s} \prod_{j=1}^{k} f_{j}(x), \tag{6}$$

where $a \in \mathbb{Z} \setminus \{0\}$, $s \in \{0, 1, ..., d\}$ and $f_1, ..., f_k \in \mathbb{Z}[x]$ are not necessarily distinct irreducible polynomials with positive leading coefficients satisfying $f_j(0) \neq 0$. Then, for each j = 1, ..., k, the polynomial f_j either has all of its roots on |z| = 1 or one of the polynomials f_j, f_j^* is expanding.

By (1), (2), (4) and Proposition 1.5, it follows that with its notation we have

$$m = M(f) = |a| \prod_{j=1}^{k} M(f_j) = |a| \prod_{j=1}^{k} m_j,$$
 (7)

where $m_j = M(f_j) = M(f_j^*) \in \mathbb{N}$. Here, $m_j = 1$ if and only if f_j is cyclotomic. In the next section we present some auxiliary results. Then, in Section 3 we will prove Theorem 1.4 and Proposition 1.5. Finally, in Section 4 we will prove Theorem 1.1.

2. Auxiliary results

For
$$\mathbf{x}=(x_1,\dots,x_d)\in\mathbb{C}^d$$
 we put
$$||\mathbf{x}||=\max_{1\leq j\leq d}|x_j|$$

for the l_{∞} norm of the vector \mathbf{x} . For a convex closed bounded set $A \subset \mathbb{R}^d$ we put

$$F(A) = \{\mathbf{x} + \mathbf{y} : \mathbf{x} \in A, \rangle ||\mathbf{y}|| \le 1/2\}$$
(8)

for the 1/2-neighbourhood of the set A. Suppose that $G \subseteq \{1, 2, ..., d\}$ and g = |G|. We denote by $\Pr_G(A)$ the orthogonal projection of the set A to the linear space \mathbb{R}^g spanned by the vectors of \mathbb{R}^d corresponding to the indices of G. Finally, denote by $\operatorname{Vol}(\Pr_G(A))$ the volume of the g-dimensional $(1 \le g \le d)$ convex set $\Pr_G(A)$. With this notation we have the following lemma for $d \ge 1$:

Lemma 2.1. We have

$$\operatorname{Vol}(F(A)) = 1 + \sum_{G} \operatorname{Vol}(\operatorname{Pr}_{G}(A)),$$

where the sum is taken over all nonempty subsets G of $\{1, 2, ..., d\}$.

See [13, Lemma 0] for the proof.

Lemma 2.2. Let V(g,n) be the maximal volume of a convex hull of n points in the parallelepiped $\prod_{j=1}^g [-u_j/2, u_j/2] \subset \mathbb{R}^g$, where u_1, \dots, u_g are positive. Then, for $n = g^{\lambda}$, where $\lambda > 1$ and g is sufficiently large, we have

$$V(g, g^{\lambda}) < \left(\frac{23.22(\lambda - 1)\log g}{g}\right)^{g/2} \prod_{j=1}^{g} u_j.$$

Proof. Let W(g,n) be the maximal volume of a convex hull of n points in the unit ball W_g in \mathbb{R}^g . The volume of W_g equals $w_g = \frac{\pi^{g/2}}{\Gamma(g/2+1)}$; see, e.g., [22]. Next, as in [9], [13], we will need a result on the estimate of the volume of a polytope with few vertices in the style of [4], [16], [18]. Specifically, in [4, eq. (4)], it was shown that for $n = g^{\lambda}$, where $\lambda > 1$, and any $\varepsilon > 0$ the inequality

$$W(g, g^{\lambda}) < (1 + \varepsilon)^g w_g \left(\frac{2e(\lambda - 1)\log g}{g}\right)^{g/2} \tag{9}$$

holds for each sufficiently large g.

As observed in [13], by rescaling, it suffices to prove the inequality of the lemma for the parallepiped

$$P_g = \prod_{j=1}^g [-u_j/2, u_j/2] = [-1/\sqrt{g}, 1/\sqrt{g}]^g.$$

Note that P_g is inscribed into the unit ball W_g with center at the origin, hence $V(g, g^{\lambda}) \leq W(g, g^{\lambda})$. Furthermore, by Stirling's formula, $\Gamma(g/2+1) > (g/2e)^{g/2}$ for g sufficiently large, so using $u_i = 2/\sqrt{g}$ we obtain

$$w_g = \frac{\pi^{g/2}}{\Gamma(g/2+1)} < \left(\frac{2\pi e}{g}\right)^{g/2} = \left(\frac{\pi e}{2}\right)^{g/2} \prod_{j=1}^g u_j.$$

This implies the required result by (9) and $(1+\varepsilon)^2\pi e^2 < 23.22$ with appropriate choice of ε .

Lemma 2.3. For every $k \in \mathbb{N}$ and any real numbers $m_1, ..., m_k \ge \sqrt{2}$ and $d_1, ..., d_k > 0$ we have

$$(m_1d_1)^{2/3} + \dots + (m_kd_k)^{2/3} \le (m_1 \dots m_k(d_1 + \dots + d_k))^{2/3}.$$
 (10)

Proof. The inequality (10) is equality for k = 1. It is sufficient to prove (10) for k = 2 and then apply induction on k. Dividing both sides of (10) with k = 2 by $d_1^{2/3}$ and setting $y = d_2/d_1$ we see that it suffices to show that $m_1^{2/3} + (m_2 y)^{2/3}$ does not exceed $(m_1 m_2 (y + 1))^{2/3}$ for y > 0.

Let us consider the function

$$\varphi(y) = (m_1 m_2 (y+1))^{2/3} - m_1^{2/3} - (m_2 y)^{2/3}.$$

It is positive at y = 0, since $m_2 > 1$. Its derivative

$$\varphi'(y) = \frac{2m_2^{2/3}}{3(y+1)^{1/3}} \left(m_1^{2/3} - \left(1 + \frac{1}{y} \right)^{1/3} \right)$$

vanishes at $y_0 = 1/(m_1^2 - 1)$. Since $\varphi'(y) < 0$ for $0 < y < y_0$ and $\varphi'(y) > 0$ for $y > y_0$, the minimum of the function $\varphi(y)$ in $[0, \infty)$ is attained at $y = y_0$. Thus, in order to prove that $\varphi(y) \ge 0$ for all y > 0 it remains to verify the inequality $\varphi(y_0) \ge 0$.

From

$$\varphi(y_0) = \varphi\left(\frac{1}{m_1^2 - 1}\right) = (m_1 m_2)^{2/3} \left(\frac{m_1^2}{m_1^2 - 1}\right)^{2/3} - m_1^{2/3} - \frac{m_2^{2/3}}{(m_1^2 - 1)^{2/3}}$$
$$= m_2^{2/3} (m_1^2 - 1)^{1/3} - m_1^{2/3}$$

we see that $\varphi(y_0) \ge 0$ is equivalent to $(m_1^2-1)^{1/3} \ge (m_1/m_2)^{2/3}$. The latter inequality is equivalent to $(m_1^2-1)m_2^2 \ge m_1^2$, and can be also written as $(m_1^2-1)(m_2^2-1) \ge 1$, which holds due to $m_1^2-1 \ge 1$ and $m_2^2-1 \ge 1$.

Lemma 2.4. For every integer $m \ge 3$ there is a constant c(m) > 0 such that for each sufficiently large integer d there are at least $c(m)d^{m-1}$ irreducible polynomials of the form

$$x^d - x^{b_{m-1}} - \cdots - x^{b_1} + m$$
,

where $b_1, ..., b_{m-1} \in \mathbb{Z}$ and $0 < b_1 < \cdots < b_{m-1} < d$.

Proof. Fix $m \ge 3$. For each d > m let S(d, m) be the set polynomials of the form $x^d - x^{b_{m-1}} - \cdots - x^{b_1} + m$ with integers b_1, \dots, b_{m-1} satisfying

$$0 < b_1 < \dots < b_{m-1} < d \tag{11}$$

and

$$\gcd(b_1, \dots, b_{m-1}) = 1. \tag{12}$$

Note that the number of vectors $(b_1, \dots, b_{m-1}) \in \mathbb{Z}^{m-1}$ satisfying (11) is $\binom{d-1}{m-1}$. It is well known that the probability of $m-1 \ge 2$ random integers being coprime

is $1/\zeta(m-1)$. Thus, there is a constant $c_1(m) > 0$ such that for each sufficiently large d we have

$$|S(d,m)| \ge c_1(m)d^{m-1}.$$
 (13)

We claim that every reciprocal monic divisor $g \in \mathbb{Z}[x]$ of $f \in S(d, m)$ must be cyclotomic. Indeed, if not, then, by Kronecker's theorem (see, e.g. [20, Theorem 4.5.4]), at least one root of g must be in |z| > 1. Since g is reciprocal, it must have a root α satisfying $|\alpha| < 1$. But then $f(\alpha) = 0$ implies

$$m = \alpha^{b_1} + \dots + \alpha^{b_{m-1}} - \alpha^d \le |\alpha^d| + \sum_{j=1}^{m-1} |\alpha^{b_j}| < m,$$

which is impossible.

By Schinzel's result [21, Theorem 4], either the nonreciprocal part of $f \in S(d,m)$ (which is equal to the noncyclotomic part by the above) is irreducible or there is a positive constant $c_2(m)$ (which given explicitly in [21] and for the polynomial of the form $x^d - x^{b_{m-1}} - \cdots - x^{b_1} + m$ depends only on m) and a vector $(\gamma_1, \dots, \gamma_m) \in \mathbb{Z}^m$ such that

$$0 < \max_{1 \le j \le m} |\gamma_j| \le c_2(m)$$

and

$$\gamma_1 b_1 + \dots + \gamma_{m-1} b_{m-1} + \gamma_m d = 0. \tag{14}$$

It is clear that at least one γ_j , $j=1,\ldots,m-1$, must be nonzero.

For each nonzero vector $(\gamma_1, ..., \gamma_m) \in \mathbb{Z}^m$ the number of vectors

$$(b_1,\dots,b_{m-1})\in\mathbb{Z}^{m-1}$$

satisfying both (11) and (14) is less than d^{m-2} . Furthermore, there are at most $(2c_2(m)+1))^m$ possible vectors $(\gamma_1, ..., \gamma_m) \in \mathbb{Z}^m$. Hence, by (13), at least

$$c_1(m)d^{m-1} - (2c_2(m) + 1)^m d^{m-2}$$
(15)

polynomials from S(d, m) have irreducible noncyclotomic part.

Now, we will show that no polynomial in S(d, m) has a cyclotomic factor. Indeed, $f \in S(d, m)$ has a cyclotomic divisor if and only if there is a root of unity ζ such that $\zeta^d = -1$ and

$$\zeta^{b_{m-1}} = \dots = \zeta^{b_1} = 1. \tag{16}$$

Then, in view of (12) there are $u_{m-1}, ..., u_1 \in \mathbb{Z}$ such that

$$b_{m-1}u_{m-1} + \dots + b_1u_1 = 1.$$

Thus, if (16) is true, we obtain

$$\zeta = \zeta^{b_{m-1}u_{m-1}+\cdots+b_1u_1} = 1,$$

which contradicts to $\zeta^d = -1$. Hence, for every $f \in S(d, m)$, the polynomial f itself coincides with its noncyclotomic part, which is shown to be irreducible with at most $(2c_2(m) + 1)^m d^{m-2}$ exceptions. Thus, by (15), we arrive at the required result with the constant, say, $c(m) = c_1(m)/2$.

3. Proof of Theorem 1.4 and Proposition 1.5

Proof of Theorem 1.4. To prove the theorem for $m \ge 3$ it suffices to show that each polynomial as in Lemma 2.4 is expanding. Indeed, it is clear that it has no roots in |z| < 1. If it has a root of unit modulus then it must be reciprocal, which is not the case. This means that all the roots of such polynomial must be in |z| > 1, and hence it is expanding.

In all that follows we will prove the theorem for m = 2. Let us consider the polynomials of the form

$$f_{a,b,c}(x) = (1 + x^a)(1 + x^b)(1 + x^c) + 1,$$

where $a \ge b \ge c$ are three positive integers satisfying a + b + c = d and, for example,

$$b \not\equiv c \pmod{3}. \tag{17}$$

There is an absolute constant $c_4 > 0$ such that, for d large enough, say $d \ge d_0$, there are at least c_4d^2 of such polynomials. (For $d \le d_0$ there is at least one expanding polynomial $x^d + 2$, so the lower bound c_5d^2 with some other constant $c_5 > 0$ also holds for all $d \in \mathbb{N}$.)

It remains to show that $f_{a,b,c}$ has no root in $|z| \leq 1$. Indeed, then all roots of $f_{a,b,c}$ are in |z| > 1 and the modulus of their product is 2, so $f_{a,b,c}$ is monic integer irreducible expanding polynomial.

Suppose $\alpha \in \mathbb{C}$ satisfying $|\alpha| \leq 1$ is a root of $f_{a,b,c}$. The numbers

$$z_a=1+\alpha^a=|z_a|e^{i\varphi_a},\quad z_b=1+\alpha^b=|z_b|e^{i\varphi_b},\quad z_c=1+\alpha^c=|z_c|e^{i\varphi_c}$$

all lie in the circle $|z-1| \le 1$ and satisfy $z_a z_b z_c = -1$. Therefore, $|z_a z_b z_c| = 1$ and

$$\varphi_a + \varphi_b + \varphi_c = \pm \pi, \quad \varphi_a, \varphi_b, \varphi_c \in (-\pi/2, \pi/2).$$
 (18)

Moreover, we must have $|z_a| \le 2|\cos(\varphi_a)|$ with equality if $|\alpha| = 1$. Likewise, $|z_b| \le 2|\cos(\varphi_b)|$ and $|z_c| \le 2|\cos(\varphi_c)|$. Hence,

$$|\cos(\varphi_a)\cos(\varphi_b)\cos(\varphi_c)| \ge \frac{1}{8}.$$
 (19)

Note that (18) implies that all three numbers $\varphi_a, \varphi_b, \varphi_c$ must be positive or all three negative. Replacing $(\varphi_a, \varphi_b, \varphi_c)$ by $(-\varphi_a, -\varphi_b, -\varphi_c)$ if necessary we may assume that all three numbers are positive. Then, $\varphi_a, \varphi_b, \varphi_c$ are angles of an acute triangle. It is an elementary exercise to show that the sum of their cosine angles $\cos(\varphi_a) + \cos(\varphi_b) + \cos(\varphi_c)$ attains its maximum 3/2 only if all three angles are $\pi/3$. Thus, by (19), we obtain

$$\frac{1}{2} \le \left(\cos(\varphi_a)\cos(\varphi_b)\cos(\varphi_c)\right)^{1/3} \le \frac{\cos(\varphi_a) + \cos(\varphi_b) + \cos(\varphi_c)}{3} \le \frac{1}{2}.$$

This implies that under assumption (18) inequality (19) only holds when $\varphi_a = \varphi_b = \varphi_c = \pm \pi/3$.

Then, we deduce $|z_a|=2|\cos(\varphi_a)|=1$ and, similarly, $|z_b|=|z_c|=1$. Hence,

$$\alpha^a = \alpha^b = \alpha^c = -1 + e^{\pm \pi i/3} = e^{\pm 2\pi i/3}.$$

This can only happen if $|\alpha| = 1$. Moreover, α must be a root of unity, since $\alpha^{3a} = 1$. Set $\alpha = e^{2\pi ki/N}$ with some $N \in \mathbb{N}$ and $k \in \{0, ..., N-1\}$, where $\gcd(k,N)=1$. Then, $2\pi ika/N=\pm 2\pi i/3+2\pi is$ with $s\in \mathbb{Z}$, which implies $ka/N\mp 1/3\in \mathbb{Z}$. Multiplying by N we see that N must be divisible by 3. Hence, k is not divisible by 3. Similarly, $kb/N\mp 1/3\in \mathbb{Z}$ and $kc/N\mp 1/3\in \mathbb{Z}$, which by subtracting implies $k(b-c)/N\in \mathbb{Z}$. Hence, k0 must be divisible by k0, and so by 3, which is impossible because of (17). This completes the proof of the theorem.

Proof of Proposition 1.5. Assume that $k \ge 1$ and for some $j \in \{1, ..., k\}$ the polynomial $g = f_j \in \mathbb{Z}[x]$ of positive degree is not as claimed in the proposition. If g has no roots on |z| = 1 and g is not as claimed in the proposition, then it must have a root in |z| < 1 and a root in |z| > 1. We will show the same is true if g has a root on |z| = 1. Indeed, then, as not all roots of g are on |z| = 1, g must have a root g of modulus distinct from 1. Note that g is reciprocal, since it has a conjugate on |z| = 1. So g and g are conjugate over g. This implies that g has a root in |z| < 1 and a root in |z| > 1 as claimed.

Therefore, if $g = f_j$ is not as claimed in the proposition, it must have a root in 0 < |z| < 1 and a root in |z| > 1. This implies $s \le d - 2$. Assume that the nonzero roots of f defined in (6) are $\alpha_1, \ldots, \alpha_{d-s}$. Without restriction of generality we can label them as

$$|\alpha_1| \geq \cdots \geq |\alpha_q| > 1 \geq |\alpha_{q+1}| \geq \cdots \geq |\alpha_{d-s}|,$$

where $1 \le q \le d-s-1$ because $|\alpha_1| > 1$ and $|\alpha_{d-s}| < 1$. Then, by the definition of Mahler's measure,

$$m = |a|b\alpha_1 ... \alpha_q$$

with some (possibly negative) nonzero integer b. Here, the product $\alpha_1 \dots \alpha_q$ is a real number, because if α is a nonreal root of f then its complex conjugate $\overline{\alpha}$ is also its root with the same multiplicity.

Take an automorphism σ of the splitting field of f that maps the root α_i of g to its another root α_t , where $1 \le i \le q < t \le d - s$. Then, as $\sigma(\alpha_i) = \alpha_t$, $\sigma(m) = m$ and $\sigma(|a|b) = |a|b$, we obtain

$$m = \frac{|a|b\alpha_t}{\sigma(\alpha_i)} \prod_{j=1}^q \sigma(\alpha_1) \dots \sigma(\alpha_q).$$

Hence,

$$|\alpha_1 \dots \alpha_q| = \frac{m}{|ab|} = \frac{|\alpha_t|}{|\sigma(\alpha_i)|} |\sigma(\alpha_1) \dots \sigma(\alpha_q)| \le |\alpha_t| \cdot |\alpha_1 \dots \alpha_{q-1}|,$$

where the last inequality holds by the definition of $\alpha_1, \ldots, \alpha_q$ (these are the only roots of f outside the unit circle). This implies $|\alpha_t| \ge |\alpha_q|$, which is impossible due to $|\alpha_t| \le 1$ and $|\alpha_q| > 1$.

4. Proof of Theorem 1.1

For any $\mathbf{w} = (w_1, ..., w_d) \in \mathbb{C}^d$ and any $k \in \mathbb{N}$ we set

$$S_k(\mathbf{w}) = \sum_{j=1}^d w_j^k.$$

In the same fashion, for a polynomial

$$f(x) = a_d x^d + a_{d-1} x^{d-1} + \dots + a_0 = a_d (x - \alpha_1) \dots (x - \alpha_d) \in \mathbb{R}[x],$$

where $a_d \neq 0$, we denote by

$$S_k(f) = \sum_{j=1}^d \alpha_j^k$$

the sum of *k*th powers of its *d* roots.

Recall that, by the Newton identities, we have

$$a_d S_k(f) + a_{d-1} S_{k-1}(f) + \dots + a_{d-k+1} S_1(f) + a_{d-k} k = 0$$
 (20)

for k = 1, 2, ..., d. For any $m \in \mathbb{N}$ and any two distinct polynomials

$$f(x) = mx^d + a_{d-1}x^{d-1} + \dots + a_0 \in \mathbb{Z}[x]$$

and

$$g(x) = mx^d + b_{d-1}x^{d-1} + \dots + b_0 \in \mathbb{Z}[x],$$

where $a_d = b_d = m$, there is a unique index $k \in \{1, 2, ..., d\}$ such that $a_{d-j} = b_{d-j}$ for j = 0, 1, ..., k-1 and $a_{d-k} \neq b_{d-k}$. This yields $S_j(f) = S_j(g)$ for j = 1, ..., k-1. Thus, by (20), we deduce

$$m(S_k(f) - S_k(g)) + k(a_{d-k} - b_{d-k}) = 0.$$

Since $a_{d-k} - b_{d-k}$ is a nonzero integer, this implies

$$|S_k(f) - S_k(g)| \ge \frac{k}{m} \tag{21}$$

for this integer $k \in \{1, 2, ..., d\}$.

We now prove the bound

$$B = B(m, d) < \exp\left(10.4(md)^{\frac{2}{3}} \left(\log(md)\right)^{\frac{4}{3}}\right)$$
 (22)

for the number B(m, d) of polynomials $f \in \mathbb{Z}[x]$ of sufficiently large degree d with leading coefficient $m \in \mathbb{N}$ and all d roots in $|z| \le 1$.

Fix

$$X := 6md. \tag{23}$$

For each complex number z = x + iy satisfying $|z| \le 1$ we define

$$\hat{z} := \frac{\lfloor X|x| \rfloor \operatorname{sign}(x) + i \lfloor X|y| \rfloor \operatorname{sign}(y)}{X}.$$

Here, sign(x) = 1 for x > 0, sign(x) = -1 for x < 0 and sign(0) = 0. It is clear that $|\hat{z}| \le 1$ and $|z - \hat{z}| < \frac{\sqrt{2}}{x}$. Hence,

$$|z^{k} - \hat{z}^{k}| = |z - \hat{z}| \cdot |z^{k-1} + \dots + \hat{z}^{k-1}| < \frac{\sqrt{2k}}{X}.$$
 (24)

Since each \hat{z} is of the form $\frac{\mathbb{Z}+i\mathbb{Z}}{X}$, the distance between two distinct \hat{z} is at least 1/X. Consider a union of open circles at distinct \hat{z} with radii 1/(2X). They are not intersecting and are all in the circle with radius 1+1/(2X). If there are N of them, then

$$\pi \left(\frac{1}{2X}\right)^2 N < \pi \left(1 + \frac{1}{2X}\right)^2,$$

which, by (23), for d large enough, implies

$$N < (2X+1)^2 \le 145m^2d^2. \tag{25}$$

Likewise, for each vector $(\alpha_1, ..., \alpha_d) \in \mathbb{C}^d$, where $|\alpha_j| \leq 1$, we can define another vector $(\hat{\alpha}_1, ..., \hat{\alpha}_d) \in \mathbb{C}^d$. Accordingly, for $f \in \mathbb{Z}[x]$ of degree d with leading coefficient m and roots $\alpha_1, ..., \alpha_d$ we define

$$\hat{f}(x) = m(x - \hat{\alpha}_1) \dots (x - \hat{\alpha}_d).$$

By the definition of \hat{z} , the set $\{\hat{\alpha}_1, \dots, \hat{\alpha}_d\}$ is symmetric with respect to complex conjugation, since so is the initial set $\{\alpha_1, \dots, \alpha_d\}$. Hence, $\hat{f} \in \mathbb{R}[x]$ which implies $S_k(\hat{f}) \in \mathbb{R}$ for $k = 1, \dots, d$.

Assume that some two integer polynomials f, g of degree d with leading coefficient m are distinct. For each k = 1, ..., n, by (23), (24), we have

$$|S_k(f) - S_k(\hat{f})| < d\frac{\sqrt{2}k}{X} < \frac{k}{4m}.$$

Choosing k as in (21) we obtain

$$|S_k(\hat{f}) - S_k(\hat{g})| \ge |S_k(f) - S_k(g)| - |S_k(f) - S_k(\hat{f})| - |S_k(g) - S_k(\hat{g})|$$

$$> \frac{k}{m} - \frac{k}{4m} - \frac{k}{4m} = \frac{k}{2m}.$$

This implies that \hat{f} and \hat{g} are distinct and that the l_{∞} -distance between any distinct vectors of the form

$$\left(2mS_1(\hat{f}), \dots, \frac{2mS_k(\hat{f})}{k}, \dots, \frac{2mS_d(\hat{f})}{d}\right) \in \mathbb{R}^d$$
 (26)

is at least 1. Note that there are B distinct vectors as in (26), since f runs over B distinct polynomials.

Let *A* be the convex hull of the vectors

$$\left(2md\Re(u), \dots, \frac{2md\Re(u^k)}{k}, \dots, \frac{2md\Re(u^d)}{d}\right) \in \mathbb{R}^d, \tag{27}$$

where u runs over all possible (at most N) images of the unit circle $|z| \le 1$ under the map $z \to \hat{z}$. Each vector in (26) belongs to A, since it is the arithmetic mean

of some d vectors as defined in (27). Since the distance between any vectors as in (26) is at least one, their number B is bounded above by the volume of the set F(A) defined in (8), namely,

$$B \leq \operatorname{Vol}(F(A)).$$

Thus, by Lemma 2.1, we obtain

$$B \le 1 + \sum_{G} \text{Vol}(\Pr_{G}(A)). \tag{28}$$

where the sum is taken over all nonempty subsets G of $\{1, 2, ..., d\}$. By (27) and $|\Re(u^k)| \le 1$, the set A is contained in the parallelepiped

$$P = \prod_{j=1}^{d} [-u_j/2, u_j/2],$$

with $u_j = 4md/j$.

$$L := 10(md)^{2/3} \left(\log(md)\right)^{1/3}.$$
 (29)

Fix a nonempty subset G of $\{1, ..., d\}$ with |G| = g. Assume first that $g \ge L$, where L is defined in (29). By (25), $\Pr_G(A) \subseteq P$ is a convex polytope with at most

$$145m^2d^2 < L^3 \le g^3$$

vertices. So, by Lemma 2.2 and $\lambda \leq 3$, we obtain

$$\mathrm{Vol}\big(\mathrm{Pr}_{G}(A)\big) < \Big(\frac{46.44\log g}{g}\Big)^{g/2} \prod_{i \in G} u_{i} \leq \Big(\frac{46.44\log L}{L}\Big)^{g/2} \prod_{i \in G} u_{i}.$$

Inserting L from (29) and using the fact that d is large enough we obtain

$$\operatorname{Vol}(\Pr_{G}(A)) < \left(\frac{0.568(md)^{1/3}}{\left(\log(md)\right)^{1/3}}\right)^{-g} \prod_{j \in G} u_{j}. \tag{30}$$

On the other hand, in case g < L, by (29), we have

$$\left(\frac{0.568(md)^{1/3}}{\left(\log(md)\right)^{1/3}}\right)^g < \exp\left(\frac{10}{3}(md)^{2/3}\left(\log(md)\right)^{4/3}\right).$$

Hence, using the trivial bound $\operatorname{Vol}(\operatorname{Pr}_G(A)) \leq \prod_{i \in G} u_i$, we derive that

$$\frac{\operatorname{Vol}(\Pr_{G}(A))}{\exp\left(\frac{10}{3}(md)^{2/3}(\log(md))^{4/3}\right)} < \left(\frac{\left(\log(md)\right)^{1/3}}{0.568(md)^{1/3}}\right)^{g} \prod_{j \in G} u_{j}.$$
(31)

By (30), the bound (31) is true for every nonempty $G \in \{1, ..., d\}$, with g = |G|. Also, from (28) it follows that

$$B - \exp\left(\frac{10}{3}(md)^{2/3} (\log(md))^{4/3}\right) < B - 1 \le \sum_{G} \text{Vol}(\Pr_{G}(A)).$$

Dividing this inequality by a corresponding exponent and combining it with

$$\frac{\left(\log(md)\right)^{1/3}u_j}{0.568(md)^{1/3}} = \frac{4md\big(\log(md)\big)^{1/3}}{0.568\,j(md)^{1/3}} < \frac{7.05(md)^{2/3}\big(\log(md)\big)^{1/3}}{j},$$

from (31) we derive that

$$\frac{B}{\exp\left(\frac{10}{3}(md)^{2/3}\left(\log(md)\right)^{4/3}\right)} < \prod_{j=1}^{d} \left(1 + \frac{7.05(md)^{2/3}\left(\log(md)\right)^{1/3}}{j}\right).$$

Now, applying the inequalities $\prod_{j=1}^{d} (1 + y_j) < \exp(y_1 + \dots + y_d)$ and

$$\sum_{j=1}^{d} \frac{1}{j} \le \log d + 1 \le \log(md) + 1,$$

we can further bound

$$\prod_{j=1}^{d} \left(1 + \frac{7.05(md)^{2/3} \left(\log(md) \right)^{1/3}}{j} \right) < \exp\left(7.06(md)^{2/3} \left(\log(md) \right)^{4/3} \right).$$

This, by the above upper bound on B and by 10/3 + 7.06 < 10.4, implies the upper bound on B as claimed in (22).

Now, we will estimate the number D = D(m, d) of distinct integer polynomials of degree d and Mahler measure m. More precisely, we proceed to show that

$$D = D(m,d) < \exp\left(10.5(md)^{2/3} \left(\log(md)\right)^{4/3}\right). \tag{32}$$

In case m=1 the result follows by Proposition 1.2. In the case when $m \ge d^{1/2}$, we have $d \le (md)^{2/3}$ and $\log m \le \log(md) \le \left(\log(md)\right)^{4/3}$, so in view of (3) the required bound (32) follows by

$$D(m,d) \le m^{d(1+\varepsilon)} < \exp\left(2(md)^{2/3} \left(\log(md)\right)^{4/3}\right).$$

So, from now on, we assume that

$$2 \le m \le d^{1/2}. \tag{33}$$

Assume that $f \in \mathbb{Z}[x]$ is a polynomial of degree d and Mahler's measure $m \ge 2$. By Proposition 1.5 (see (6) and (7)), we can write f in the form

$$f(x) = f_1(x)f_2(x),$$

where $f_1 \in \mathbb{Z}[x]$ has the leading coefficient $\pm m_1$, degree d_1 and all roots in $|z| \le 1$, and $f_2 \in \mathbb{Z}[x]$ has the constant coefficient $\pm m_2$, degree $d_2 = d - d_1$ and all roots in |z| > 1. Here, m_1 and m_2 are positive integers such that $m_1 m_2 = m$, $M(f_1) = m_1$, $M(f_2) = M(f_2^*) = m_2$.

The number of such polynomials with $d_2 = 0$ is bounded above by 2B(m, d), where B(m, d) has been defined in (22). If $d_2 > 0$ then $m_2 > 1$. The number

of such polynomials with $d_1 = 0$ is bounded above by 2B(m, d) as well. If $m_1 = 1$ then f has all roots in $|z| \ge 1$, so the number of such polynomials can be bounded by 2B(m, d) too. Thus,

$$D(m,d) \le 6B(m,d) + E(m,d),\tag{34}$$

where B(m,d) has been defined in (22) and E(m,d) stands for the number of polynomials with Mahler's measure m representable in the form f_1f_2 , where $f_1 \in \mathbb{Z}[x]$ of degree $d_1 \geq 1$ has all roots in $|z| \leq 1$ and Mahler measure $m_1 \geq 2$, and $f_2 \in \mathbb{Z}[x]$ of degree $d_2 = d - d_1 \geq 1$ has all roots in |z| > 1 and Mahler measure $m_2 \geq 2$. (Of course, the part E(m,d) only appears for composite m.) Here, the leading coefficient of f_1 (with all roots in $|z| \leq 1$) is $\pm m_1$, and the leading coefficient of f_2^* (with all roots in |z| < 1) is $\pm m_2$. Consequently,

Note that there are at most m pairs of positive integers (m_1, m_2) satisfying $m_1m_2 = m$ and exactly d pairs of positive integers (d_1, d_2) for which $d_1 + d_2 = d$. Thus,

$$E(m,d) \le 4md \max_{\substack{m_1 m_2 = m, \rangle m_1, m_2 \ge 2 \\ \rangle d_1 + d_2 = d}} B(m_1, d_1) B(m_2, d_2).$$
(35)

Take a positive integer d_0 for which the bound (22) on B(m, d) is true for all $d \ge d_0$. For $d < d_0$ we will use the trivial bound

$$B(m,d) < c_6 m^{d+1}, (36)$$

where c_6 is a constant depending on d_0 only (see (3)).

Now, we are ready to show the required bound (32) for d large enough. Without loss of generality, we may assume that $d \ge 2d_0$. Also, from $d_1 + d_2 = d$ we see that at least one of the numbers d_1, d_2 is greater than or equal to d_0 . If both d_1 and d_2 are at least d_0 then the product $B(m_1, d_1)B(m_2, d_2)$ is less than

$$\exp\left(10.4(m_1d_1)^{2/3}\left(\log(m_1d_1)\right)^{4/3}+10.4(m_2d_2)^{2/3}\left(\log(m_2d_2)\right)^{4/3}\right)$$

by (22). This implies the required bound (32) by Lemma 2.3 with k=2 due to $m_1, m_2 \ge 2$, and (22), (34), (35).

Otherwise, we must have either $d_1 < d_0 \le d_2$ or $d_2 < d_0 \le d_1$. In the first case, $d_1 < d_0 \le d_2$, by (22) and (36), we obtain

$$B(m_1, d_1)B(m_2, d_2) < c_6 m_1^{d_1 + 1} \exp\left(10.4(m_2 d_2)^{2/3} \left(\log(m_2 d_2)\right)^{4/3}\right).$$

Here, the factor $c_6 m_1^{d_1+1}$ is very small, since from (33) it follows that

$$\log c_6 + (d_1 + 1)\log m_1 \le \log c_6 + (d_1 + 1)\log m < c_7 \log d.$$

This immediately yields the desired bound (32) by $m_2d_2 \le md$, (22), (34) and (35). It is clear that the second case, $d_2 < d_0 \le d_1$, is symmetric to that above and can be treated analogously. This completes the proof of Theorem 1.1.

References

- [1] AKIYAMA, SHIGEKI; DRUNGILAS, PAULIUS; JANKAUSKAS, JONAS. Height reducing problem on algebraic integers. Funct. Approx. Comment. Math. 47 (2012), 105–119. MR2987115, Zbl 1290.11144, doi: 10.7169/facm/2012.47.1.9. 829
- [2] AKIYAMA, SHIGEKI; PETHŐ, ATTILA. On the distribution of polynomials with bounded roots II. Polynomials with integer coefficients. *Unif. Distrib. Theory* 9 (2014), no. 1, 5–19. MR3237072, Zbl 1384.11081. 829, 831
- [3] AKIYAMA, SHIGEKI; ZAIMI, TOUFIK. Comments on the height reducing property. Cent. Eur. J. Math. 11 (2013), no. 9, 1616–1627. MR3071928, Zbl 1356.11074, doi: 10.2478/s11533-013-0262-4. 829
- [4] BÁRÁNY, IMRE; FÜREDI, ZOLTÁN. Approximation of the sphere by polytopes having few vertices. Proc. Amer. Math. Soc. 102 (1988), no. 3, 651–659. MR0928998, Zbl 0669.52003, doi: 10.2307/2047241.832
- [5] BOYD, DAVID W.; MONTGOMERY, HUGH L. Cyclotomic partitions. In: Number theory (Banff, AB, 1988), pp. 7–25, de Gruyter, Berlin, 1990. MR1106647, Zbl 0697.10040. 830
- [6] BRUNOTTE, HORST. On expanding real polynomials with a given factor. *Publ. Math. Debrecen* 83 (2013), no. 1-2, 161–178. MR3081232, Zbl 1274.11072, doi: 10.5486/PMD.2013.5568. 829
- [7] CHERN, SHEY-JEY; VAALER, JEFFREY D. The distribution of values of Mahler's measure. J. Reine Angew. Math. 540 (2001), 1–47. MR1868596, Zbl 0986.11017, doi: 10.1515/crll.2001.084. 829
- [8] DILL, GABRIEL A. On the frequency of height values. *Res. Number Theory* **7** (2021), no. 2, Paper No. 33, 33 p. MR4252906, Zbl 1479.11114, doi: 10.1007/s40993-021-00261-1. 829
- [9] DUBICKAS, ARTŪRAS. On the number of polynomials of small house. *Lithuanian Math. J.* **39** (1999), no. 2, 168–172. MR1754098, Zbl 0947.11032, doi: 10.1007/BF02469281. 832
- [10] DUBICKAS, ARTŪRAS. Mahler measures close to an integer. Canad. Math. Bull. 45 (2002), no. 2, 196–203. MR1904083, Zbl 1086.11049, doi: 10.4153/CMB-2002-022-8. 831
- [11] DUBICKAS, ARTŪRAS. Nonreciprocal algebraic numbers of small measure. *Comment. Math. Univ. Carolin.* **45** (2004), no. 4, 693–697. MR2103084, Zbl 1127.11070. 829
- [12] DUBICKAS, ARTŪRAS; JANKAUSKAS, JONAS. Nonreciprocal algebraic numbers of small Mahler's measure. Acta Arith. 157 (2013), no. 4, 357–364. MR3019421, Zbl 1284.11137, doi: 10.4064/aa157-4-3. 829, 831
- [13] DUBICKAS, ARTŪRAS; KONYAGIN, SERGEI V. On the number of polynomials of bounded measure. *Acta Arith.* **86** (1998), no. 4, 325–342. MR1659085, Zbl 0926.11080, doi:10.4064/aa-86-4-325-342. 829, 832
- [14] FILI, PAUL A.; POTTMEYER, LUKAS; ZHANG, MINGMING. On the behavior of Mahler's measure under iteration. *Monatsh. Math.* 193 (2020), no. 1, 61–86. MR4127434, Zbl 1450.11110, doi: 10.1007/s00605-020-01416-5. 831
- [15] FILI, PAUL A.; POTTMEYER, LUKAS; ZHANG, MINGMING. Wandering points for the Mahler measure. Acta Arith. 204 (2022), no. 3, 225–252. MR4460207, Zbl 1506.11138, doi: 10.4064/aa210930-6-5. 831
- [16] GALICER, DANIEL; MERZBACHER, MARIANO; PINASCO, DAMIÁN. Asymptotic estimates for the largest volume ratio of a convex body. *Rev. Mat. Iberoam.* **37** (2021), no. 6, 2347–2372. MR4310295, Zbl 1472.52008, doi:10.4171/rmi/1263.832
- [17] KIRSCHENHOFER, PETER; THUSWALDNER, JÖRG. Distribution results on polynomials with bounded roots. *Monatsh. Math.* 185 (2018), no. 4, 689–715. MR3777427, Zbl 1403.05009, doi: 10.1007/s00605-017-1054-x. 829
- [18] KOCHOL, MARTIN. A note on approximation of a ball by polytopes. *Discrete Optim.* **1** (2004), no. 2, 229–231. MR2099676, Zbl 1085.52502, doi: 10.1016/j.disopt.2004.07.003. 832
- [19] MIGNOTTE, MAURICE. Sur les nombres algébriques de petite mesure. In: Mathematics, CTHS: Bull. Sec. Sci., III, pp. 65–80, Bib. Nat., Paris, 1981. MR0638732, Zbl 0467.12008. 829

- [20] PRASOLOV VICTOR V. Polynomials. Algorithms and Computation in Mathematics, 11, Springer-Verlag, Berlin, 2010. MR2683151, Zbl 1272.12001. 830, 834
- [21] SCHINZEL, ANDRZEJ. Reducibility of lacunary polynomials. I. *Acta Arith.* **16** (1969/70), 123–159. MR0252362, Zbl 0196.06903, doi: 10.4064/aa-16-2-123-160. 834
- [22] SMITH, DAVID J.; VAMANAMURTHY, MAVINA K. How small is a unit ball? Math. Mag. 62 (1989), no. 2, 101–107. MR0991538, Zbl 0702.52006, doi: 10.1080/0025570X.1989.11977419.
 832
- [23] ZAITSEVA, TATYANA I.; PROTASOV, VALDIMIR YU. Self-affine 2-attractors and tiles. Sb. Math. 213 (2022), no. 6, 794–830. MR4461454, Zbl 1526.37021, doi:10.1070/SM9682. 829, 830, 831

(Artūras Dubickas) Institute of Mathematics, Faculty of Mathematics and Informatics, Vilnius University, Naugarduko 24, LT-03225 Vilnius, Lithuania arturas.dubickas@mif.vu.lt

This paper is available via http://nyjm.albany.edu/j/2024/30-37.html.