MAHLER'S MEASURE AND ITS RELATED TWO OPEN PROBLEMS

by

Yun Wang
B. Sc., University of Northern British Columbia, 2022

THESIS SUBMITTED IN PARTIAL FULFILMENT OF
THE REQUIREMENTS OF THE DEGREE OF
MASTER OF SCIENCE
IN
MATHEMATICS

UNIVERSITY OF NORTHERN BRITISH COLUMBIA
April 2024

Abstract

The main achievement of the thesis is the proof that $1+\sqrt{17}$ is not a Mahler measure of an algebraic number. This answers a question of A. Schinzel posted in [6] in 2004. We also show that, theoretically, there exists an algorithm to reduce the shortness of a polynomial without changing its Mahler measure, a problem considered in [5] by J. McKee and C. Smyth. However the number of computations required makes this algorithm infeasible.

Contents

Chapter 1

Introduction

My graduate thesis is about Mahler measure. In this paper, I plan to solve two relevant open problems. We start by the key definition.

Definition 1 *Let* $P(z) = a_0 z^d + a_1 z^{d-1} + \ldots + a_d \in \mathbb{Z}[z]$ *with* $a_0 \neq 0$*, and let its zeros in* $\mathbb{C}$ *be* $\alpha_1, \alpha_2, \ldots, \alpha_d$*. The Mahler measure,* $M(P)$*, is defined to be the product of* $|a_0|$ *and all* $|\alpha_i|$ *for which* $|\alpha_i| > 1$*, where* $1 \leq i \leq d$*.*
$M(P) = |a_0| \prod_{|\alpha_i|>1} |\alpha_i|$

The Mahler measure of an algebraic number α is denoted by $M(\alpha)$.

Chapter 2

Is $1+\sqrt{17}$ a Mahler measure of an algebraic number?

This question was asked by A.Schinzel [6] and quoted by A.Dubickas [2] ,J.McKee and C.Smyth [5], P.A.Fili, L.Potmeyer, and M.Zhang [3], among others.
The Mahler measure of an algebraic number is defined as the Mahler measure of its minimal polynomial over $\mathbb{Z}$.

Lemma 1 *Let O_K be the ring of algebraic integers of a number field K. If*

$$f(x) = a\prod_{i=1}^{n}(x-\alpha_i) \in O_K[x]$$

then $a\alpha_1\ldots\alpha_s$ is an algebraic integer for $1 \leq s \leq n$.

The following proof will make this lemma more clear.

Proof 1 $f(x) = a\prod_{i=1}^{n}(x-\alpha_i) = ax^n - a\sigma_1 x^{n-1} + \cdots + (-1)^n a\sigma_n$. It's trivial to see that

$$\sigma_1 = \alpha_1 + \alpha_2 + \cdots + \alpha_n;$$

$$\sigma_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \cdots + \alpha_1\alpha_n + \alpha_2 + \cdots + \alpha_3\alpha_{n-1}\alpha_n;$$

$$\cdots$$

$$\sigma_n = \alpha_1\alpha_2\ldots\alpha_n.$$

The numbers $a, \sigma_1, \sigma_2, \sigma_n$ are all algebraic numbers because $f(x) \in O_K[x]$.
In order to prove that $a\alpha_1\ldots\alpha_s$ is an algebraic integer, it suffices to show that it is a root of a nonzero monic polynomial in $O_K[x]$. It is not difficult to check that

$$F(x) = \prod_{\rho\in S_n}(x - a\alpha_{\rho(1)}\cdots\alpha_{\rho(s)})$$

is such polynomial. Here S_n is the permutation group on the set of n elements. Indeed,the coefficients of F are sums of symmetric functions in $\alpha_1,\ldots,\alpha_n$ multiplied by powers of a. Each monomial in these functions is of the form $a^k\alpha_{i_1}^{n_1}\ldots\alpha_{i_m}^{n_m}$ with some positive integer m and $k \geq \max\{n_1,\ldots,n_m\}$. By the Fundamental Theorem of Symmetric Functions, the coefficients of F are polynomials in elementary symmetric functions $\sigma_1,\ldots,\sigma_n$ of the roots of f. Further, by examining the standard procedure for the conversion of a symmetric function into a polynomial in elementary symmetric functions, as outlined, for example in [4] we conclude that the monomials occurring in these polynomials are of the form $a^k\sigma_1^{m_1}\ldots\sigma_n^{m_n}$, where $k, m_1,\ldots,m_n$ are nonnegative integers, and $k \geq m_1+\cdots+m_n$, hence they are algebraic integers because $f \in O_K[x]$ and, consequently, $a\sigma_i$, $i = 1\ldots n$ are algebraic integers.

By using this lemma, we have the following corollary.

Corollary 1 *If $f \in \mathbb{Z}[x]$ is a nonzero polynomial,then $M(f)$, the Mahler's measure of f, is an algebraic integer.*

Proposition 1 *Let $K = \mathbb{Q}(\sqrt{d})$, where $d > 1$ is a square-free integer then every element of O_K has the form*

$$\begin{cases} \beta = b + c\sqrt{d}, & \textit{if } d \not\equiv 1 \mod 4 \\ \beta = b + c\frac{1+\sqrt{d}}{2}, & \textit{if } d \equiv 1 \mod 4. \end{cases},$$

where b and c are any rational integers.

Proposition 2 *Let $\beta > 1$ be an irrational algebraic integer in a real quadratic field $\mathbb{Q}(\sqrt{d})$ and let β' be its algebraic conjugate. If $|\beta'| \leq 1$, then β is a Mahler's measure of a monic irreducible polynomial in $\mathbb{Z}[x]$.*

Proof 2 $M(f) = \beta$ for $f(x) = (x-\beta)(x-\beta')$. We can see $f \in \mathbb{Z}[x]$ because its coefficients are symmetric functions of algebraic numbers.

The case of $|\beta'| > 1$ is more interesting. In this direction we have the following theorem.

Theorem 1 *Let $\beta > 1$ be an irrational algebraic integer in a real quadratic field $\mathbb{Q}(\sqrt{d})$ and suppose that $|\beta'| > 1$. Then β is not a Mahler's measure for any irreducible, monic polynomial in $\mathbb{Z}[x]$.*

Proof 3 For a contradiction, suppose that $f \in \mathbb{Z}[x]$ is a monic irreducible polynomial and $M(f) = \beta$. Let

$$f(x) = \prod_{i=1}^{n}(x - \alpha_i).$$

Suppose that $|\alpha_i| > 1$ for $1 \leq i \leq s$ and $|\alpha_i| \leq 1$ for $s+1 \leq i \leq n$. By the definition of Mahler measure, we have

$$\beta = M(f) = \prod_{i=1}^{s}|\alpha_i|, 1 \leq i \leq s.$$

Next,we claim that

$$\beta = \varepsilon\alpha_1 \ldots \alpha_s \text{ where } \varepsilon \in \{-1, +1\}.$$

For this note that if $|\alpha_i| > 1$ and $\alpha_i \in \mathbb{C} \setminus \mathbb{R}$ then $|\bar{\alpha}_i|$ is also greater than 1, so it occurs in the product $\alpha_1 \ldots \alpha_s$. Hence this product is a real number and, consequently $\beta = \pm\alpha_1 \ldots \alpha_s$.

Further, we must have $s < n$, since otherwise $M(f)$ will be equal to the constant term in $f(x)$ which is a rational integer.

For convenience we will denote the conjugates $\alpha_{s+1}, \ldots, \alpha_n$ by $\alpha'_1, \ldots, \alpha'_r$, so that $n = s + r$.

Let $L = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ and $K = \mathbb{Q}(\sqrt{d})$, so

$$\mathbb{Q} \subset K \subset L.$$

Then L/K and $L/\mathbb{Q}$ are Galois extensions. A finite extension L/K is called a Galois extension if $|Aut(L/K)| = [L : K]$. Let $G = Gal(L/\mathbb{Q})$ and $H = Gal(L/K)$. Let $D = |G|$ be the order of G. Then $|H| = \frac{D}{2}$, as $[K : Q] = 2$. In particular, D is even. Then we have

$$\sigma(\beta) = \beta \text{ for every } \sigma \in H$$

while

$$\sigma(\beta) = \beta' \text{ for every } \sigma \in G \setminus H.$$

The first statement implies that

$$\textit{Every } \sigma \in H \textit{ is a permutation of the set } S = \{\alpha_1, \ldots, \alpha_s\}$$
$$\textit{and a permutation of the set } R = \{\alpha'_1, \ldots, \alpha'_r\} \tag{2.1}$$

In order to see this, notice that $|\alpha_1 \ldots \alpha_s|$ is strictly larger than absolute value of any other product of s conjugates from the set $\{\alpha_1,\dots,\alpha_n\}$ because $|\alpha_i|>1$ for $i=1\dots s$. Since $|\sigma(\beta)|=|\beta|=|\prod_{i=1}^{s}\sigma(\alpha_1)\dots\sigma(\alpha_s)|$, all $\sigma(\alpha_i)$ for $1\le i\le s$ must belong to S. Further, σ is one-to-one from S to S, so a permutation of S. This implies that $\sigma(R)\cap S=\emptyset$, so that σ is also a permutation of R.

Now consider

$$\mathfrak{L}=\prod_{\sigma\in G}\sigma(\alpha_1\dots\alpha_s)=\prod_{\sigma\in G}\sigma(\alpha_1)\dots\sigma(\alpha_s).$$

The Galois group G acts transitively on the set $\{\alpha_1,\dots,\alpha_n\}$ because f is irreducible. Clearly $\mathfrak{L}$ is a product of conjugates and because of transitivity, each conjugate occurs in $\mathfrak{L}$ with the same frequency. Hence

$$\mathfrak{L}=(\alpha_1\dots\alpha_n)^{\frac{sD}{n}}=((-1)^n a_n)^{\frac{sD}{n}},$$

where $D=|G|$ is the order of G, and $a_n=f(0)$ is the constant term of f.

Observe that G is a disjoint union of two cosets $G=H\bigcup\sigma(H)$, where σ is any automorphism from $G\setminus H$.

By $\alpha_1\dots\alpha_s=\varepsilon\beta$ and $\sigma(\beta)=\beta$ for $\sigma\in H$ and $\sigma(\beta)=\beta'$ for $\sigma\in G\setminus H$ we get

$$\mathfrak{L}=\prod_{\sigma\in G}\sigma(\varepsilon\beta)=\prod_{\sigma\in H}\varepsilon\beta\prod_{\sigma\in G\setminus H}\beta'.$$

With our notation for β we have $\beta\beta'=N(\beta)=\begin{cases}b^2-c^2d, & \text{if } d\not\equiv 1 \mod 4\\ \frac{(2b+c)^2-c^2d}{4}, & \text{if } d\equiv 1 \mod 4\end{cases}.$

Hence

$$\mathfrak{L}=(\beta)^{\frac{D}{2}}(\beta')^{\frac{D}{2}}=N(\beta)^{\frac{D}{2}}=((-1)^n a_n)^{\frac{sD}{n}}$$

We get

$$|a_n|^{\frac{2s}{n}} = |N(\beta)| = |\beta\beta'| > |\beta| \text{ because } |\beta'| > 1.$$

However $|a_n| = |\alpha_1 \dots \alpha_s||\alpha_{s+1} \dots \alpha_n| \leq \beta$. Thus

$$\beta \geq |a_n| > \beta^{\frac{n}{2s}}$$

and we conclude that $2s > n$, so $2s > s + r$, $s > r$.

We shall show that the last inequality, $s > r$, together with (2.1) contradicts the irreducibility of f.

For this let

$$f_1(x) = \prod_{i=1}^{s}(x - \alpha_i) \text{ and } f_2(x) = \prod_{i=1}^{r}(x - \alpha_i').$$

The coefficients of these polynomials are symmetric functions of $\{\alpha_1, \dots, \alpha_s\}$ and $\{\alpha_1', \dots, \alpha_r'\}$, respectively. Hence by (2.1) they are preserved by any σ from H, also they are algebraic integers. By Galois theory we conclude that the coefficients of both polynomials are algebraic integers in the field K. Now, let σ be any automorphism in $G \setminus H$, then $f_i(x)\sigma(f_i(x))$ for $i = 1$ and $i = 2$ are in $\mathbb{Z}[x]$, because $\sigma(K) = K$, and its restriction to K is the nonidentity automorphism. Further $f(x) = f_1(x)f_2(x)$. We get

$$f^2(x) = f(x)\sigma(f(x)) = (f_1(x)\sigma(f_1(x)))(f_2(x)\sigma(f_2(x))).$$

The degree of integer polynomial $f_2(x)\sigma(f_2(x))$ is $2r < n$. However $f^2(x)$ as a product of two irreducible factors of degree n cannot have a factor of degree $2r < n$. This completes the proof of Theorem 1.

The main theorem

In [6] Schinzel studied the conditions under which a quadratic algebraic integer is a Mahler measure of an algebraic number. Let $\mathcal{M} = \{M(\alpha) | \alpha \in \bar{\mathbb{Q}}\}$, where $\bar{\mathbb{Q}}$ is the algebraic closure of $\bar{\mathbb{Q}}$.He proves there two theorems:

Theorem 2 *A primitive real quadratic integer β is in $\mathcal{M}$ if and only if there exists a rational integer a such that $\beta > a > |\beta'|$ and $a \mid \beta\beta'$, where $\beta'$is the conjugate of β. If the condition is satisfied then $\beta = M(\beta/a)$ and $a = N(a, \beta)$, where N denotes the absolute norm.*

Here 'primitive' means that β has no rational integer factor, other than ± 1. Let $\mathcal{J}$ be an ideal of O_K. The absolute norm of $\mathcal{J}$ is the number of residue class of in O_K, that is $N(\mathcal{J}) = |O_K/\mathcal{J}|$.For quadratic integers that are not primitive he considers the numbers $p\beta$, where p is a rational prime and β a primitive algebraic integer, and proves

Theorem 3 *Let K be a quadratic field with discriminant $\Delta > 0$, β, β' be primitive conjugate integers of K and p a prime. If*

1.
$$p\beta \in \mathcal{M},$$
then either there exists an integer r such that

2.
$$p\beta > r > p \quad \beta'| \text{ and } r \mid \beta\beta' \quad p \nmid r$$
or

3.
$$\beta \in \mathcal{M} \text{ and } p \text{ splits in } K$$
Conversely, (2) implies (1), while (3) implies (1) provided either

4.
$$\beta > \max\left\{-4\beta', \left(\frac{1+\sqrt{\Delta}}{4}\right)^2\right\}$$

or

5.

$$p > \sqrt{\Delta}.$$

In Schinzel's notation $1+\sqrt{17} = 2\beta$, where $\beta = \frac{1+\sqrt{17}}{2}$ is primitive and $p = 2$. With $K = \mathbb{Q}(\sqrt{17})$ we have $\Delta = 17$. Thus condition (2) fails, condition (3)is satisfied but without (4) or (5). This fact motivates Schinzel's question:

Is $1+\sqrt{17}$ a Mahler measure of an algebraic number?

Let α be an algebraic number and suppose that $M(\alpha) = \beta$. Then, by definition of $M(\alpha)$, we would have $M(\alpha) = M(f)$, where $f \in \mathbb{Z}[x]$ is the minimal polynomial of α. So f is irreducible in $\mathbb{Z}[x]$. However we shall prove that it is impossible for $\beta = 1+\sqrt{17}$. More specifically I shall prove the following theorem.

Theorem 4 *Let $f \in \mathbb{Z}[x]$ be irreducible over $\mathbb{Q}[x]$. If $M(f) = 1+\sqrt{17}$ then 2 divides the content of f and*

$$f(x) = 4x^{2s} \pm 2x^s - 4.$$

Note: In algebra, the *content* of a nonzero polynomial with integer coefficients is the greatest common divisor of its coefficients.This theorem implies that f is not a minimal polynomial of an algebraic number and consequently $\beta = 1+\sqrt{17}$ is not a measure of an algebraic number. For example, we can check directly that

$$M(4x^2 - 2x - 4) = M(4x^2 + 2x - 4) = \beta.$$

The content of both polynomials is 2, $c(4x^2 - 2x - 4) = c(4x^2 + 2x - 4) = 2$.

Proof 4 Suppose that $f \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Q}[x]$ and $M(f) = \beta$. The first step consists of showing that

Claim 1

$$f(x) = 4x^n + a_1x^{n-1} + \cdots + a_{n-1}x - 4.$$

Proof of claim 1 For this we are following the steps of Theorem 1.

Let $f(x) = a\prod_{i=1}^{n}(x - \alpha_i)$, where a is a positive integer and suppose that $|\alpha_i| > 1$ for $i = 1 \ldots s$ while $|\alpha_i| \leq 1$ for $i = s+1, \ldots, n$.

Again we use the notation $\alpha'_i = \alpha_{s+i}$ for $i = 1 \ldots r$, where $r = n - s$, $S = \{\alpha_1, \ldots, \alpha_s\}$ and $R = \{\alpha'_1, \ldots, \alpha'_r\}$, $L = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ and $K = \mathbb{Q}(\sqrt{17}) = \mathbb{Q}(\beta)$, $G = Gal(L/\mathbb{Q})$, and $H = Gal(L/K)$. Let $D = |G|$. Then again $|H| = D/2$, every σ from H is a permutation of S and R. Now

$$M(f) = \varepsilon a\alpha_1 \ldots \alpha_s, \text{ where } \varepsilon \in \{-1, +1\}.$$

This time we define

$$\mathfrak{L} = \prod_{\sigma \in G} \sigma(a\alpha_1 \ldots \alpha_s)$$

and conclude that

$$\mathfrak{L} = a^D(\alpha_1 \ldots \alpha_n)^{\frac{sD}{n}} = a^D(-1)^{sD}\left(\frac{a_n}{a}\right)^{\frac{sD}{n}},$$

where $a_n = f(0)$.

On the other hand $a\alpha_1 \ldots \alpha_s = \varepsilon\beta$, so that

$$\mathfrak{L} = \prod_{\sigma \in H} \sigma(\beta) \prod_{\sigma \in G \setminus H} \sigma(\beta) = (\beta\beta')^{D/2} = (-16)^{D/2},$$

as $\beta\beta' = (1 + \sqrt{17})(1 - \sqrt{17}) = -16$.

By comparing both expressions of $|\mathfrak{L}|$ we get

$$a^{\frac{D(n-s)}{n}} |a_n|^{\frac{sD}{n}} = 4^D$$

which simplifies to

$$(a^{\frac{D(n-s)}{n}}|a_n|^{\frac{sD}{n}})^{\frac{n}{D}} = (4^D)^{\frac{n}{D}} \text{ and so } a^r|a_n|^s = 4^n.$$

Further

$$|a_n| = |a\alpha_1 \dots \alpha_n| \leq |a\alpha_1 \dots \alpha_s| = \beta = 1 + \sqrt{17}.$$

Since the previous equation shows that $|a_n|$ is a power of 2 we conclude that

$$|a_n| \leq 4.$$

Now consider the polynomial

$$g(x) = sign(a_n)x^n f(x^{-1}).$$

If $f(x) = ax^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$ then $g(x) = \eta(a_nx^n + a_{n-1}x^{n-1} + \dots + a_1x + a)$, where $\eta = sign(a_n)$. We know that g is irreducible over $\mathbb{Q}[x]$ and that $M(g) = M(f)$ because of reciprocality. However, the leading coefficient of g is $|a_n|$, while its constant coefficient is ηa. By applying the same argument to g as we applied to f we conclude that $a \leq 4$.

The inequalities $|a_n| \leq 4$ and $a \leq 4$ together with $a^r|a_n|^s = 4^n$ show that $|a_n| = a = 4$. Hence $r = s$, so $n = 2s$ is even. Further we notice that every $\sigma \in G \setminus H$ maps S onto R and vice versa. Indeed, we have

$$|a_n| = a|\alpha_1 \dots \alpha_s||\alpha'_1 \dots \alpha'_r| \text{ and so } 4 = 4|\alpha_1 \dots \alpha_s||\alpha'_1 \dots \alpha'_r|.$$

and since $|\alpha_1 \dots \alpha_s| = \frac{\beta}{4}$ we deduce that $|\alpha'_1 \dots \alpha'_r| = \frac{4}{\beta}$. But $\frac{\beta}{4} = |\frac{4}{\beta'}| = |\sigma(\frac{4}{\beta})|$. Hence

$$|\sigma(\alpha'_1 \dots \alpha'_r)| = |\sigma(\alpha'_1) \dots \sigma(\alpha'_r)| = |\alpha_1 \dots \alpha_s|.$$

Hence the last term has strictly the largest value among absolute values of any choice of s conjugates, hence must have $\sigma(R) = S$. By applying σ to both sides of this equality and noticing that $\sigma^2 \in H$, because $\sigma^2(\sqrt{17}) = \sqrt{17}$, we also find out that $\sigma(S) = R$. Thus we have

$$a_n = (-1)^n a\alpha_1 \dots \alpha_n = (4\alpha_1 \dots \alpha_s)(\alpha'_1 \dots \alpha'_r) = (\varepsilon\beta)(\varepsilon\sigma(\beta/4)) = -4,$$

where σ is any automorphism in $G \setminus H$.

We have proved that f and g have the following forms:

$$f(x) = 4x^n + \sum_{i=1}^{n-1} a_i x^{n-i} - 4, \qquad g(x) = 4x^n - \sum_{i=1}^{n-1} a_{n-i} x^{n-i} - 4.$$

This concludes the proof of claim 1.

In the step 2, we separate f, g into 4 new polynomials and introduce some arithmetical facts.

We denote the roots of g by $\gamma_1, \dots, \gamma_s$ and $\gamma'_1, \dots, \gamma'_s$, where $\gamma_i = (\alpha'_i)^{-1}$, and $\gamma'_i = (\alpha_i)^{-1}$, for $i = 1 \dots s$. In what follows we use the fact that $K = \mathbb{Q}(\sqrt{17})$ has class number 1. This implies that every irreducible element in O_K is a prime element and the greatest common divisor is defined. Consequently the content of a polynomial is defined and we denote it by $c(f)$. It is determined uniquely up to a unit factor.

We need to establish some arithmetical facts about O_K

We have

- $u = 4 + \sqrt{17}$ is the fundamental unit. That means that group of unit of O_K is of the form $U = \{\pm u^n : n \in \mathbb{Z}\}$,
- $\pi_1 = \frac{-3+\sqrt{17}}{2}$ and $\pi_2 = \frac{-3-\sqrt{17}}{2}$ are primes,

- $\pi_1\pi_2 = -2$,
- $\frac{1+\sqrt{17}}{2} = u\pi_1^2$,
- $\frac{1-\sqrt{17}}{2} = -u^{-1}\pi_2^2$.

Next we define four polynomials:

$$\hat{f}(x) = 4\prod_{i=1}^{s}(x-\alpha_i), \quad \check{f}(x) = 4\prod_{i=1}^{s}(x-\alpha_i')$$

and

$$\hat{g}(x) = 4\prod_{i=1}^{s}(x-\gamma_i), \quad \check{g}(x) = 4\prod_{i=1}^{s}(x-\gamma_i').$$

Then by Lemma 1, all four polynomials are in $\mathbb{O}_K[x]$, and

- $4\alpha_1\ldots\alpha_s = \varepsilon\beta, \quad 4\alpha_1'\ldots\alpha_s' = \varepsilon\beta'$,
- $4\gamma_1\ldots\gamma_s = -\varepsilon\beta, \quad 4\gamma_1'\ldots\gamma_s' = -\varepsilon\beta'$,
- $4f(x) = \hat{f}(x)\check{f}(x)$ and $4g(x) = \hat{g}(x)\check{g}(x)$,
- $\hat{f}(0) = (-1)^s\varepsilon\beta = (-1)^s\varepsilon u 2\pi_1^2$,
- $\check{f}(0) = (-1)^s\varepsilon\beta' = -(-1)^s\varepsilon u^{-1}2\pi_2^2$,
- $\hat{g}(0) = -(-1)^s\varepsilon\beta = -(-1)^s\varepsilon u 2\pi_1^2$,
- $\check{g}(0) = -(-1)^s\varepsilon\beta' = (-1)^s\varepsilon u^{-1}2\pi_2^2$.

We can see that all zeros of $\hat{f}$ lie strictly outside the unit circle while the zeros of $\check{f}$ lie inside or on the unit circle. We shall show that, in fact, the zeros of $\check{f}$ must lie strictly inside the unit circle. For this, suppose that a zero of $\check{f}$, α lies on the unit circle. Then $\alpha \neq 1$ because $4f = \hat{f}\check{f}$, by our assumption is irreducible over $\mathbb{Q}$. Suppose then that $|\alpha| = 1$ and $\alpha \in \mathbb{C}\setminus\mathbb{R}$. Then $\bar{\alpha} = \alpha^{-1}$ is another zero of $\check{f}$. Then by transitivity of action of G on the zeros of f, $\{\sigma(\alpha^{-1})|\sigma \in G\} = \{\alpha_i^{-1} : i = 1\ldots n\}$

must be the set of the zeros of f, thus showing that f is reciprocal, so that we have $f(x) = 4\prod_{i=1}^{n}(x-\alpha_i) = 4\prod_{i=1}^{n}(x-\alpha_i^{-1})$

$$x^n f(x^{-1}) = 4x^n \prod_{i=1}^{n}(x^{-1}-\alpha_i) = 4\prod_{i=1}^{n}(1-x\alpha_i) = 4\prod_{i=1}^{n}(-\alpha_i)\prod_{i=1}^{n}(x-\alpha_i^{-1}) = -4\prod_{i=1}^{n}(x-\alpha_i^{-1}) = -f(x)$$

, because $4\prod_{i=1}^{n}(-\alpha_i) = a_n = -4$. Now substituting $x = 1$ gives $-f(1) = f(1)$. Hence $f(1) = 0$ which contradicts the irreducibility of f. We have

$$c(4f) = 4c(f) = c(\hat{f})c(\check{f}).$$

This implies that $4|c(\hat{f})c(\check{f})$. For any $\sigma \in G\setminus H$ we have $\sigma(\hat{f}) = \check{f}$ and $\sigma(\hat{g}) = \check{g}$. Thus, $2|c(\hat{f})$ if and only if $2|c(\check{f})$.Further, $4 = \pi_1^2\pi_2^2$ and $\pi_1\pi_2 = -2$, so if $2 \nmid c(\hat{f})$ then either $\pi_1 \nmid c(\hat{f})$ or $\pi_2 \nmid \hat{f}$. So We have two possibilities

1. $2|c(\hat{f})$ and $2|c(\check{f})$

   or

2. $\pi_1^2|c(\hat{f})$ and $\pi_2^2|c(\check{f})$.

Note that we cannot have $\pi_1^2|c(\check{f})$ and $\pi_2^2|c(\hat{f})$ because π_2 does not divide the constant term of $\hat{f}$. We claim that if the second possibility occurs then $2|c(\hat{g})$, so also $2|c(\check{g})$.

We have

$$\hat{g}(x) = \frac{4}{\check{f}(0)}x^s\check{f}(x^{-1}) = \frac{4\varepsilon u}{-(-1)^s 2\pi_2^2}x^s\check{f}(x^{-1}).$$

Hence $c(\hat{g}) = c(\pm\frac{2u}{\pi_2^2})c(x^s\check{f}(x^{-1})) = c(\pm\frac{2u}{\pi_2^2})c(\check{f})$, we deduce that $2|c(\hat{g})$ because $\pi_2^2|c(\check{f})$. Similarly, we show that $2|c(\check{g})$. However $M(f) = M(g)$, and if we prove that $g(x) = 4x^{2s} \pm 2x^s - 4$ then it would imply that $f(x) = 4x^{2s} \pm 2x^s - 4$ as well. Therefore if the second case occurs we can work with polynomial g instead of f, so without loss of generality we can assume that the first case occurs. We thus conclude that

$$\hat{f}_1(x) = \frac{1}{2}\hat{f}(x) = 2x^s + \sum_{i=1}^{s-1} A_i x^{s-i} + (-1)^s \varepsilon u \pi_1^2$$

and

$$\check{f}_1(x) = \frac{1}{2}\check{f}(x) = 2x^s + \sum_{i=1}^{s-1} \tilde{A}_i x^{s-i} - (-1)^s \frac{\varepsilon}{u} \pi_2^2$$

are in $O_K[x]$, and $f = \hat{f}_1(x)\check{f}_1(x)$ Here $\tilde{A}_i$ are algebraic conjugates of A_i, $i = 1 \dots s$.

In the final step, we'll show that all coefficients A_i is equal to 0 with Schur lemma.

The following is Schur [7] lemma, employed in the Schur-Cohn algorithm to determine the distribution of roots of a complex polynomial relative to the unit circle. The version below is presented in Wikipedia [8].

Lemma 2 *Let p be a complex polynomial of degree $n \geq 1$ and let p^* be defined by $p^*(z) = z^n \overline{p(\bar{z}^{-1})}$. Define Tp by $Tp = \overline{p(0)}p - \overline{p^*(0)}p^*$, and let $\delta = Tp(0)$.*

1. *If $\delta \neq 0$ then p, Tp, and p^* share zeros on the unit circle.*
2. *If $\delta > 0$ then p and Tp have the same number of zeros inside the unit circle.*
3. *If $\delta < 0$ then p^* and Tp have the same number of zeros inside the unit circle.*

If $\delta < 0$ the Tp and p^* have the same number of roots inside the unit circle.

We apply this lemma to

$$p(x) = x^s \hat{f}_1(x^{-1}) = (-1)^s \varepsilon u \pi_1^2 x^s + \sum_{i=1}^{s-1} A_i x^i + 2$$

and to $p*(x) = \hat{f}_1(x)$. Here p has all its roots inside the unit circle. We get

$$Tp(x) = \sum_{i=1}^{s-1} (2A_i - (-1)^s \varepsilon u \pi_1^2 A_{s-i}) x^i + 4 - \varepsilon^2 u^2 \pi_1^4.$$

$$\delta = 4 - \varepsilon^2 u^2 \pi_1^4 \approx -2.56 < 0$$

The polynomial $p*$ has no roots inside the unit circle, therefore the same is true about Tp. The degree of Tp is less than s. Suppose that $\deg Tp = i$ for some i, $1 \leq i \leq s-1$. Then the leading coefficient of Tp is $2A_i - (-1)^s \varepsilon u \pi_1^2 A_{s-i}$. Since all roots of Tp lie outside of the unit circle, we must have

$$|2A_i - (-1)^s \varepsilon u \pi_1^2 A_{s-i}| < |4 - \varepsilon^2 u^2 \pi_1^4| = |Tp(0)|.$$

Now we apply the same argument to $p = \check{f}_1 = 2x^s + \sum_{i=1}^{s-1} \tilde{A}_i x^{s-i} - (-1)^s \varepsilon \frac{1}{u} \pi_2^2$ whose roots lie inside the unit circle. Then $p^*(x) = -(-1)^s \varepsilon \frac{1}{u} \pi_2^2 x^s + \sum_{i=1}^{s-1} \tilde{A}_i x^i + 2$.

$$Tp(x) = \sum_{i=1}^{s-1} (-(-1)^s \varepsilon u^{-1} \pi_2^2 \tilde{A}_{s-i} - 2\tilde{A}_i) x^i + \varepsilon^2 u^{-2} \pi_2^4 - 4.$$

We find the corresponding

$$\delta = \varepsilon^2 \frac{1}{u^2} \pi_2^4 - 4 \approx -1.56 < 0$$

We conclude as in the previous case that

$$|\frac{-\varepsilon}{u} (-1)^s \pi_2^2 \tilde{A}_{s-i} - 2\tilde{A}_i| = |2\tilde{A}_i + \frac{\varepsilon}{u} (-1)^s \pi_2^2 \tilde{A}_{s-i}| < |\frac{1}{u^2} \pi_2^4 - 4|.$$

From both inequalities we get

$$|2A_i - (-1)^s \varepsilon u \pi_1^2 A_{s-i}||2\tilde{A}_i + \frac{\varepsilon}{u} (-1)^s \pi_2^2 \tilde{A}_{s-i}| = |N(2A_i - (-1)^s \varepsilon u \pi_1^2 A_{s-i})| < |4 - \varepsilon^2 u^2 \pi_1^4||\frac{1}{u^2} \pi_2^4 - 4| = 4,$$

where N is the norm from K to $\mathbb{Q}$. Further

$$2A_i - (-1)^s \varepsilon u \pi_1^2 A_{s-i} = -\pi_1 (\pi_2 A_i - (-1)^s \varepsilon u \pi_1 A_{s-i})$$

and

$$2\tilde{A}_i+\frac{\varepsilon}{u}(-1)^s\pi_2^2\tilde{A}_{s-i}=-\pi_2(\pi_1\tilde{A}_i-(-1)^s\frac{\varepsilon}{u}\pi_2\tilde{A}_{s-i}).$$

Hence

$$|N(\pi_2A_i+(-1)^s\varepsilon u\pi_1A_{s-i})|=\frac{1}{2}|N(2A_i-(-1)^s\varepsilon u\pi_1^2A_{s-i}|<2.$$

We conclude that $\pi_2A_i-(-1)^s\varepsilon u\pi_1A_{s-i}$ is a unit.

However we have

$$|\pi_2A_i+(-1)^s\varepsilon u\pi_1A_{s-i}|<|\frac{4-\varepsilon^2u^2\pi_1^4}{\pi_1}|<4.562$$

and

$$|\pi_1\tilde{A}_i-(-1)^s\frac{\varepsilon}{u}\pi_2\tilde{A}_{s-i}|<|\frac{\frac{1}{u^2}\pi_2^4-4}{\pi_2}|<0.4385$$

The last inequality excludes the possibility $\pi_2A_i+(-1)^s\varepsilon u\pi_1A_{s-i}=\pm1$. It remains the possibility that $\pi_2A_i+(-1)^s\varepsilon u\pi_1A_{s-i}=\pm u^k$ with $k\neq0$. However then $\pi_1\tilde{A}_i-(-1)^s\frac{\varepsilon}{u}\pi_2\tilde{A}_{s-i}=\pm u^{-k}$, but $\max(|u^k|,|u^{-k}|)\geq u=4+\sqrt{17}>4.562$, hence this possibility is also excluded. Finally, we have proved that Tp has degree 0, so that

$$\pi_2A_i+(-1)^s\varepsilon u\pi_1A_{s-i}=0 \text{ for } i=1\ldots s-1.$$

This implies that π_1 and π_2 divide each A_i for $i=1\ldots s-1$, so also divide each $\tilde{A}_i$. Thus $2|A_i$, so also $2|\tilde{A}_i$. Hence $A_i=2B_i$ with $B_i\in O_K$ for all$i$. and we get

$$\pi_2B_i+(-1)^s\varepsilon u\pi_1B_{s-i}=0 \text{ for } i=1\ldots s-1.$$

We can repeat the same argument again and conclude that $2|B_i$ for all i. After several repetitions we get

$$2^k|A_i \text{ for every positive integer } k \text{ and all } i.$$

Hence all coefficients A_i are zero. We have

$$\hat{f}_1 = 2x^s + (-1)^s \varepsilon u \pi_1^2 \text{and} \check{f}_1 = 2x^s - (-1)^s \varepsilon u^{-1} \pi_2^2.$$

Finally,with $d = s$ we get

$$f(x) = \frac{1}{4}\hat{f}\check{f} = \hat{f}_1\check{f}_1 = 4x^{2s} \pm 2x^s - 4.$$

This completes the proof of Theorem 4.

Chapter 3

Does there exists an algorithm to reduce the shortness of a polynomial without changing its Mahler measure?

J. McKee and C. Smyth in [5] mentioned that so far no algorithm that can reduce the shortness of a polynomial without changing its Mahler measure is known. To partially answer this problem, we need to use the theorem of Dobrowolski [1] and its corollary.

Definition 2 *Let* $P(x) = \sum_{i=0}^{n} a_i x^{n-i} \in \mathbb{C}[x]$. *The* length *of* P *denoted by* $L(P)$ *is the sum of absolute values of the coefficients of* P, *that is,* $L(P) = |a_0| + \cdots + |a_n|$.

Definition 3 *Let* $P(z) \in \mathbb{Z}[z]$. *A* short polynomial *for* P *is a polynomial of minimum length of the shape* $P(z)Q(z)$, *where* $Q(z)$ *is a product of cyclotomic polynomials.*

Definition 4 *The* shortness of a polynomial $P(z) \in \mathbb{Z}[z]$ *is the length of a short polynomial for* P. *The shortness of an algebraic integer* α *is the shortness of its minimal polynomial.*

In the following theorem, f_c denotes the product of all cyclotomic factors of f.

Theorem 5 *(Dobrowolski [1]) Let $f \in \mathbb{Z}[x]$, $f(0) \neq 0$, be a polynomial with k nonzero coefficients. There are positive constants c_1, c_2, depending only on k, and polynomials $f_0, f_2 \in \mathbb{Z}[x]$ such that if*

$$\deg f_c \geq (1 - \frac{1}{c_1}) \deg f$$

then either

- $f(x) = f_0(x^l)$, *where* $\deg f_0 \leq c_2$

  or

- $f(x) = (\prod_i \Phi_{q_i}(x^{l_i})) f_2(x)$, *where* $\min_i\{l_i\} > \max\{\frac{1}{2c_1} \deg f, \deg f_2\}$.

The size of the constants are: $c_i \leq \exp(3^{\lfloor \frac{k-2}{4} \rfloor} s_i k^2 \log k)$ with $s_1 = 0.636$ and $s_2 = 1.06$ for f with reciprocal exponents; $c_i \leq \exp(3^{\lfloor \frac{k-2}{2} \rfloor} t_i k^2 \log k)$ with $t_1 = 1.81$ and $t_2 = 2.841$ for f that does not have reciprocal exponents.

Note: In the second case in the original paper we have $\min_i\{l_i\} \geq \max\{\frac{1}{2c_1} \deg f, \deg f_2\}$ was not sharp, however the proof implies a sharp inequality.

Corollary 2 *Let $f(x) = \sum_{i=1}^{k} a_i x^{n_i} \in \mathbb{Z}[x], f(0) \neq 0$, be a polynomial with k nonzero coefficients. If the second case of Theorem 5 occurs then $f_2(x) = \pm \sum_{i=j}^{k} a_i x^{n_i}$ with some $j, 1 < j < k$.*

Note: In this theorem, we assume that $f(x) = \sum_{i=1}^{k} a_i x^{n_i}$ with k nonzero coefficients, the exponents $n_1, \ldots, n_k$ are strictly decreasing; f_c denotes the product of all cyclotomic factors of f, f_n denotes the product of all noncyclotomic factors and possibly a constant, so that $f = f_c f_n$. When we say f has reciprocal exponents, the exponents of x in $x^{\deg f} f(x^{-1})$ are the same as in $f(x)$. Φ_q denotes the qth cyclotomic polynomial. If $f(x) = f_0(x^l)$ occurs then also $f_n(x)$ is a polynomial in x^l. Hence, this case in the theorem is not interesting, because $M(f(x)) = M(f(x^l))$ for any polynomial f, so if we are studying Mahler measure we can assume that $f(x) \neq f_0(x^l)$ with $l > 1$.

Let $f_n \in \mathbb{Z}[x]$ be a monic and noncyclotomic polynomial, and $f_c(x) \in \mathbb{Z}[x]$ be a product of cyclotomic polynomials. Corollary 2 implies that if $f_c f_n$ has the minimal number of nonzero terms, we must have

$$\deg f_c < (1 - \frac{1}{c_1}) \deg(f_c f_n)$$

since otherwise the part of $f_n f_c$ which contains power of x with exponents less than some m, would form the polynomial f_2 that is a multiple of f_n and some cyclotomic polynomials, and has even smaller number of nonzero terms and which contradicts that $f_c f_n$ has minimal number of terms.

Concerning the minimal length of $f_c f_n$ we notice that if $f_c f_n$ has k nonzero terms then $L(f_c f_n) \geq k$. Thus for the shortest length we need to examine polynomials which have fewer than $L(f_n)$ nonzero terms. The inequality

$$\deg f_c < (1 - \frac{1}{c_1}) \deg(f_c f_n)$$

implies that

$$\deg f_c < (c_1 - 1) \deg f_n.$$

This means that if we want to find a polynomial with smallest number of nonzero coefficients that is a multiple of f_c and f_n, we can limit the search for polynomials f_c with $\deg f_c < (c_1 - 1) \deg f_n$. The same inequality applies for the search of shortest polynomials, but we have to replace k in c_1 by $L(f_n)$.

However, we tried to use the formula in the theorem 5 to calculate c_1 and find a bound of maximum degree of the product of cyclotomic polynomials required for the search, but even a very small values of k resulted in a bound exceeding computer's limit. Hence, the algorithm exists only theoretically and cannot be implemented for calculations.

Appendix A

Complementary facts

- All fields considered are subfields of $\mathbb{C}$, so we do not discuss separability.
- A field L is an *extension* of a field K if $K \subseteq L$, and the operations of K are those of L restricted to K.
- A *splitting field* of a polynomial with coefficients in a field is the smallest field extension of that field which contains the zeros of the polynomial.
- The *automorphism group* of a field extension L/K is the group consisting of field automorphisms of L that fix K, that is they are identities on K.
- If f is a polynomial over F and if E is its splitting field over F, then $G(E/F)$ denotes all automorphisms of E that fix F and it is called the *Galois group* of f over F.
- The *symmetric group* defined over any set is the group whose elements are all the bijections from the set to itself, and whose group operation is the composition of functions.

Theorem 6 *Let K be a quadratic field.Let $d = d(K)$. Let p be a rational prime. Then*

- $\langle p \rangle$ *splits* $\Leftrightarrow (\frac{d}{p}) = 1$,

- $\langle p \rangle$ *ramifies* $\Leftrightarrow (\frac{d}{p}) = 0$,

- $\langle p \rangle$ *is inert* $\Leftrightarrow (\frac{d}{p}) = -1$,

where $(\frac{d}{p})$ *is the Legendre symbol for* $p > 2$ *and Kronecker symbol for* $p = 2$.

Definition 5 *Let* d *be a nonsquare integer with* $d \equiv 0$ *or* $1 \mod 4$. *The Kronecker symbol* $\left(\frac{d}{2}\right)$ *is defined by*

$$\left(\frac{d}{2}\right) = \begin{cases} 0, & \textit{if } d \equiv 0 \mod 4, \\ 1, & \textit{if } d \equiv 1 \mod 8, \\ -1, & \textit{if } d \equiv 5 \mod 8 \end{cases} \tag{A.1}$$

Bibliography

[1] E. Dobrowolski, *Mahler's measure of a polynomial in terms of the number of its monomials*, Acta Arith. 123, 2006, 201–231.

[2] A. Dubickas, *Mahler measures in a cubic field*, Czechoslovak Math. J., 56(131), 2006, 949–956.

[3] P.A. Fili, L. Pottmeyer, and M. Zhang, *On the behavior of Mahler's measure under iteration*, Monathsh. Math. 193 (2020), 61–86.

[4] C. R. Hadlock, *Field theory and its classical problems*, MMA, CM 19, 1978.

[5] J. McKee and C. Smyth, *Around the unit circle*, Springer UTX 2021.

[6] A. Schinzel, *On values of the Mahler measure in a quadratic field (solution of a problem of Dixon and Dubickas)*,Acta Arith. 113.4 (2004), 401–408.

[7] I. Schur, *Über Potenzreichen, die im Innern des Einheitskreises beschränkt sind*, J. Reine Amgew. Math. 147(1917), 205–232.

[8] Wikipedia contributors, *Lehmer–Schur algorithm*, Wikipedia, The Free Encyclopedia, Retrived on Dec. 30, 2023, `https://en.wikipedia.org/w/index.php?title=Lehmer%E2%80%93Schur_algorithm&oldid=1189645486`