On Mahler's inequality
and small integral generators of
totally complex number fields

by

Murray Child and Martin Widmer (London)

Abstract. We improve Mahler's lower bound for the Mahler measure in terms of the discriminant and degree for a specific class of polynomials: complex monic polynomials of degree $d \geq 2$ such that all roots with modulus greater than some fixed value $r \geq 1$ occur in equal modulus pairs. We improve Mahler's exponent $\frac{1}{2d-2}$ on the discriminant to $\frac{1}{2d-3}$. Moreover, we show that this value is sharp, even when restricting to minimal polynomials of integral generators of a fixed non-totally-real number field.

An immediate consequence of this new lower bound is an improved lower bound for integral generators of number fields, generalising a simple observation of Ruppert from imaginary quadratic to totally complex number fields of arbitrary degree.

1. Introduction. In this short note we prove a new lower bound for the Mahler measure of a monic polynomial in $\mathbb{C}[x]$ whose "large" roots come in pairs of equal modulus. The bound is expressed in terms of the degree and the discriminant, and the dependence on the discriminant is best-possible. The result implies a new lower bound for the smallest integral generator of a totally complex number field.

We refer the reader to Smyth's survey article [14] (see also [9]) for a detailed account on the Mahler measure and its significance.

Our proofs are completely elementary and straightforward but the results seem to close a gap in the literature.

Let $f = a_0(x - \alpha_1) \cdots (x - \alpha_d) \in \mathbb{C}[x]$ be of degree $d \geq 2$. The *Mahler measure $M(f)$* and the *discriminant Δ_f* of f are defined by

$$M(f) := |a_0| \prod_{i=1}^{d} \max\{1, |\alpha_i|\} \quad \text{and} \quad \Delta_f := a_0^{2d-2} \prod_{1 \le i < j \le d} (\alpha_i - \alpha_j)^2.$$

Mahler's classical inequality bounds the former from below in terms of the latter.

THEOREM 1 (Mahler, 1964 [8]). *Let* $f \in \mathbb{C}[x]$ *be a polynomial of degree* $d \ge 2$. *Then*

$$M(f)^{2d-2} \ge d^{-d}|\Delta_f|.$$

Moreover, Mahler showed that we have equality if and only if $f = a_0 x^d + a_d$ with $|a_0| = |a_d| > 0$. Note that for irreducible $f \in \mathbb{Z}[x]$ this only happens when $f = \pm(x^d + 1)$ and d is a power of 2. However, for primes p the irreducible polynomials $f = (p+1)x^d - p$ in $\mathbb{Z}[x]$ satisfy (^{1})

$$M(f)^{2d-2} = d^{-d}|\Delta_f|\left(\frac{p+1}{p}\right)^{d-1},$$

and thus, even when restricting to irreducible polynomials, neither the exponent $2d - 2$ nor the constant d^{-d} can be improved. What if we restrict to monic irreducible polynomials in $\mathbb{Z}[x]$? Using Swan's discriminant formula for trinomials [15, Theorem 2] we get, for the p-Eisenstein polynomial $f = x^d + px^{d-1} + (-1)^{d+1}p$,

$$|\Delta_f| = p^{d-1}\big(d^d + ((d-1)p)^{d-1}\big) > (d-1)^{d-1}p^{2d-2}.$$

On the other hand, $M(f) \le (2 + 1/p)p < 3p$ (using inequality (1.2) below), and therefore

$$M(f)^{2d-2} < \left(\frac{9}{d-1}\right)^{d-1}|\Delta_f|.$$

Hence, at least the exponent $2d - 2$ is sharp, even when restricting to monic irreducible polynomials in $\mathbb{Z}[x]$.

Next, let us consider a monic quadratic polynomial $f = x^2 + bx + c$ with coefficients $b, c \in \mathbb{R}$ and no real roots. Then, as noted by Ruppert [12],

$$(1.1) \qquad M(f) = \max\left\{1, \frac{b^2 + |\Delta_f|}{4}\right\} \ge \frac{|\Delta_f|}{4}.$$

So instead of Mahler's exponent $2d - 2 = 2$ one obtains the much better exponent 1. This raises the question: can one improve Mahler's exponent $2d - 2$ when restricting to monic $f \in \mathbb{R}[x]$ with no real roots – and in particular, what is the sharp exponent in this case? We have been unable to find the answer in the literature but our next result shows that for such polynomials the exponent can be improved to $2d - 3$.

(^{1}) A simple calculation gives $|\Delta_f| = d^d(p(p+1))^{d-1}$ and $M(f) = p + 1$.

THEOREM 2. *Let m be non-negative and even, let $r \geq 1$, and let*

$$f(x) = \Big(\prod_{i=1}^{m/2} (x - \alpha_i)(x - \alpha_i') \Big) \Big(\prod_{i=m/2+1}^{d-m/2} (x - \alpha_i) \Big) \in \mathbb{C}[x]$$

be a monic polynomial of degree $d \geq 2$, with $|\alpha_i| = |\alpha_i'|$ for all $i = 1, \ldots, m/2$ and $|\alpha_i| \leq r$ for all $i = m/2 + 1, \ldots, d - m/2$. Then

$$M(f)^{2d-3} \geq (2r)^{d(1-d)} |\Delta_f|.$$

The exponent $2d-3$ in Theorem 2 is sharp, even when restricting to minimal polynomials of integral generators of a given non-totally-real number field.

Let K be a number field of degree d, and $\mathcal{O}_K$ its ring of integers. For $\alpha \in K$ we write $f_{\alpha,\mathbb{Z}}$ for the minimal polynomial ([2]) of α over $\mathbb{Z}$. Recall that $\alpha \in \mathcal{O}_K$ if and only if $f_{\alpha,\mathbb{Z}}$ is monic.

PROPOSITION 1. *Let K be a number field of degree d with a non-real embedding. Then there exists $c_K > 0$ depending only on K such that there are infinitely many $\alpha \in \mathcal{O}_K$ with $K = \mathbb{Q}(\alpha)$,*

$$M(f_{\alpha,\mathbb{Z}})^{2d-3} \leq c_K |\Delta_{f_{\alpha,\mathbb{Z}}}|,$$

and all roots of $f_{\alpha,\mathbb{Z}}$, except one pair of complex conjugate roots, have modulus at most c_K.

Under the hypothesis that the number field K possesses a real embedding one can prove in the same way that there are infinitely many $\alpha \in \mathcal{O}_K$ with $K = \mathbb{Q}(\alpha)$ and $M(f_{\alpha,\mathbb{Z}})^{2d-2} \leq c_K |\Delta_{f_{\alpha,\mathbb{Z}}}|$, and all roots of $f_{\alpha,\mathbb{Z}}$, except one, have modulus at most c_K.

Next we apply Theorem 2 to get a new lower bound for integral generators of totally complex number fields.

Let K be a number field. Then every $\alpha \in K$ with $K = \mathbb{Q}(\alpha)$ is called a *generator* of K. It is natural to ask: how "large" must a generator of K be in terms of the degree d and the modulus of the discriminant $|\Delta_K|$? And what happens if we restrict to *integral* generators? This problem has been studied by several authors, including Cochrane et al. [2], Dubickas [3], Eldredge & Petersen [4], Kihel & Lizotte [6], Pierce & Turnage-Butterbaugh & Wood [11], Ruppert [12], and Vaaler & Widmer [17, 16].

A good measure for size here is the Mahler measure $M(f_{\alpha,\mathbb{Z}})$ of the minimal polynomial $f_{\alpha,\mathbb{Z}}$ of α over $\mathbb{Z}$. Following Eldredge & Petersen [4] and Dubickas [3] we use the following notation:

$$M(K) := \min \{ M(f_{\alpha,\mathbb{Z}}) : \alpha \in K, \mathbb{Q}(\alpha) = K \}$$

([2]) The *minimal polynomial* $f_{\alpha,\mathbb{Z}}$ of α over $\mathbb{Z}$ is the unique polynomial in $\mathbb{Z}[x]$ of minimal degree with positive leading coefficient and coprime coefficients, vanishing at α.

and

$$M(\mathcal{O}_K) := \min \{M(f_{\alpha,\mathbb{Z}}) : \alpha \in \mathcal{O}_K, \mathbb{Q}(\alpha) = K\}.$$

Writing $\|f\|_1$ for the L^1-norm of the coefficient vector of f, by a result of Mahler [7] one has

(1.2) $$2^{-d}\|f\|_1 \leq M(f) \leq \|f\|_1$$

for each $f \in \mathbb{C}[x]$ of degree $d \geq 1$. Hence there are only finitely many polynomials $f \in \mathbb{Z}[x]$ of degree at most D and $M(f) \leq T$, irrespective of how large D and T are. This shows that the minima in the definitions of $M(K)$ and $M(\mathcal{O}_K)$ exist.

Now recall that if $\alpha \in \mathcal{O}_K$ with $K = \mathbb{Q}(\alpha)$ then $f_{\alpha,\mathbb{Z}}$ is monic and $\Delta_{f_{\alpha,\mathbb{Z}}} = \Delta_K[\mathcal{O}_K : \mathbb{Z}[\alpha]]^2$, where the positive integer $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ is the index of the order $\mathbb{Z}[\alpha]$ in the maximal order $\mathcal{O}_K$. Therefore Mahler's inequality (Theorem 1) implies

(1.3) $$M(\mathcal{O}_K) \geq d^{-\frac{d}{2d-2}} |\Delta_K|^{\frac{1}{2d-2}}.$$

Silverman [13] proved this bound holds even for $M(K)$, and it is known (^{3}) (cf. [12]) that the exponent $\frac{1}{2d-2}$ on $|\Delta_K|$ is sharp for $M(K)$ and every $d \geq 2$.

Ruppert [12] showed that $M(K) \ll_d |\Delta_K|^{\frac{1}{2d-2}}$ when $d = 2$ and asked [12, Question 1] whether this remains true when $d > 2$. This was answered in the negative by Vaaler & Widmer [17] for composite d, and by Dubickas [3] for prime $d \geq 3$. Ruppert [12, Question 2] also asked the analogous question with exponent $1/2$ instead of $1/(2d - 2)$. This question is still open but has been affirmatively answered for non-totally-complex number fields, and, conditionally under GRH, also for general number fields [16].

Less is known for $M(\mathcal{O}_K)$. The best general upper bound is

$$M(\mathcal{O}_K) \leq |\Delta_K|,$$

which follows easily from Minkowski's convex body theorem (cf. [10, Lemma 7.1]). The question of whether the exponent $1/(2d-2)$ in (1.3) is sharp seems more delicate than its counterpart for $M(K)$. The cubic case was affirmatively answered by Eldredge & Petersen [4, Theorem 1.1]. Motivated by a different question, Jones published a result [5, Theorem 1.5(3)] that gives an affirmative answer for all $d \in \{3, 4, 5, 7, 9\}$. He shows that if $(d, w) \in \{(3, 1), (4, 2), (5, 1), (7, 1), (9, 2)\}$ then there are infinitely many primes t such that

$$P_t(x) = x^d - 16d(dt + w)x^{d-1} + dt + w \in \mathbb{Z}[x]$$

_____

(^{3}) If $p < q < 2p$ are two primes and $K = \mathbb{Q}((p/q)^{1/d})$ then $M(K) \leq q < (2pq)^{1/2} \leq 2^{1/2}|\Delta_K|^{1/(2d-2)}$.

is irreducible and monogenic, i.e., $\mathcal{O}_K = \mathbb{Z}[\alpha]$ where $K = \mathbb{Q}(\alpha)$ and α is any root of $P_t(x)$. Hence, $\Delta_{P_t} = \Delta_K$, and Swan's discriminant formula shows that $|\Delta_{P_t}| \gg t^{2d-2}$ while (1.2) implies that $M(\mathcal{O}_K) \leq M(P_t) \ll t$.

However, just as for $M(K)$, the exponent $2d - 2$ is certainly not always sharp when $d > 2$. Eldredge & Petersen [4, Theorem 1.2] proved for cubic, and Dubickas ([4]) [3, Theorem 2] for arbitrary degrees $d \geq 2$, that there are infinitely many number fields K of degree d such that

$$\frac{1}{30}|\Delta_K|^{1/d} < M(\mathcal{O}_K) < \frac{4}{3}|\Delta_K|^{1/d}.$$

These fields K are very special and are all of the form $\mathbb{Q}(p^{1/d})$ for certain primes p. It would be interesting to find improved lower bounds that apply to more general families of number fields. Ruppert [12] observed that for all imaginary quadratic fields K,

(1.4) $$M(\mathcal{O}_K) \geq \frac{1}{4}|\Delta_K|.$$

The bound (1.4) suggests that such improvements of Mahler's exponent $1/(2d - 2)$ might hold for the family of totally complex fields of any fixed degree $d \geq 2$.

Theorem 2 with $m = d/2$ and $r = 1$ applied to the minimal polynomial of integral generators yields a generalisation of Ruppert's observation (1.4) to totally complex number fields of arbitrary degree d.

COROLLARY 1. *Let K be a totally complex number field of degree $d \geq 2$. Then*

$$M(\mathcal{O}_K) \geq 2^{\frac{d(1-d)}{2d-3}}|\Delta_K|^{\frac{1}{2d-3}}.$$

From number fields K back to polynomials $f \in \mathbb{C}[x]$, here is another application of Theorem 2. Mahler [8, Corollary to Theorem 1] combined Theorem 1 and formula (1.2) to get

(1.5) $$|\Delta_f| \leq d^d\|f\|_1^{2d-2}.$$

For polynomials f as in Theorem 2 we get a better bound whenever $\|f\|_1$ is sufficiently large.

COROLLARY 2. *For polynomials $f \in \mathbb{C}[x]$ satisfying the conditions in Theorem 2 we have*

$$|\Delta_f| \leq (2r)^{d(d-1)}\|f\|_1^{2d-3}.$$

Note that if K is a non-totally-real number field of degree d, and $f = f_{\alpha, \mathbb{Z}}$ is as in Proposition 1, then

$$\|f\|_1^{2d-3} \ll_K |\Delta_f|.$$

([4]) Dubickas proves the sharper inequality $(1 - \epsilon)|\Delta_K|^{1/d} < M(\mathcal{O}_K) < |\Delta_K|^{1/d}$ for arbitrary $\epsilon > 0$.

2. Discrete logarithmic energy for point configurations. Theorem 2 is proved by considering the complex roots of f as points in $\mathbb{R}^2$, and then bounding the logarithmic energy of this point configuration in $\mathbb{R}^2$ from below in terms of the number of points and the product of their Euclidean norms (ignoring those points inside the unit disc). Our simple argument is agnostic to the dimension and thus works for point configurations in arbitrary dimensions.

Let $k, d \in \mathbb{N}$, $d \geq 2$, let $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_d$ be points in $\mathbb{R}^k$, and set $\boldsymbol{\alpha} = (\boldsymbol{a}_1, \ldots, \boldsymbol{a}_d)$. We define

$$\mathfrak{M}(\boldsymbol{\alpha}) := \prod_{i=1}^{d} \max\{1, |\boldsymbol{a}_i|\},$$

and

$$|\Delta_{\boldsymbol{\alpha}}| := \prod_{1 \leq i < j \leq d} |\boldsymbol{a}_i - \boldsymbol{a}_j|^2,$$

where $|\cdot|$ on the right-hand side denotes the Euclidean norm on $\mathbb{R}^k$.

Note that $-\log|\Delta_{\boldsymbol{\alpha}}|$ is the discrete logarithmic energy $E_{\log}(\boldsymbol{\alpha})$ of a d-point configuration $\boldsymbol{\alpha}$ in $\mathbb{R}^k$ (cf. [1]), and thus our goal is to bound $E_{\log}(\boldsymbol{\alpha})$ from below in terms of $\mathfrak{M}(\boldsymbol{\alpha})$ and d. Mahler's inequality shows that $E_{\log}(\boldsymbol{\alpha})$ for a d-point configuration $\boldsymbol{\alpha}$ on the closed unit disc in $\mathbb{R}^2$ is at least $-d \log d$, and that this value is attained if and only if the points are equidistributed on the unit circle. But finding the minimal logarithmic energy $E_0(d; k)$ for a d-point configuration in the closed unit ball in $\mathbb{R}^k$ for higher dimensions $k \geq 3$ is a difficult open problem about which we have nothing to say.

Let $r \geq 1$ be a real number, and let $m \in \{0, 1, \ldots, d\}$ be the number of points $\boldsymbol{a}_i$ in $\boldsymbol{\alpha}$ with Euclidean norm strictly greater than r. We prove the following generalisation of Theorem 2.

THEOREM 3. *Suppose m is even and that the points in $\boldsymbol{\alpha}$ with Euclidean norm greater than r occur in pairs of equal Euclidean norm. Then*

$$(2.1) \qquad \mathfrak{M}(\boldsymbol{\alpha})^{2d-3} \geq (2r)^{d(1-d)} |\Delta_{\boldsymbol{\alpha}}|.$$

Moreover, the exponent $2d - 3$ is sharp.

The case $m = 0$ corresponds to an arrangement of d points in a closed ball of radius r in $\mathbb{R}^k$. In this case our theorem only yields the trivial lower bound $d(1 - d) \cdot \log(2r)$ for the logarithmic energy. On the other hand, it is clear from the proof that good lower bounds for $E_0(d - m; k)$ can be used to refine the constant $(2r)^{d(1-d)}$ in our theorem, at least if $d \geq m + 2$. However, in this work we are only concerned with the exponent of the discriminant and for simplicity we have decided to record only the simplest possible explicit constant which is $(2r)^{d(1-d)}$.

Proof of Theorem 3. Without loss of generality, we can relabel the points $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_d$ in $\boldsymbol{\alpha}$ in the order of decreasing Euclidean norm:

$$\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_1', \ldots, \boldsymbol{\alpha}_{m/2}, \boldsymbol{\alpha}_{m/2}', \boldsymbol{\alpha}_{m/2+1}, \boldsymbol{\alpha}_{m/2+2}, \ldots, \boldsymbol{\alpha}_{d-m/2},$$

where $|\boldsymbol{\alpha}_i| = |\boldsymbol{\alpha}_i'|$ $(i = 1, \ldots, \frac{m}{2})$. Note that the points of Euclidean norm strictly greater than r are exactly the m points $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_1', \ldots, \boldsymbol{\alpha}_{m/2}, \boldsymbol{\alpha}_{m/2}'$, so

$$|\boldsymbol{\alpha}_1| = |\boldsymbol{\alpha}_1'| \geq |\boldsymbol{\alpha}_2| = |\boldsymbol{\alpha}_2'| \geq \ldots \geq |\boldsymbol{\alpha}_{m/2}| = |\boldsymbol{\alpha}_{m/2}'|$$
$$> r \geq |\boldsymbol{\alpha}_{m/2+1}| \geq \ldots \geq |\boldsymbol{\alpha}_{d-m/2}|.$$

If any two of these points are equal then $|\Delta_{\boldsymbol{\alpha}}| = 0$, and (2.1) is trivially true. Hence, we can assume that all of them are distinct.

Recall that

$$\boldsymbol{\alpha} = (\boldsymbol{a}_1, \ldots, \boldsymbol{a}_d) = (\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_1', \ldots, \boldsymbol{\alpha}_{m/2}, \boldsymbol{\alpha}_{m/2}', \boldsymbol{\alpha}_{m/2+1}, \ldots, \boldsymbol{\alpha}_{d-m/2}),$$

so by definition of the discriminant we have

$$(2.2) \quad |\Delta_{\boldsymbol{\alpha}}| = \prod_{1 \leq i < j \leq d} |\boldsymbol{a}_i - \boldsymbol{a}_j|^2$$

$$= \prod_{i=1}^{m/2} \left(|\boldsymbol{\alpha}_i - \boldsymbol{\alpha}_i'|^2 \prod_{\boldsymbol{\beta} \in \beta_i} |\boldsymbol{\alpha}_i - \boldsymbol{\beta}|^2 |\boldsymbol{\alpha}_i' - \boldsymbol{\beta}|^2 \right) \prod_{m/2+1 \leq i < j \leq d-m/2} |\boldsymbol{\alpha}_i - \boldsymbol{\alpha}_j|^2,$$

where β_i means the set $\{\boldsymbol{\alpha}_{i+1}, \boldsymbol{\alpha}_{i+2}, \ldots, \boldsymbol{\alpha}_{d-m/2}, \boldsymbol{\alpha}_{i+1}', \boldsymbol{\alpha}_{i+2}', \ldots, \boldsymbol{\alpha}_{m/2}'\}$.

Let us start by evaluating the right-most product here, which we denote by C_0 for convenience ([5]). We have $|\boldsymbol{\alpha}_i|, |\boldsymbol{\alpha}_j| \leq r$ whenever $\frac{m}{2} + 1 \leq i < j \leq d - \frac{m}{2}$, so by the triangle inequality for all terms in this product,

$$|\boldsymbol{\alpha}_i - \boldsymbol{\alpha}_j|^2 \leq (|\boldsymbol{\alpha}_i| + |\boldsymbol{\alpha}_j|)^2 \leq (2r)^2.$$

Hence,

$$C_0 \leq \prod_{m+1 \leq i < j \leq n} (2r)^2 = (2r)^{2\binom{d-m}{2}} = (2r)^{(d-m)(d-m-1)}.$$

Now let us evaluate the left-most product in (2.2). Recalling that $|\boldsymbol{\alpha}_i| = |\boldsymbol{\alpha}_i'|$ $(i = 1, \ldots, m/2)$, we have

$$|\boldsymbol{\alpha}_i - \boldsymbol{\alpha}_i'|^2 \leq (|\boldsymbol{\alpha}_i| + |\boldsymbol{\alpha}_i'|)^2 = (2|\boldsymbol{\alpha}_i|)^2 = 2^2 |\boldsymbol{\alpha}_i|^2.$$

Likewise, noting that $|\boldsymbol{\beta}| \leq |\boldsymbol{\alpha}_i| = |\boldsymbol{\alpha}_i'|$ for all $\boldsymbol{\beta} \in \beta_i$ $(i = 1, \ldots, m/2)$, we have

$$|\boldsymbol{\alpha}_i - \boldsymbol{\beta}|^2 \leq 2^2 |\boldsymbol{\alpha}_i|^2 \quad \text{and} \quad |\boldsymbol{\alpha}_i' - \boldsymbol{\beta}|^2 \leq 2^2 |\boldsymbol{\alpha}_i|^2.$$

([5]) Of course the sharp upper bound here is $C_0 \leq r^{(d-m)(d-m-1)} e^{-E_0(d-m;k)}$ where $E_0(d-m;k)$ denotes the minimal logarithmic energy of a $(d-m)$-configuration in the unit ball in $\mathbb{R}^k$.

Combining this all, we get

$$|\Delta_{\boldsymbol{\alpha}}| \le C_0 \cdot \prod_{i=1}^{m/2} \left(2^2 |\boldsymbol{\alpha}_i|^2 \prod_{\boldsymbol{\beta} \in \beta_i} 2^2 |\boldsymbol{\alpha}_i|^2 \cdot 2^2 |\boldsymbol{\alpha}_i|^2 \right)$$

$$= C_0 \cdot \prod_{i=1}^{m/2} \left(2^2 |\boldsymbol{\alpha}_i|^2 \cdot (2^4 |\boldsymbol{\alpha}_i|^4)^{|\beta_i|} \right).$$

Now consider the number of elements in β_i. This is straightforward to calculate:

$$|\beta_i| = (d - m/2 - i) + (m/2 - i) = d - 2i.$$

So

$$|\Delta_{\boldsymbol{\alpha}}| \le C_0 \cdot \prod_{i=1}^{m/2} \left(2^2 |\boldsymbol{\alpha}_i|^2 \cdot (2^4 |\boldsymbol{\alpha}_i|^4)^{d-2i} \right)$$

$$= C_0 \cdot 2^m \cdot 2^{2dm} \cdot \prod_{i=1}^{m/2} (2^{-8i} |\boldsymbol{\alpha}_i|^{4d-8i+2})$$

$$= C_0 \cdot 2^{m(2d+1)} \cdot \prod_{i=1}^{m/2} 2^{-8i} \cdot \prod_{i=1}^{m/2} |\boldsymbol{\alpha}_i|^{4d-6-8i+8}$$

$$= C_0 \cdot 2^{m(2d-m-1)} \prod_{i=1}^{m/2} |\boldsymbol{\alpha}_i|^{4d-6} \cdot \prod_{i=1}^{m/2} |\boldsymbol{\alpha}_i|^{-8i+8}.$$

Let

$$C(d, m) := C_0 \cdot 2^{m(2d-m-1)}.$$

Then we see that

$$C(d, m) \le (2r)^{d^2+m^2-2dm-d+m} \cdot 2^{m(2d-m-1)}$$

$$= (2r)^{d(d-1)+m(m+1-2d)} \cdot 2^{m(2d-m-1)}$$

$$\le (2r)^{d(d-1)} \cdot 2^{m(m+1-2d+2d-m-1)} = (2r)^{d(d-1)},$$

where we have used $r \ge 1$ and $m + 1 - 2d \le d + 1 - 2d \le 0$. Hence,

$$|\Delta_{\boldsymbol{\alpha}}| \le (2r)^{d(d-1)} \prod_{i=1}^{m/2} |\boldsymbol{\alpha}_i|^{4d-6} \cdot \prod_{i=1}^{m/2} |\boldsymbol{\alpha}_i|^{-8i+8}$$

$$= (2r)^{d(d-1)} \prod_{i=1}^{m/2} (|\boldsymbol{\alpha}_i|^2)^{2d-3} \prod_{i=1}^{m/2} |\boldsymbol{\alpha}_i|^{-8i+8}$$

$$\le (2r)^{d(d-1)} \mathfrak{M}(\boldsymbol{\alpha})^{2d-3} \prod_{i=1}^{m/2} |\boldsymbol{\alpha}_i|^{-8i+8}.$$

Consider the remaining product here. We have $|\boldsymbol{\alpha}_i| > r \geq 1$ for all $i = 1, \ldots, m/2$; and $-8i + 8 \leq 0$ also for all $i = 1, \ldots, m/2$. Hence, $0 < |\boldsymbol{\alpha}_i|^{-8i+8} \leq 1$ for all $i = 1, \ldots, m/2$, and thus $0 < \prod_{i=1}^{m/2} |\boldsymbol{\alpha}_i|^{-8i+8} \leq 1$. We conclude that

$$|\Delta_{\boldsymbol{\alpha}}| \leq (2r)^{d(d-1)} \mathfrak{M}(\boldsymbol{\alpha})^{2d-3},$$

which proves inequality (2.1).

Finally, to see that the exponent $2d - 3$ is sharp it suffices to consider $d-2$ distinct fixed points on the $(k-1)$-sphere of radius r centred at the origin and to take the remaining two points $\boldsymbol{\alpha}_1$ and $\boldsymbol{\alpha}_1' = -\boldsymbol{\alpha}_1$ with arbitrarily large Euclidean distance. This completes the proof of Theorem 3. ∎

3. Upper bounds for the Mahler measure of minimal polynomials of integral generators. In this section we prove Proposition 1. Let K be a number field of degree d. Let $\sigma_i : K \to \mathbb{R}$ for $1 \leq i \leq r$ be the r real embeddings, and let $\sigma_i, \sigma_{i+s} : K \to \mathbb{C}$ for $r + 1 \leq i \leq r + s$ be the s pairs of complex conjugate embeddings, so that $d = r + 2s$. Let

$$\boldsymbol{\sigma} : K \to \mathbb{R}^r \times \mathbb{C}^s, \quad \alpha \mapsto (\sigma_1(\alpha), \ldots, \sigma_r(\alpha), \sigma_{r+1}(\alpha), \ldots, \sigma_{r+s}(\alpha))$$

be the Minkowski embedding of K, and set $\Lambda = \boldsymbol{\sigma} O_K \subseteq \mathbb{R}^r \times \mathbb{C}^s$. Identifying $\mathbb{C} \cong \mathbb{R}^2$ via the isomorphism $\alpha \mapsto (\mathrm{Re}(\alpha), \mathrm{Im}(\alpha))$ turns Λ into a lattice in $\mathbb{R}^d$. For the convenience of the reader we recall Proposition 1.

PROPOSITION 1. *Let K be a number field of degree d with a non-real embedding (i.e. $s \geq 1$). Then there exists $c_K > 0$ depending only on K such that there are infinitely many $\alpha \in \mathcal{O}_K$ with $K = \mathbb{Q}(\alpha)$,*

$$M(f_{\alpha,\mathbb{Z}})^{2d-3} \leq c_K |\Delta_{f_{\alpha,\mathbb{Z}}}|,$$

and all roots of $f_{\alpha,\mathbb{Z}}$, except one pair of complex conjugate roots, have modulus at most c_K.

Proof. For real $c, T \geq 1$ we define the subset $S_{c,T}$ of $\mathbb{R}^r \times \mathbb{C}^s$ as the set of points $\mathbf{x} = (x_1, \ldots, x_{r+s}) \in \mathbb{R}^r \times \mathbb{C}^s$ such that

$$\begin{cases} (2i-2)c < x_i < (2i-1)c & \text{for } i = 1, \ldots, r, \\ (2i-2)c < \mathrm{Re}(x_i) < (2i-1)c & \text{for } i = r+1, \ldots, r+s-1, \\ c < \mathrm{Im}(x_i) < 2c & \text{for } i = r+1, \ldots, r+s-1, \\ T < \mathrm{Re}(x_{r+s}) < T + c, \\ 3c + T < \mathrm{Im}(x_{r+s}) < T + 4c. \end{cases}$$

If we identify $\mathbb{R}^r \times \mathbb{C}^s$ with $\mathbb{R}^d$ like before, then $S_{c,T}$ is a box with sides parallel to the axes, each of length c. Therefore, there exists c_Λ such that $S_{c,T}$ contains a point of the lattice Λ whenever $c \geq c_\Lambda$.

Furthermore, for all $\mathbf{x} = (x_1, \ldots, x_{r+s}) \in S_{c,T}$,

$$|x_i - x_j| > c \quad (1 \le i < j \le r + s).$$

This implies that for $\alpha \in K$ and $\boldsymbol{\sigma}(\alpha) \in S_{c,T}$,

(3.1) $$|\sigma_i(\alpha) - \sigma_j(\alpha)| > c \quad (1 \le i < j \le r + s).$$

If $r + s + 1 \le i < j \le r + 2s$, then $|\sigma_i(\alpha) - \sigma_j(\alpha)| = |\overline{\sigma_{i-s}(\alpha) - \sigma_{j-s}(\alpha)}| = |\sigma_{i-s}(\alpha) - \sigma_{j-s}(\alpha)| > c$, by (3.1). If $1 \le i \le r + s$ and $j \ge r + s + 1$ then

$$|\sigma_i(\alpha) - \sigma_j(\alpha)| \ge |\mathrm{Im}(\sigma_i(\alpha)) - \mathrm{Im}(\sigma_j(\alpha))| > |0 - (-c)| = c.$$

We have shown that if $\alpha \in K$ and $\boldsymbol{\sigma}(\alpha) \in S_{c,T}$ then

(3.2) $$|\sigma_i(\alpha) - \sigma_j(\alpha)| > c$$

whenever $1 \le i < j \le d$.

Take $c = c_\Lambda \ge 1$ as before. Then there exists $\alpha \in \mathcal{O}_K$ such that $\boldsymbol{\sigma}(\alpha) \in \Lambda \cap S_{c,T}$. Let $f_{\alpha,\mathbb{Z}} \in \mathbb{Z}[x]$ be the minimal polynomial of α. Now (3.2) implies that $\sigma_i(\alpha) \ne \sigma_j(\alpha)$ for all $1 \le i < j \le d$. Hence, we conclude $\mathbb{Q}(\alpha) = K$. Finally, using (3.2) we get

$$\begin{aligned}
|\Delta_{f_{\alpha,\mathbb{Z}}}| &= \prod_{i \ne j} |\sigma_i(\alpha) - \sigma_j(\alpha)| \\
&= \prod_{\substack{i \ne j \\ i,j \ne r+s, r+2s}} |\sigma_i(\alpha) - \sigma_j(\alpha)| \cdot \prod_{i \ne r+s} |\sigma_i(\alpha) - \sigma_{r+s}(\alpha)|^2 \\
&\quad \cdot \prod_{\substack{i \ne r+2s \\ i \ne r+s}} |\sigma_i(\alpha) - \sigma_{r+2s}(\alpha)|^2 \\
&\ge c^{(d-3)(d-2)} \cdot T^{2(d-1)} \cdot T^{2(d-2)} = c^{(d-3)(d-2)} \cdot T^{2(2d-3)}.
\end{aligned}$$

On the other hand, using $|z| \le |\mathrm{Re}(z)| + |\mathrm{Im}(z)|$ for $z \in \mathbb{C}$, we get

(3.3) $$\begin{aligned}
M(f_{\alpha,\mathbb{Z}}) &= \prod_{i=1}^{d} \max\{1, |\sigma_i(\alpha)|\} \\
&\le \left((2(r+s-1)+1)c\right)^{d-2}(2T+5c)^2 \\
&\le (2dc)^{d-2}(3T)^2 \le (2dc)^d T^2,
\end{aligned}$$

provided $T \ge 5c$. Hence,

$$\begin{aligned}
M(f_{\alpha,\mathbb{Z}})^{2d-3} &\le (2dc)^{d(2d-3)} c^{-(d-3)(d-2)} |\Delta_{f_{\alpha,\mathbb{Z}}}| \le (2dc)^{d(2d-3)} |\Delta_{f_{\alpha,\mathbb{Z}}}| \\
&= c_K |\Delta_{f_{\alpha,\mathbb{Z}}}|,
\end{aligned}$$

where $c_K := (2dc)^{d(2d-3)}$ depends only on K, as c_Λ depends only on $\boldsymbol{\sigma}\mathcal{O}_K = \Lambda$.

Choosing a sequence of T's, say $T_1, T_2, \ldots$ with $T_{i+1} > T_i + c$, yields a sequence of disjoint boxes S_{c,T_i}, each box containing an admissible $\alpha_i \in \mathcal{O}_K$ with $K = \mathbb{Q}(\alpha_i)$ and $M(f_{\alpha_i,\mathbb{Z}})^{2d-3} \le c_K |\Delta(f_{\alpha_i,\mathbb{Z}})|$. Moreover, as observed

in (3.3), all roots of $f_{\alpha_i,\mathbb{Z}}$ have modulus at most $2dc \leq c_K$, except one pair of complex conjugate roots. This proves Proposition 1. ∎

It is clear that the above proof can be adapted to show that for any given number field K of degree $d \geq 2$ with at least one real embedding there exist infinitely many $\alpha \in \mathcal{O}_K$ with $K = \mathbb{Q}(\alpha)$,

$$M(f_{\alpha,\mathbb{Z}})^{2d-2} \leq c_K|\Delta_{f_{\alpha,\mathbb{Z}}}|,$$

and all roots of $f_{\alpha,\mathbb{Z}}$, except one, have modulus at most c_K.

References

[1] J. S. Brauchart and P. J. Grabner, *Distributing many points on spheres: Minimal energy and designs*, J. Complexity 31 (2015), 293–326.

[2] T. Cochrane, R. M. S. Dissanayake, N. Donohoue, M. I. M. Ishak, V. Pigno, C. Pinner and C. Spencer, *Minimal Mahler measure in real quadratic fields*, Experiment. Math. 25 (2016), 107–115.

[3] A. Dubickas, *Minimal Mahler measures for generators of some fields*, Rev. Mat. Iberoam. 39 (2023), 269–282.

[4] L. Eldredge and K. Petersen, *Minimal Mahler measure in cubic number fields*, Int. J. Number Theory 18 (2022), 2157–2169.

[5] L. Jones, *Monogenic Pisot and anti-Pisot polynomials*, Taiwanese J. Math. 26 (2022), 233–250.

[6] O. Kihel and J. Lizotte, *Small generators of quadratic fields and reduced elements*, J. Number Theory 132 (2012), 1888–1895.

[7] K. Mahler, *An application of Jensen's formula to polynomials*, Mathematika 7 (1960), 98–100.

[8] K. Mahler, *An inequality for the discriminant of a polynomial*, Michigan Math. J. 11 (1964), 257–262.

[9] J. McKee and C. Smyth, *Around the Unit Circle. Mahler Measure, Integer Matrices and Roots of Unity*, Springer, Cham, 2021.

[10] F. Pazuki and M. Widmer, *Bertini and Northcott*, Res. Number Theory 7 (2021), no. 1, art. 12, 18 pp.

[11] L. B. Pierce, C. L. Turnage-Butterbaugh and M. M. Wood, *An effective Chebotarev density theorem for families of number fields, with an application to ℓ-torsion in class groups*, Invent. Math. 219 (2020), 701–778.

[12] W. M. Ruppert, *Small generators of number fields*, Manuscripta Math. 96 (1998), 17–22.

[13] J. H. Silverman, *Lower bounds for height functions*, Duke Math. J. 51 (1984), 395–403.

[14] C. Smyth, *The Mahler measure of algebraic numbers: a survey*, in: Number Theory and Polynomials, London Math. Soc. Lecture Note Ser. 352, Cambridge, Univ. Press, Cambridge, 2008, 322–349.

[15] R. G. Swan, *Factorization of polynomials over finite fields*, Pacific J. Math. 12 (1962), 1099–1106.

[16] J. D. Vaaler and M. Widmer, *A note on generators of number fields* in: Diophantine Methods, Lattices, and Arithmetic Theory of Quadratic Forms, Contemp. Math. 587, Amer. Math. Soc., Providence, RI, 2013, 201–211.

[17] J. D. Vaaler and M. Widmer, *Number fields without small generators*, Math. Proc. Cambridge Philos. Soc. 159 (2015), 379–385.

Murray Child, Martin Widmer
Department of Mathematics
Royal Holloway, University of London
TW20 0EX Egham, UK
E-mail: murray.child.2020@live.rhul.ac.uk
         martin.widmer@rhul.ac.uk