O.B. Berrevoets

On Lehmer's problem

Bachelor thesis

Supervisor: Dr J.H. Evertse

Date bachelor exam: 24 juni 2016

Mathematical Institute, Leiden University

Contents

1 Introduction

In this thesis, we will discuss lower bounds of the Mahler measure. First we examine two lower bounds given by Dobrowolski. Thereafter, we will consider polynomials which are 'near' products of cyclotomic polynomials. We will give another lower bound for the Mahler measure of such polynomials as well.

1.1 History of the Mahler measure

Lehmer gives a detailed study of a method for finding large primes in [10] in 1933. Suppose $\alpha_1, \ldots, \alpha_d \in \mathbb{C}$ are the roots of a monic polynomial f with integer coefficients. Then he defines for all $n \geq 1$ the rational integers

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

These numbers are called *Pierce numbers* and more information about these can be found in [15]. The large primes are sought after in the prime factorizations of those integers $\Delta_n(f)$ that have large absolute value. This can be done fairly quickly if the absolute values of $\Delta_1(f), \Delta_2(f), \ldots$ do not increase too rapidly. If f has no roots on the unit circle, then the limit $\lim_{n\to\infty} |\Delta_{n+1}(f)/\Delta_n(f)|$ exists and equals

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

[10, Theorem 16]. Therefore, Lehmer posed the question of whether for all $\varepsilon > 0$ there exists a monic polynomial $f \in \mathbb{Z}[X]$ with $1 < M(f) < 1 + \varepsilon$. It is conjectured that the answer is no [19], and this conjecture is known as Lehmer's conjecture. In [10], Lehmer finds a monic polynomial $\mathcal{L}$ with integer coefficients with $M(\mathcal{L}) = 1.176\ldots$. Since then, a monic polynomial f with integer coefficients and with $1 < M(f) < M(\mathcal{L})$ has not been found. Moreover, Lehmer's conjecture remains unsolved.

For a non-zero polynomial $f \in \mathbb{C}[X]$ with $f = a_0(X - \alpha_1)\ldots(X - \alpha_d)$ (again $\alpha_1, \ldots, \alpha_d \in \mathbb{C}$), we define

$$M(f) = |a_0| \prod_{i=1}^{d} \max\{1, |\alpha_i|\}.$$

The definition of $M(f)$ for a non-zero polynomial $f \in \mathbb{C}[X]$ coincides (see [20]) with a definition by Mahler: he defined in [12] in 1962 the quantity

$$M^*(f) := \exp\left(\int_0^1 \log \left| f(e^{2\pi i t}) \right| \, \mathrm{d}t \right).$$

For all non-zero $f \in \mathbb{C}[X]$ the real number $M^*(f) = M(f)$ is called the *Mahler measure* of f.

1.2 Results on Lehmer's conjecture

We notice that the Mahler measure of polynomials is multiplicative. So in order to find an answer on Lehmer's question, we only need to consider monic polynomials with coefficients in $\mathbb{Z}$ that are irreducible over $\mathbb{Q}$. If $\alpha \in \mathbb{C}$ is a zero of such a polynomial f, then α is called an *algebraic integer* and we define the Mahler measure of α as $M(\alpha) := M(f)$. In this case, the roots of f in $\mathbb{C}$ are called the *conjugates* of α, and f is called the *monic minimal polynomial* of α. If α is a non-zero algebraic integer, then Kronecker's theorem asserts that

$$M(\alpha) = 1 \quad \Longleftrightarrow \quad \alpha \text{ is a root of unity.} \tag{1}$$

This follows from the work of Kronecker in [8].

We will state the best results obtained concerning Lehmer's conjecture. For more results on Lehmer's conjecture, see [19]. By an irreducible polynomial with integer coefficients we mean irreducible over $\mathbb{Q}$. The first unconditional lower bound for $M(\alpha)$ for a non-zero algebraic integer α that is not a root of unity, was given by A. Schinzel and H. Zassenhaus in 1965 [17]. Namely, if α is such an algebraic integer, and if it has exactly $2s$ conjugates that are complex (i.e., elements of $\mathbb{C}\backslash\mathbb{R}$), then

$$M(\alpha) > 1 + 4^{-s-2}.$$

In 1979, Dobrowolski proved the following theorem. For all non-zero algebraic integers α of degree $d \geq 2$ that are not a root of unity, the inequality

$$M(\alpha) \geq 1 + c(d) \left(\frac{\log \log d}{\log d} \right)^3 \tag{2}$$

holds, where $c(d)$ only depends on d and is such that $\lim_{n\to\infty} c(n) = 1$. A key ingredient of his proof is the following: if p is a prime and α, α^p are algebraic integers of degree d, then the resultant of f_α and f_{α^p} is divisible by p^d. Furthermore, he uses Siegel's lemma to construct an auxiliary function. This result of Dobrowolski has been improved by Cantor and Straus in 1982 [3]. They proved the same statement with $\lim_{n\to\infty} c(n) = 2$. However, they used a different method: they construct a Vandermonde matrix whose determinant is an integer and has a large factor. Louboutin improved this in 1983 to the result with $\lim_{n\to\infty} c(n) = 9/4$, using the same proof as Cantor and Straus [11]. In 1996 Voutier obtained the explicit lower bound

$$M(f) \geq 1 + \frac{1}{4} \left(\frac{\log \log d}{\log d} \right)^3$$

for all monic irreducible polynomials f of degree $d \geq 2$ with $M(f) > 1$, also using the idea of Cantor and Straus [21].

A polynomial $f = f_0 + f_1 X + \cdots + f_d X^d$ with integer coefficients is called

reciprocal if $f = f_d + f_{d-1}X + \cdots + f_0X^d$. A polynomial that is not reciprocal is called *non-reciprocal*. In 1971, Smyth proves that all monic irreducible polynomials $f \in \mathbb{Z}[X]$ satisfying

$$M(f) < M(X^3 - X - 1) \approx 1.324\ldots$$

are reciprocal [20]. The constant $M(X^3 - X - 1)$ is optimal, since $X^3 - X - 1$ is non-reciprocal.

In 1999, Amoroso and David showed that Lehmer's conjecture is true for α such that the extension $\mathbb{Q} \subset \mathbb{Q}(\alpha)$ is Galois [1]. More precisely, they proved that there exists an $\varepsilon > 0$ such that for all non-zero algebraic numbers α, not a root of unity, and $\mathbb{Q} \subset \mathbb{Q}(\alpha)$ a Galois extension, we have $M(\alpha) > 1 + \varepsilon$. Borwein, Dobrowolski and Mossinghoff proved in [2] in 2007 that for all non-zero irreducible polynomials $f \in \mathbb{Z}[X]$ with only odd coefficients and $M(f) > 1$ we have $M(f) > 5^{1/4}$.

For a positive integer n we denote by $\omega(n)$ the number of distinct prime factors of n. For a polynomial $f \in \mathbb{C}[X]$, we write $\|f\|$ for the sum of the absolute values of the coefficients of f. For all positive integers n we denote by Φ_n the minimal polynomial of a n-th root of unity. In this thesis, we will prove the following. Let $n_1, \ldots, n_k$ be positive integers, f a monic irreducible polynomial with integer coefficients and assume that for $D := \|f - \Phi_{n_1} \ldots \Phi_{n_k}\|$ we have $D < \|f\|$. Also assume $M(f) > 1$. Then $s := 2^{\omega(n_1)} + \cdots + 2^{\omega(n_k)}$ gives

$$M(f) \geq 1 + \frac{\log 2}{\left(1 + \frac{1}{2}s^2\right) 2^{1+s/2}(D+1)}. \tag{3}$$

The proof is based on Dobrowolski's proof of (2). In particular, we use (3) to show that for a monic irreducible polynomial $f \in \mathbb{Z}[X]$ with $\|f - \Phi_p\| \leq 4$ for some prime p, we have $M(f) \geq 1.0115$.

2 Preliminaries

We call α *algebraic* if $\alpha \in \mathbb{C}$ and α is algebraic over $\mathbb{Q}$. We denote the set of algebraic numbers by $\overline{\mathbb{Q}}$. We will denote the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$ by $\overline{\mathbb{Q}}$, the set of algebraic numbers. For all $\alpha \in \overline{\mathbb{Q}}$, we will write f_α for the monic minimal polynomial of α over $\mathbb{Q}$. The *conjugates* of α are the algebraic numbers $\alpha_1, \ldots, \alpha_d$ such that $f_\alpha = (X - \alpha_1)\ldots(X - \alpha_d)$.

2.1 The Mahler measure

Definition 2.1. Let α be algebraic and let a be the smallest positive integer such that $af_\alpha \in \mathbb{Z}[X]$. Then the *primitive minimal polynomial* F_α of α is defined to be af_α.

Definition 2.2. Let $f \in \mathbb{C}[X]$ be a polynomial of degree $d > 0$ and let $a_d, \alpha_1, \ldots, \alpha_d \in \mathbb{C}$ be such that $f = a_d(X - \alpha_1)\ldots(X - \alpha_d)$. Then the *Mahler*

measure of f is given by

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

Definition 2.3. We define the *Mahler measure* of an algebraic number α to be $M(\alpha) := M(F_\alpha)$.

Example 2.4. Let $d > 0$ be an integer. Consider $\alpha := \sqrt[d]{2}$. Its minimal polynomial is $X^d - 2$ and the zeroes of this polynomial over $\mathbb{C}$ are $\exp(2\pi i/k)\sqrt[d]{2}$ for $k = 0, \ldots, d-1$. Hence, we find

$$M(\alpha) = \prod_{k=0}^{d-1} \max\left\{1, \left|\exp(2\pi i/k)\sqrt[d]{2}\right|\right\} = 2. \qquad \blacksquare$$

Notice that the Mahler measure is multiplicative: for two polynomials $f_1,\ f_2$ in $\mathbb{C}[X]$ we have $M(f_1 f_2) = M(f_1)M(f_2)$. Therefore, to understand the behaviour of the Mahler measure on $\mathbb{Z}[X]$, it suffices to consider only the irreducible polynomials in $\mathbb{Z}[X]$. Because of this, we will only study the Mahler measure of algebraic numbers. An algebraic number α is called an *algebraic integer* if $f_\alpha \in \mathbb{Z}[X]$. The sums and products of algebraic integers are again algebraic integers, as stated in the following proposition. A proof is given in [9, Chapter 1, Proposition 5].

Proposition 2.5. *The algebraic integers form a subring of* $\overline{\mathbb{Q}}$.

Corollary 2.6. *Let* α *be an algebraic integer and* $g \in \mathbb{Z}[X]$ *a polynomial. Then the norm and trace*

$$N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(g(\alpha)) \quad \textit{and} \quad \mathrm{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(g(\alpha))$$

are rational integers.

Proof. $g(\alpha)$ is an algebraic integer by Proposition 2.5. Hence, all its conjugates are algebraic integers. Let Σ be the set of field embeddings of $\mathbb{Q}(\alpha)$ into $\mathbb{C}$. Then we find that

$$N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(g(\alpha)) = \prod_{\sigma \in \Sigma} \sigma(g(\alpha))$$

is the product of algebraic integers. Hence, this norm is an algebraic integer. Since it is also rational, we conclude that it is a rational integer. Similarly, the trace can be proved to be a rational integer. $\square$

Notice that an algebraic number α is an algebraic integer if and only if $f_\alpha = F_\alpha$. Hence, all algebraic numbers α with $M(\alpha) < 2$ are algebraic integers. In fact, then also α^{-1} is an algebraic integer, which will be proven in Lemma 2.9.

Definition 2.7. An algebraic number α is called an *algebraic unit*, if $\alpha,\ \alpha^{-1}$ are algebraic integers.

We give a characterization of the algebraic units.

Lemma 2.8. *Let α be an algebraic integer. Then α is an algebraic unit if and only if $N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha) = \pm 1$.*

Proof. If α is an algebraic unit, then $N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)$, $N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha^{-1})$ are rational integers and $N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha^{-1}) = 1$, so $N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha) \in \{\pm 1\}$. Conversely, suppose that $N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha^{-1}) = \pm 1$. Let $\alpha_1, \alpha_2, \ldots, \alpha_d$ be the conjugates of α with $\alpha_1 = \alpha$. Notice that the product of algebraic integers

$$\alpha^{-1} = N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha^{-1})\alpha_2 \ldots \alpha_d = \pm \alpha_2 \ldots \alpha_d$$

is itself an algebraic integer by Proposition 2.5. □

Lemma 2.9. *Let α be an algebraic number and suppose $M(\alpha) < 2$. Then α is an algebraic unit.*

Proof. We have already seen that α is an algebraic integer. The product $N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)$ of all conjugates α is a rational integer by Corollary 2.6. Because $M(\alpha) < 2$ this norm now equals either 1 or -1. So α is an algebraic unit by Lemma 2.8. □

2.2 The house of an algebraic number

A concept related to the Mahler measure of an algebraic number, is the house of an algebraic number.

Definition 2.10. Let α be an algebraic number and $\alpha_1, \ldots, \alpha_d \in \mathbb{C}$ its conjugates. Then the *house* of α is given by $\overline{|\alpha|} := \max\{|\alpha_1|, \ldots, |\alpha_d|\}$.

Notice that for any non-zero algebraic integer α we have $\overline{|\alpha|} \geq 1$, since the product of the conjugates of α is a non-zero rational integer. For all non-zero algebraic integers α we also have

$$\overline{|\alpha|} \leq M(\alpha) \leq \overline{|\alpha|}^d. \tag{4}$$

The first inequality is obvious and the second inequality follows from $\overline{|\alpha|} \geq 1$ and the fact that $M(\alpha)$ is the product of some conjugates of α.

Lemma 2.11. *Let α be an algebraic number. Then $\overline{|\alpha^n|} = \overline{|\alpha|}^n$ for all integers $n > 0$.*

Proof. The Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts transitively on the conjugates of α, as well as on the conjugates of α^n. By the multiplicativity of the automorphisms, the set of the conjugates of α^n equals the set of n-th powers of the conjugates of α. Hence $\overline{|\alpha^n|} = \overline{|\alpha|}^n$. □

The following theorem follows from the work of Northcott, in which he proves a similar statement for points in a projective space [14, Theorem 1].

Theorem 2.12 (Northcott)**.** *Let $C, D > 0$ be real numbers. Then there are only finitely many algebraic integers α such that $\overline{|\alpha|} \leq C$ and $\deg \alpha \leq D$.*

Proof. Consider an algebraic integer α satisfying the inequalities. Write

$$f_\alpha = a_0 + \cdots + a_{d-1}X^{d-1} + X^d = (X - \alpha_1)\dots(X - \alpha_d)$$

with $\deg \alpha = d$ and $\alpha_1, \dots, \alpha_d \in \mathbb{C}$. Expanding the product and using the triangle inequality, we find that the coefficients of f are rational integers whose absolute values are bounded by $(2C)^D$:

$$|a_{d-n}| = \left| \sum_{i_1 \leq \cdots \leq i_n} \alpha_{i_1} \dots \alpha_{i_n} \right| \leq \binom{d}{n} |\overline{\alpha}|^n \leq (2C)^D \qquad \text{for } n = 1, \dots, d.$$

We conclude that there are only finitely many possible minimal polynomials of algebraic numbers satisfying the stated inequalities. □

The following theorem, known as Kronecker's theorem, follows from the work of Kronecker in [8].

Theorem 2.13 (Kronecker)**.** *Let α be an algebraic integer. Then*

$$|\overline{\alpha}| = 1 \quad \iff \quad \alpha \text{ is a root of unity.}$$

Proof. The equivalence is clear for $\alpha = 0$. So assume $\alpha \neq 0$. If α is a root of unity, then all conjugates of α are roots of unity and hence $|\overline{\alpha}| = 1$. Now suppose $|\overline{\alpha}| = 1$. To show that α is a root of unity, consider the sequence $\{\alpha^n\}_{n=1}^{\infty}$, which consists of algebraic integers by Proposition 2.5. The elements of this sequence have degree at most $\deg \alpha$ and for all $n \in \mathbb{Z}_{>0}$ we have $|\overline{\alpha^n}| = |\overline{\alpha}|^n = 1$ by Lemma 2.11. By Theorem 2.12 the sequence only contains finitely many distinct elements. Hence, there exist distinct $k, l \in \mathbb{Z}_{>0}$ such that $\alpha^k = \alpha^l$. Since $\alpha \neq 0$, we conclude that α is a root of unity. □

Remark 2.14. Not every algebraic number α with $|\overline{\alpha}| = 1$ is a root of unity. For instance, $\alpha = (3 + 4i)/5$ is not an algebraic integer and thus not a root of unity. ■

If α is an algebraic integer with $M(\alpha) = 1$, then it follows from Theorem 2.13 that α is a root of unity. In 1933 Lehmer posed the question whether for all real $\varepsilon > 0$ there exists a non-zero algebraic number α that is not a root of unity and is such that $M(\alpha) < 1 + \varepsilon$ holds [10]. The following has been conjectured and this conjecture is known as Lehmer's conjecture.

Conjecture 2.15. There exists a real number $\varepsilon > 0$ such that for all non-zero algebraic numbers α which are not a root of unity, we have $M(\alpha) > 1 + \varepsilon$.

Example 2.16. Consider the polynomial

$$\mathcal{L} := X^{10} + X^9 - X^7 - X^6 - X^5 - X^4 - X^3 + X + 1.$$

It has exactly 8 roots on the unit circle [13]. The other two roots are real numbers, of which one has an absolute value larger than 1. Therefore, $M(\mathcal{L})$ equals the largest real root and we find $M(\mathcal{L}) \approx 1.176$. To this day, a non-zero

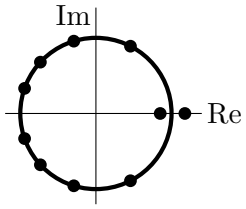

Figure 1: roots of $\mathcal{L}$ in the complex plane. The circle is the unit circle.

polynomial $f \in \mathbb{Z}[X]$ with $1 < M(f) < M(\mathcal{L})$ has not been found. ■

There are similar results to Conjecture 2.15, but where ε depends on the degree of α. We will examine such a result in the next section.

2.3 A lower bound for the house

The next result is due to Dobrowolski and can be found in [4]. It provides a lower bound for the house of a non-zero algebraic number α which is not a root of unity.

Theorem 2.17 (Dobrowolski)**.** *Let α be a non-zero algebraic integer of degree d. Suppose*

$$|\overline{\alpha}| \leq 1 + \frac{1}{4ed^2}, \quad \text{where } e = 2.718\ldots.$$

Then α is either zero or a root of unity.

However, Schinzel and Zassenhaus conjectured a stronger bound: there exists a constant $c > 0$ such that for all non-zero algebraic integers α that are not a root of unity, we have $|\overline{\alpha}| \geq 1 + c/d$ where d is the degree of α [17]. This conjecture is true if Lehmer's conjecture is true by (4). Also notice that by (4) this theorem of Dobrowolski gives a lower bound for the Mahler measure of a non-zero algebraic integer α that is not a root of unity.

To prove Theorem 2.17, we need a few lemmas. The following useful lemma resembles the linearity of the Frobenius automorphism on finite fields.

Lemma 2.18. *Let $f \in \mathbb{Z}[X_1, \ldots, X_n]$ be a polynomial and $p \in \mathbb{Z}_{>0}$ be prime. Denote by (p) the prime ideal of $\mathbb{Z}[X_1, \ldots, X_n]$ generated by p. Then*

$$f(X_1, \ldots, X_n)^p \equiv f(X_1^p, \ldots, X_n^p) \mod (p).$$

Proof. We prove this by induction on the number of terms of f. We will write $\mathbf{X} = (X_1, \ldots, X_n)$ and $\mathbf{X}^p = (X_1^p, \ldots, X_n^p)$. If f has only one term, the statement follows from Fermat's little theorem: for any $a \in \mathbb{Z}$ we have

$$(a\mathbf{X})^p = a^p \mathbf{X}^p \equiv a\mathbf{X}^p \mod (p).$$

Now suppose f has at least 2 terms and assume the assertion holds for all polynomials with fewer terms. Write $f = f_1 + f_2$ with $f_1, f_2 \in \mathbb{Z}[X_1, \ldots, X_n]$

both having fewer terms than f. Since the ring $\mathbb{Z}[X_1, \ldots, X_n]/(p)$ has characteristic p, the identity $(a+b)^p = a^p + b^p$ holds for all $a, b \in \mathbb{Z}[X_1, \ldots, X_n]/(p)$. By the induction hypothesis, we find

$$\begin{aligned} f(\mathbf{X})^p &= (f_1(\mathbf{X}) + f_2(\mathbf{X}))^p \equiv f_1(\mathbf{X})^p + f_2(\mathbf{X})^p \\ &= f_1(\mathbf{X}^p) + f_2(\mathbf{X}^p) \equiv f(\mathbf{X}^p) \mod (p). \end{aligned}$$

This proves the induction step. □

The prime p with which Lemma 2.18 will be applied to prove Theorem 2.17, will be chosen by means of Bertrand's postulate. A proof can be found in [6].

Lemma 2.19 (Bertrand's postulate)**.** *For all real $x > 1$ there exists a prime p such that $x < p < 2x$.*

We finish with two other lemmas which are needed for the proof of Theorem 2.17.

Lemma 2.20. *Let $S_0, \ldots, S_d \in \mathbb{Z}[T_1, \ldots, T_d]$ be the elementary symmetric polynomials, i.e., such that*

$$(X - T_1) \ldots (X - T_d) = S_0 X^d - S_1 X^{d-1} \pm \cdots + (-1)^d S_d.$$

For all positive integers n, write $\Sigma_n = T_1^n + \cdots + T_d^n$. Then $S_0, \ldots, S_d$ are elements of $\mathbb{Q}[\Sigma_1, \ldots, \Sigma_n]$.

Proof. This follows inductively from the Newton identities: for all $n = 1, \ldots, d$ we have

$$\Sigma_n S_0 - \Sigma_{n-1} S_1 + \Sigma_{n-2} S_2 \mp \cdots + (-1)^{n-1} \Sigma_1 S_{n-1} + (-1)^n n S_n = 0$$

[18]. □

We follow the proof of the following lemma of Dobrowolski in [5].

Lemma 2.21. *Let α be an algebraic number and suppose there exist distinct $k, l \in \mathbb{Z}_{>0}$ such that α^k and α^l are conjugate. Then $\alpha = 0$ or α is a root of unity.*

Proof. Let $k, l \in \mathbb{Z}_{>0}$ be distinct and such that α^k and α^l are conjugate. Let $K \subset \mathbb{C}$ be the splitting field of f_α, i.e., K is the field extension of $\mathbb{Q}$ generated by the conjugates of α. Let $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ be such that $\sigma(\alpha^k) = \alpha^l$. By induction it follows that

$$\sigma^n\big(\alpha^{k^n}\big) = \alpha^{l^n} \quad \text{for all } n \in \mathbb{Z}_{>0}. \tag{5}$$

Indeed, the base case $n = 1$ is trivial and the induction step follows from the fact that for all positive integers n we have

$$\sigma^n\big(\alpha^{k^n}\big) = \sigma^{n-1}(\sigma(\alpha^k))^{k^{n-1}} = \sigma^{n-1}(\alpha^l)^{k^{n-1}} = \sigma^{n-1}\big(\alpha^{k^{n-1}}\big)^l.$$

Let N be the order of σ in the finite group $\mathrm{Gal}(K/\mathbb{Q})$. From (5) we now find

$$\alpha^{k^N} = \sigma^N\left(\alpha^{k^N}\right) = \alpha^{l^N}.$$

From $k \neq l$ we conclude that α is either zero or a root of unity. □

Proof of Theorem 2.17. We will show that α is either 0 or a root of unity. Let $\alpha_1, \ldots, \alpha_d$ be the conjugates of α. By Bertrand's postulate, there is a prime p such that $2ed < p < 4ed$.

Define $\sigma_n := \alpha_1^n + \cdots + \alpha_d^n$. We will prove $\sigma_{np} = \sigma_n$ for any $n \in \{1, \ldots, d\}$. Consider such an n. We will use the primality of p to prove $\sigma_{np} \equiv \sigma_n \pmod{p}$ and use the bounds on p to show that $|\sigma_{np} - \sigma_n| < p$. Since the trace $\mathrm{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha^n)$ equals σ_n, we have $\sigma_n \in \mathbb{Z}$ by Corollary 2.6. By Lemma 2.18, there is a $g_n \in \mathbb{Z}[T_1, \ldots, T_d]$ such that $\sigma_n^p - \sigma_{np} = p g_n(\alpha_1, \ldots, \alpha_d)$. Then $g_n(\alpha_1, \ldots, \alpha_d)$ is rational and an algebraic integer, hence it is an element of $\mathbb{Z}$. We conclude that, using Fermat's little theorem,

$$\sigma_{np} \equiv \sigma_n^p \equiv \sigma_n \pmod{p}, \quad \text{for all } n \in \mathbb{Z}_{>0}. \tag{6}$$

Using the bounds on p and the assumed upper bound for $\overline{|\alpha|}$, we get

$$\begin{aligned} |\sigma_{np}| &= \left|\alpha_1^{np} + \cdots + \alpha_d^{np}\right| \leq d\overline{|\alpha|}^{np} \leq d\left(1 + \frac{1}{4ed^2}\right)^{np} \leq d\left(1 + \frac{1}{4ed^2}\right)^{4ed^2} \\ &\leq de, \\ |\sigma_n| &= |\alpha_1^n + \cdots + \alpha_d^n| \leq d\overline{|\alpha|}^n \leq d\left(1 + \frac{1}{4ed^2}\right)^n \leq d\left(1 + \frac{1}{4ed^2}\right)^{4ed^2} \leq de. \end{aligned}$$

Hence,

$$|\sigma_{np} - \sigma_n| \leq |\sigma_{np}| + |\sigma_n| \leq 2de < p. \tag{7}$$

Combining (6) and (7) we obtain $\sigma_{np} = \sigma_n$.

We will use the notation of Lemma 2.20. Since for any $n \in \{1, \ldots, d\}$,

$$\Sigma_n(\alpha_1^p, \ldots, \alpha_d^p) = \sigma_{np} = \sigma_n = \Sigma_n(\alpha_1, \ldots, \alpha_d),$$

we conclude by Lemma 2.20 that $S_n(\alpha_1^p, \ldots, \alpha_d^p) = S_n(\alpha_1, \ldots, \alpha_d)$ for all n in $\{0, \ldots, d\}$. Hence,

$$(X - \alpha_1^p) \ldots (X - \alpha_d^p) = (X - \alpha_1) \ldots (X - \alpha_d).$$

This shows that α^p and α are conjugates. Using Lemma 2.21, we conclude that $\alpha = 0$ or α is a root of unity. □

3 Siegel's lemma

In the next chapter, we will use an important lemma in the proof of a lower bound of the Mahler measure for non-zero algebraic integers that are not a

root of unity. This lemma was for the first time formally stated by Siegel [7].

Consider a system of linear equations

$$\begin{array}{ccccccc} a_{11}x_1 & + & \dots & + & a_{1N}x_N & = 0 \\ \vdots & & \vdots & & \vdots & \\ a_{M1}x_1 & + & \dots & + & a_{MN}x_N & = 0, \end{array} \tag{8}$$

where a_{ij} are coefficients ($1 \leq i \leq M,\ 1 \leq j \leq N$) and $x_1, \dots, x_N$ unknowns. For now, assume the coefficients a_{ij} are all rational integers. If $N > M$, then there is a non-trivial solution $(x_1, \dots, x_N) \in \mathbb{Q}^N$ of (8). This also gives an integer solution of this system of equations: multiply the rational solution by the product of the denominators of the entries of the solution. Intuitively, if $N - M$ is large, then there is a non-trivial solution $(x_1, \dots, x_n) \in \mathbb{Z}^N$ for which the value $\max_j |x_j|$ is small, since the dimension of the solution space over $\mathbb{Q}$ is at least $N - M$. However, the minimal value of $\max_j |x_j|$ for non-trivial solutions $(x_1, \dots, x_N) \in \mathbb{Z}^N$ also depends on the coefficients of the linear equations. For instance, if L is an integer, then any non-trivial solution $(x_0, x_1, \dots, x_N) \in \mathbb{Z}^N$ of $x_0 + Lx_1 + \cdots + L^N x_N = 0$ has $\max_j |x_j| \geq |L|$.

Lemma 3.1 (Siegel's lemma)**.** *Let $N > M$ be positive integers and $a_{ij} \in \mathbb{Z}$ for $1 \leq i \leq M,\ 1 \leq j \leq N$. Define $A := \max_{ij} |a_{ij}|$ (with $1 \leq i \leq M,\ 1 \leq j \leq N$). Then there exists a solution $(x_1, \dots, x_N) \in \mathbb{Z}^N \backslash \{0\}$ such that*

$$\max_{1 \leq j \leq N} |x_j| \leq (NA)^{M/(N-M)}.$$

The proof of this lemma makes use of the pigeonhole principle and can be found in [7]. It is an existence theorem: the proof does not give an efficient method of finding such a solution $(x_1, \dots, x_N)$.

We prove an adaptation of Siegel's lemma, where the coefficients are algebraic integers which are not necessarily rational integers. Notice the similarities with the original lemma.

Lemma 3.2 (Siegel's Lemma (modified))**.** *Let $\mathbb{Q} \subset K$ be a finite extension of degree d, and let $a_{ij} \in K$ for $i = 1, \dots, M$ and $j = 1, \dots, N$ be algebraic integers. Assume that for each $i \in \{1, \dots, M\}$ there exists a $j \in \{1, \dots, N\}$ with $a_{ij} \neq 0$. Also suppose $N > dM$. Let $\sigma_1, \dots, \sigma_d$ be the embeddings of K into $\mathbb{C}$. Then (8) has a non-trivial solution $(x_1, \dots, x_N) \in \mathbb{Z}^N$ satisfying*

$$\max_{1 \leq i \leq N} |x_i| \leq \left(2\sqrt{2}N \left(\prod_{i=1}^{M} \prod_{k=1}^{d} \max_j |\sigma_k(a_{ij})| \right)^{1/(dM)} \right)^{dM/(N-dM)}.$$

Remark 3.3. We are given a finite field extension $\mathbb{Q} \subset K$ of degree d, algebraic integers $a_{ij} \in K$ and $N > dM$. Is it clear that (8) has a non-trivial

solution $(x_1, \ldots, x_N) \in \mathbb{Z}^N$ at all? Yes: we can choose a basis of K over $\mathbb{Q}$ and express all coefficients a_{ij} as $\mathbb{Q}$-linear combinations of this basis. Then we get an equivalent system of dM linear homogeneous equations over $\mathbb{Q}$. Since $N > dM$, this system has a non-trivial solution $(x_1, \ldots, x_N) \in \mathbb{Z}^N$. ■

Proof of Lemma 3.2. We will use the pigeonhole principle to establish the existence of a non-trivial tuple $(x_1, \ldots, x_N) \in \mathbb{Z}^N$ such that $\max_j |x_j|$ and

$$\left| \sigma_k\Big(\sum_{j=1}^{N} a_{ij} x_j \Big) \right|$$

are small for all $k \in \{1, \ldots, d\}$ and $i \in \{1, \ldots, M\}$. Then we conclude that $(x_1, \ldots, x_N)$ satisfies (8), by showing

$$\left| N_{K/\mathbb{Q}}\Big(\sum_{j=1}^{N} a_{ij} x_j \Big) \right| < 1$$

for all $i \in \{1, \ldots, M\}$.

Write $d = r_1 + 2r_2$ where r_1 and $2r_2$ are the numbers of real embeddings and complex embeddings respectively. Without loss of generality, assume $\sigma_1, \ldots, \sigma_{r_1}$ are the real embeddings and assume that $\sigma_{r_1+k} = \overline{\sigma}_{r_1+r_2+k}$ for $k = 1, \ldots, r_2$. For $k = 1, \ldots, d$ define

$$\tau_k := \begin{cases} \sigma_k & \text{if } k \le r_1, \\ \operatorname{Re} \sigma_k & \text{if } r_1 < k \le r_1 + r_2, \\ \operatorname{Im} \sigma_k & \text{if } r_1 + r_2 < k \le r_1 + 2r_2. \end{cases}$$

Let $Y > 0$ be an integer, which we will specify later. For any $(y_1, \ldots, y_N)$ in $\{0, \ldots, Y\}^N$ and for $k \in \{1, \ldots, d\}$, $i \in \{1, \ldots, M\}$, the inequalities

$$\left| \tau_k\Big(\sum_{j=1}^{N} a_{ij} y_j \Big) \right| \le NY \max_{1 \le j \le N} |\tau_k(a_{ij})| =: A_{k,i} \tag{9}$$

hold, so $\left| \tau_k(\sum_{j=1}^{N} a_{ij} y_j) \right|$ lies in the interval $[-A_{k,i}, A_{k,i}]$. For all $k \in \{1, \ldots, d\}$, $i \in \{1, \ldots, M\}$, we divide $[-A_{k,i}, A_{k,i}]$ in $n_i > 0$ intervals, each with the same length $2A_{k,i}/n_i$, where n_i is an integer to be specified later. Suppose the following inequality holds:

$$(Y+1)^N > \prod_{i=1}^{M} \prod_{k=1}^{d} n_i = \prod_{i=1}^{M} n_i^d. \tag{10}$$

Then by the pigeonhole principle, there exist $(y_1, \ldots, y_N)$, $(y'_1, \ldots, y'_N)$ in

$\{0,\dots,Y\}$ satisfying

$$\left|\tau_k\Big(\sum_{j=1}^{N} a_{ij}y_j\Big) - \tau_k\Big(\sum_{j=1}^{N} a_{ij}y'_j\Big)\right| \le \frac{2A_{k,i}}{n_i} \quad \text{for all } k\in\{1,\dots,d\}, i\in\{1,\dots,M\}.$$

Take $(x_1,\dots,x_N) := (y_1-y'_1,\dots,y_N-y'_N)\in\{-Y,\dots,Y\}^N$ and consider an $i\in\{1,\dots,M\}$ Notice that

$$\left|\tau_k\Big(\sum_{j=1}^{N} a_{ij}x_j\Big)\right| \le \frac{2A_{k,i}}{n_i} \quad \text{for all } k\in\{1,\dots,d\}, i\in\{1,\dots,M\}.$$

Then for $k=1,\dots,r_1$ we have

$$\left|\sigma_k\Big(\sum_{j=1}^{N} a_{ij}x_j\Big)\right| = \left|\tau_k\Big(\sum_{j=1}^{N} a_{ij}x_j\Big)\right| \le \frac{2A_{k,i}}{n_i} = \frac{2NY\max_{1\le j\le N}|\sigma_k(a_{ij})|}{n_i},$$

while for $k=r_1+1,\dots,r_1+r_2$ we get

$$\begin{aligned}\left|\sigma_k\Big(\sum_{j=1}^{N} a_{ij}x_j\Big)\right| &= \sqrt{\left((\operatorname{Re}\sigma_k)\Big(\sum_{j=1}^{N} a_{ij}x_j\Big)\right)^2 + \left((\operatorname{Im}\sigma_k)\Big(\sum_{j=1}^{N} a_{ij}x_j\Big)\right)^2}\\ &\le \sqrt{\left(\frac{2A_{k,i}}{n_i}\right)^2 + \left(\frac{2A_{k+r_1,i}}{n_i}\right)^2}\\ &\le \sqrt{2\left(\frac{2NY\max_{1\le j\le N}|\sigma_k(a_{ij})|}{n_i}\right)^2}\\ &= \frac{2\sqrt{2}NY\max_{1\le j\le N}|\sigma_k(a_{ij})|}{n_i}.\end{aligned}$$

This leads to

$$\left|\sigma_k\Big(\sum_{j=1}^{N} a_{ij}x_j\Big)\right| \le \frac{2\sqrt{2}NY\max_{1\le j\le N}|\sigma_k(a_{ij})|}{n_i} \quad \text{for } k=1,\dots,d. \tag{11}$$

Again, consider an $i\in\{1,\dots,M\}$. We will choose n_i such that

$$\left|N_{K/\mathbb{Q}}\Big(\sum_{j=1}^{N} a_{ij}x_j\Big)\right| < 1.$$

Then it follows that $\sum_{j=1}^{N} a_{ij}x_j = 0$ since this sum is an algebraic integer, and

thus its norm is a rational integer by Corollary 2.6. By (11), we have

$$\left|N_{K/\mathbb{Q}}\Big(\sum_{j=1}^{N} a_{ij}x_j\Big)\right| = \prod_{k=1}^{d}\left|\sigma_k\Big(\sum_{j=1}^{N} a_{ij}x_j\Big)\right| \le \prod_{k=1}^{d}\frac{2\sqrt{2}NY\max_{1\le j\le N}|\sigma_k(a_{ij})|}{n_i}$$
$$= \left(\frac{2\sqrt{2}NY}{n_i}\prod_{k=1}^{d}\max_{1\le j\le N}|\sigma_k(a_{ij})|^{1/d}\right)^d.$$

So by taking

$$n_i := \left\lfloor 1 + 2\sqrt{2}NY\prod_{k=1}^{d}\max_{1\le j\le N}|\sigma_k(a_{ij})|^{1/d}\right\rfloor,$$

we ensure that $\left|N_{K/\mathbb{Q}}(\sum_{j=1}^{N} a_{ij}x_j)\right| < 1$. Since this norm is a rational integer, we find $\sum_{j=1}^{N} a_{ij}x_j = 0$.

It remains to verify (10). Notice that

$$\prod_{i=1}^{M} n_i^d = \prod_{i=1}^{M}\left\lfloor 1 + 2\sqrt{2}NY\prod_{k=1}^{d}\max_{1\le j\le N}|\sigma_k(a_{ij})|^{1/d}\right\rfloor^d$$
$$\le \prod_{i=1}^{M}\left(1 + 2\sqrt{2}NY\prod_{k=1}^{d}\max_{1\le j\le N}|\sigma_k(a_{ij})|^{1/d}\right)^d$$
$$< \prod_{i=1}^{M}\left(2\sqrt{2}N(Y+1)\prod_{k=1}^{d}\max_{1\le j\le N}|\sigma_k(a_{ij})|^{1/d}\right)^d$$
$$= \Big(2\sqrt{2}N(Y+1)\Big)^{dM}\prod_{i=1}^{M}\prod_{k=1}^{d}\max_{1\le j\le N}|\sigma_k(a_{ij})|,$$

where the strict inequality holds because for all $i \in \{1,\dots,M\}$ there exists an $\ell \in \{1,\dots,N\}$ such that $a_{i\ell} \neq 0$ and thus

$$2\sqrt{2}N\prod_{k=1}^{d}\max_{1\le j\le N}|\sigma_k(a_{ij})|^{1/d} > \left(\prod_{k=1}^{d}|\sigma_k(a_{i\ell})|\right)^{1/d} = \big|N_{K/\mathbb{Q}}(a_{i\ell})\big| \ge 1.$$

So (10) is satisfied if

$$(Y+1)^{N-dM} \ge (2\sqrt{2}N)^{dM}\prod_{i=1}^{M}\prod_{k=1}^{d}\max_{1\le j\le N}|\sigma_k a_{ij}|. \tag{12}$$

Now take

$$Y := \left\lfloor\left((2\sqrt{2}N)^{dM}\prod_{i=1}^{M}\prod_{k=1}^{d}\max_{1\le j\le N}|\sigma_k a_{ij}|\right)^{1/(N-dM)}\right\rfloor$$

and notice that (12) (and thus (10)) is satisfied. These choices of $n_1, \ldots, n_M$ and Y result in a solution $(x_1, \ldots, x_N) \in \{-Y, \ldots, Y\}^N$ of (8) with $\max_j |x_j|$ bounded as desired. □

4 Dobrowolski's Theorem

We prove a slightly weaker version of a theorem of Dobrowolski [5].

Theorem 4.1. *Let α be a non-zero algebraic number of degree $d \geq 2$ that is not a root of unity. Then*

$$M(\alpha) \geq 1 + \frac{1}{11700} \left(\frac{\log \log d}{\log d} \right)^3 .$$

We follow the proof given by Dobrowolski of this theorem. It relies on the construction of a polynomial with small length.

Definition 4.2. The *length* of a polynomial $f = f_0 + f_1 X + \cdots + f_d X^d \in \mathbb{C}[X]$ is defined as

$$\|f\| := |f_0| + |f_1| + \cdots + |f_d| .$$

The idea of the proof of the theorem is constructing a multiple F of a power f_α^M of f_α with $M > 0$ an integer, such that the length $\|F\|$ of F is small. We subsequently choose a prime p for which $N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(F(\alpha^p))$ is non-zero. Then p^{dM} will be a lower bound for the absolute value of this norm, and an upper bound will be obtained in terms of $M(\alpha)$ and $\|F\|$. Comparing the bounds will yield the result.

Remark 4.3. The length $\|\cdot\|$ clearly is a norm on the $\mathbb{C}$-vector space $\mathbb{C}[X]$. Moreover, for $f, g \in \mathbb{C}[X]$ we have $\|fg\| \leq \|f\| \, \|g\|$. Namely, if we write $f = f_0 + \cdots + f_n X^m$, then we have

$$\|fg\| \leq \sum_{i=0}^{m} \|f_i g\| = \sum_{i=0}^{m} |f_i| \, \|g\| = \|f\| \, \|g\| . \qquad \blacksquare$$

The following lemma is a consequence of Lemma 2.18 and plays a key role in the proof of Theorem 4.1: it will eventually provide a lower bound for the quantity $\left| N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(F(\alpha^p)) \right|$.

Lemma 4.4. *Let α be an algebraic integer of degree d and let p be a prime. Then $N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(f_\alpha(\alpha^p))$ is a rational integer divisible by p^d.*

Proof. By Lemma 2.18 there exists $g \in \mathbb{Z}[X]$ such that

$$f_\alpha(X^p) - f_\alpha(X)^p = p g(X).$$

Then we have

$$f_\alpha(\alpha^p) = f_\alpha(\alpha)^p + pg(\alpha) = pg(\alpha).$$

Hence,

$$N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(f_\alpha(\alpha^p)) = N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(pg(\alpha)) = p^d N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(g(\alpha)). \tag{13}$$

$N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(g(\alpha))$ is a rational integer by Corollary 2.6. Now (13) proves the lemma. □

The prime counting function $\pi : \mathbb{R}_{\geq 1} \to \mathbb{Z}$ is defined by $x \mapsto \#\{p \leq x \mid p \text{ is prime}\}$. The following result is stated in [16, Corollary 3].

Lemma 4.5. *$\pi(2x) - \pi(x) > 3x/(5 \log x)$ for all real $x \geq 41/2$.*

Before we give the proof of Theorem 4.1, we finish with three lemmas.

Lemma 4.6. *Let α be an algebraic number of degree d, not a root of unity, and suppose $\deg(\alpha^n) = d$ for all integers $n \geq 1$. Let $F \in \mathbb{Z}[X]$ be a non-zero polynomial of degree N and assume $N/d \geq 13$. Define $x := 3(N/d)\log(N/d)$. Then there exists a prime p such that*

$$F(\alpha^p) \neq 0 \quad \textit{and} \quad x < p \leq 2x.$$

Proof. Lemma 2.21 implies that if n, m are distinct positive integers, then α^n, α^m are not conjugate. Let ζ be the number of primes $p \in (x, 2x]$ such that $F(\alpha^p) = 0$. Then we have $N = \deg F \geq d\zeta$, since $\deg(\alpha^n) = d$ for all integers $n \geq 1$ and because F is non-zero. Hence, $\zeta \leq N/d$, so it suffices to show $\pi(2x) - \pi(x) > N/d$. Write $y := N/d$ and notice that $x \geq 41/2$ since $y \geq 13$. By Lemma 4.5,

$$\pi(2x) - \pi(x) > \frac{3x}{5 \log x} = \frac{9y \log y}{5 \log(3y \log y)} > y = N/d,$$

where the last inequality holds because $y \geq 10$. We find $\pi(2x) - \pi(x) > \zeta$ and this proves the lemma. □

Lemma 4.7. *Let α be an algebraic number of degree d and suppose there exists a positive integer n such that $\deg(\alpha^n) < d$. Then there exists an algebraic number β such that $\deg \beta < d$ and $1 < M(\beta) \leq M(\alpha)$.*

Proof. Let $f \in (\mathbb{Q}(\alpha^n))[X]$ be the monic minimal polynomial of α over the field $\mathbb{Q}(\alpha^n)$ and consider $\beta := f(0) \in \mathbb{Q}(\alpha^n)$. Let ζ_n be a n-th root of unity. Then f divides the polynomial

$$g := X^n - \alpha^n = \prod_{k=1}^{n} (X - \zeta_n^k \alpha)$$

since $g(\alpha) = 0$. So β is the product of $\deg f$ zeroes of g. Therefore, for some integer m we have $\beta = f(0) = \zeta_n^m \alpha^r$ with $r := \deg f = [\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^n)]$. Since

$\beta \in \mathbb{Q}(\alpha^n)$ and $\deg(\alpha^n) < \deg \alpha$, we have $\deg \beta < \deg \alpha$.

Let Σ be the set of embeddings of $\mathbb{Q}(\alpha)$ into $\mathbb{C}$. Notice that $\zeta_n^m \in \mathbb{Q}(\alpha)$, so for all $\sigma \in \Sigma$ we have

$$|\sigma(\beta)| = |\sigma(\zeta_n^m)|\,|\sigma(\alpha^r)| = |\sigma(\alpha)^r| = |\sigma(\alpha)|^r\,. \tag{14}$$

Moreover, all conjugates of β appear exactly $[\mathbb{Q}(\alpha) : \mathbb{Q}(\beta)]$ times in the sequence $(\sigma(\alpha))_{\sigma\in\Sigma}$. Hence,

$$\begin{aligned} M(\beta) &= \left(\prod_{\sigma\in\Sigma} \max\{1, |\sigma(\beta)|\}\right)^{1/[\mathbb{Q}(\alpha):\mathbb{Q}(\beta)]} = \left(\prod_{\sigma\in\Sigma} \max\{1, |\sigma(\alpha)|\}\right)^{r/[\mathbb{Q}(\alpha):\mathbb{Q}(\beta)]} \\ &\le \prod_{\sigma\in\Sigma} \max\{1, |\sigma(\alpha)|\} = M(\alpha), \end{aligned}$$

where we have used

$$r = [\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^n)] \le [\mathbb{Q}(\alpha) : \mathbb{Q}(\beta)].$$

Finally, (14) also shows that $M(\beta) > 1$ since $M(\alpha) > 1$. □

Lemma 4.8. *Let α be an algebraic integer of degree d. Let N, M be positive integers satisfying*

$$M \ge 3, \quad N \ge 10, \quad dM < \tfrac{1}{2}N. \tag{15}$$

Then there exists a non-zero polynomial $F \in \mathbb{Z}[X]$ with $\deg F \le N$, such that α is a zero of F of multiplicity M and

$$\max_{0\le i\le N} |F_i| \le N^{2dM^2/N} M(\alpha)^{2M}. \tag{16}$$

Proof. Let $\sigma_1, \dots, \sigma_d$ be the embeddings of $\mathbb{Q}(\alpha)$ into $\mathbb{C}$. Define $\binom{n}{k} := 0$ for all integers n, k with $k < 0$. Consider the equations in $(F_0, \dots, F_N) \in \mathbb{Z}^N$ given by

$$\sum_{j=0}^{N} \binom{j}{j-i} F_k \alpha^{j-i} = 0, \quad 0 \le i \le M-1. \tag{17}$$

By Lemma 3.2 there exists a non-trivial solution $(F_0, \dots, F_N) \in \mathbb{Z}^N$ of (17) such that

$$\begin{aligned} \max_{0\le i\le N} |F_i| &\le \left(\left(2\sqrt{2}(N+1)\right)^{dM} \left(\prod_{k=1}^{d}\prod_{i=0}^{M-1} \max_{0\le j\le N} \left|\binom{j}{j-i}\sigma_k(\alpha^{j-i})\right|\right)\right)^{1/(N-dM)} \\ &\le \left(\left(2\sqrt{2}(N+1)\right)^{dM} \left(\prod_{k=1}^{d}\prod_{i=0}^{M-1} N^i \max\{1, \sigma_k(\alpha)\}^N\right)\right)^{1/(N-dM)} \\ &\le \left(\left(2\sqrt{2}(N+1)\right)^{dM} N^{dM^2/2} M(\alpha)^{MN}\right)^{1/(N-dM)} \end{aligned} \tag{18}$$

Now consider the polynomial $F = F_0 + F_1 X + \cdots + F_N X^N$. Then α is a zero of F with multiplicity M, since for all integers $i \in \{0, \ldots, M-1\}$, the i-th derivative $F^{(i)}$ of F satisfies

$$F^{(i)}(\alpha) = i! \sum_{j=0}^{N} \binom{j}{j-i} F_k \alpha^{j-i} = 0.$$

By the assumed inequalities involving $M \geq 3$ and $N \geq 10$, we have

$$2\sqrt{2}(N+1) \leq 2\sqrt{2} \cdot \frac{11}{10} N \leq N^{1/2} \cdot N \leq N^{M/2}.$$

Since also $dM \leq \frac{1}{2}N$ by assumption, inequality (18) simplifies to

$$\max_{0 \leq i \leq N} |F_i| \leq \left(N^{dM^2} M(\alpha)^{MN} \right)^{2/N} = N^{2dM^2/N} M(\alpha)^{2M}. \qquad \square$$

Proof of Theorem 4.1. Let α be a non-zero algebraic integer that is not a root of unity and of degree d. First notice that the theorem holds for $d \leq 20$ by Theorem 2.17. Now suppose $d \geq 21$. Consider integers N, M satisfying (15) and $N/d \geq 13$. By Lemma 4.8 there exists a non-zero polynomial $F \in \mathbb{Z}[X]$ with $\deg F \leq N$, such that α is a zero of F of multiplicity M, and such that (16) holds. Suppose $\deg(\alpha^n) = d$ holds for all positive integers n, otherwise we finish the proof by an inductive argument using Lemma 4.7. By Lemma 4.6, there is a prime $p \in (3(N/d)\log(N/d), 6(N/d)\log(N/d)]$ such that $F(\alpha^p) \neq 0$. Write $F = F_0 + \cdots + F_N X^N$. Then we have

$$\begin{aligned} \left| N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(F(\alpha^p)) \right| &= \prod_{k=1}^{d} |F(\sigma_k \alpha^p)| \leq \prod_{k=1}^{d} \|F\| \max\{1, |\sigma_k \alpha|\}^{pN} \\ &\leq \|F\|^d M(\alpha)^{pN}. \end{aligned} \tag{19}$$

On the other hand, we have that f_α^M divides F in $\mathbb{Z}[X]$ since α is a zero of F with multiplicity M and f_α is monic. Thus we can write $f_\alpha^M g = F$ with $g \in \mathbb{Z}[X]$. Then

$$N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(F(\alpha^p)) = N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(f_\alpha(\alpha^p))^M \cdot N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(g(\alpha^p))$$

is a rational integer divisible by p^{dM} by Lemma 4.4. Since $F(\alpha^p) \neq 0$, we conclude that

$$\left| N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(F(\alpha^p)) \right| \geq p^{dM}. \tag{20}$$

From (19) and (20) we get

$$p^{dM} \leq \left| N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(F(\alpha^p)) \right| \leq \|F\|^d M(\alpha)^{pN}. \tag{21}$$

We now use $\|F\| \leq N \cdot \max_{0 \leq i \leq N} |F_i|$ and (16) to give an upper bound for $\|F\|$. Together with (21) this gives

$$p^M \leq \|F\| M(\alpha)^{pN/d} \leq N^{1+2dM^2/N} M(\alpha)^{2M+pN/d}.$$

Hence,

$$\left(2M + \frac{pN}{d}\right) \log M(\alpha) \geq M \log p - \left(1 + \frac{2dM^2}{N}\right) \log N. \tag{22}$$

By (15) we have

$$2M + \frac{pN}{d} = \frac{2dM + pN}{d} \leq \frac{(p+1)N}{d} \leq \frac{3pN}{2d},$$

so (22) gives

$$\log M(\alpha) \geq \frac{2d}{3pN} \left(M \log p - \left(1 + \frac{2dM^2}{N}\right) \log N\right). \tag{23}$$

We take M, N such that they satisfy assumptions (15) and maximize the lower bound

$$\min_{x \in I} \frac{2d}{3xN} \left(M \log x - \left(1 + \frac{2dM^2}{N}\right) \log N\right) \tag{24}$$

for $\log M(\alpha)$, where $I := (3(N/d)\log(N/d), 6(N/d)\log(N/d)]$. We take

$$M := \left\lceil 7 \frac{\log d}{\log\log d} \right\rceil, \quad \text{and} \quad N := dM^2,$$

which turns out in Remark 4.9 to be an almost optimal choice. Notice that the assumptions $N/d \geq 13$ and (15) are satisfied.

We find

$$\left(1 + \frac{2dM^2}{N}\right) \log N = 3(\log d + 2\log M) \leq 9 \log d, \tag{25}$$

where the inequality holds because $d \geq 21$. Moreover, $\log p \geq \log(N/d) = 2\log M$, and this gives

$$M \log p \geq 2M \log M = 14 \log d \left(1 + \frac{\log 7 - \log\log\log d}{\log\log d}\right) \geq 13 \log d. \tag{26}$$

The last inequality can be obtained by substituting $c := 7/\log\log d$ and observing that $c \log c \geq -1/e$ for all $c > 0$. From (23), (25) and (26) we get

$$\begin{aligned} \log M(\alpha) &\geq \frac{2d}{3pN} \cdot \frac{4}{13} M \log p = \frac{8}{39} \cdot \frac{dM}{N} \cdot \frac{\log p}{p} \geq \frac{8}{39} \cdot M^{-1} \cdot \frac{2\log M}{6M^2 \log(M^2)} \\ &= \frac{4}{117M^3} \geq \frac{1}{11700} \left(\frac{\log\log d}{\log d}\right)^3, \end{aligned}$$

where we used $d \geq 21$ for the last inequality. $M(\alpha) \geq 1 + \log M(\alpha)$ completes the proof. □

Remark 4.9. We will use the notation of the proof of Theorem 4.1. From the

lower bound (24) for $\log M(\alpha)$, it is only possible to improve the lower bound

$$\frac{1}{11700}\left(\frac{\log\log d}{\log d}\right)^3$$

for $\log M(\alpha)$ by a constant factor. We will show this. Define

$$\mu(M,N) := \min_{x\in I} \frac{2d}{3xN}\left(M\log x - \left(1+\frac{2dM^2}{N}\right)\log N\right)$$

and assume that M, N are such that

$$\mu(M,N) \geq \left(\frac{\log\log d}{\log d}\right)^3. \tag{27}$$

Also assume that $N > dM$ and $d \geq 3$. From $d \geq 3$ and (27) it follows that $\mu(M,N) \geq 0$. In order to show the bound cannot be much improved, we can make these assumptions.

For functions $f_1(M,N),\ f_2(M,N)$ depending on integers N, M, we will write $f_1(M,N) \gg f_2(M,N)$ if there exists a constant $c > 0$ such that the inequality $f_1(M,N) \leq c f_2(M,N)$ holds for all integers M, N that satisfy assumptions (27) and $N > dM$. Similarly we write $f_1(M,N) \gg f_2(M,N)$ if we have $f_2(M,N) \ll f_1(M,N)$.

We will prove three inequalities:

$$\text{(i)} \qquad \mu(M,N) \ll \frac{d^2M}{N^2}$$

$$\text{(ii)} \qquad M \gg \frac{\log d}{\log\log d}$$

$$\text{(iii)} \qquad \frac{N}{dM} \gg \frac{\log d}{\log\log d}.$$

Assuming these inequalities, we have

$$\mu(M,N) \ll \left(\frac{N}{dM}\right)^{-2} M^{-1} \ll \left(\frac{\log\log d}{\log d}\right)^3,$$

which is what we want to show. Now we prove (i), (ii) and (iii).

(i) Using that $I = [3(N/d)\log(N/d), 6(N/d)\log(N/d)]$, we find

$$\mu(M,N) \leq \min_{x\in I} \frac{dM\log x}{xN} \ll \frac{dM\log(\frac{N}{d}\log\frac{N}{d})}{\frac{N^2}{d}\log\frac{N}{d}} \gg\ll \frac{d^2M}{N^2}.$$

(ii), (iii) From (i) and assumption (27) it follows that

$$\frac{d^2M}{N^2} \gg \mu(M,N) \gg (\log d)^{-3}.$$

Using this and the inequality $N > dM$ shows that

$$\frac{N}{d} \leq \frac{N}{d} \cdot \frac{N}{dM} \ll (\log d)^3.$$

Hence,

$$\log \frac{N}{d} \ll \log \log d.$$

By the non-negativity of $\mu(M, N)$, we now find

$$M \log \log d \gg \left(1 + \frac{2dM^2}{N}\right) \log N \geq \left(1 + \frac{2dM^2}{N}\right) \log d.$$

Hence

$$M \log \log d \gg \log d, \qquad \text{and} \qquad M \log \log d \gg \frac{dM^2 \log d}{N}.$$

These two inequalities prove (ii) and (iii) respectively. ■

Example 4.10. Consider Lehmer's polynomial

$$\mathcal{L} := X^{10} + X^9 - X^7 - X^6 - X^5 - X^4 - X^3 + X + 1.$$

We will follow the proof of Theorem 4.1 and consider the inequalities in (21):

$$p^{dM} \leq \left|N_{\mathbb{Q}/\mathbb{Q}(\alpha)} F(\alpha^p)\right| \leq \|F\|^{dM} (\alpha)^{pN}. \tag{28}$$

Which of the two bounds is the closest to the value of $\left|N_{\mathbb{Q}/\mathbb{Q}(\alpha)} F(\alpha^p)\right|$? We will investigate this.

$\mathcal{L}$ has exactly 8 roots on the unit circle [13]. The other two roots are real. Let α be the real root larger than 1. Then $M(\alpha) \approx 1.176$. It is of degree $d := 10$. As in the proof of Theorem 4.1, we take

$$M := \left\lceil 7 \frac{\log d}{\log \log d} \right\rceil = 20, \quad N := dM^2 = 4000.$$

We search for a polynomial F such that f_α^M divides it, $\deg F \leq N$ and such that

$$\|F\| \leq N^{2dM^2/N} M(\alpha)^{2M}.$$

This is possible by Lemma 4.8. We take $F := (\Phi_6 \mathcal{L})^M$ where $\Phi_6 := X^2 - X + 1$. Then $\|F\| = 1996907431 \approx 1.997 \cdot 10^9$ and this is smaller than

$$N^{2dM^2/N} M(\alpha)^{2M} = 4000^2 M(\alpha)^{40} \approx 1.058 \cdot 10^{10}.$$

The degree of F is 240. We also choose a prime p such that

$$3 \frac{N}{d} \log \frac{N}{d} \leq p \leq 6 \frac{N}{d} \log \frac{N}{d}.$$

Since $(N/d) \log(N/d) \approx 2396.6$, we can take the prime $p := 10007$.

The following upper bound for $\left|N_{\mathbb{Q}(\alpha)/\mathbb{Q}} F(\alpha^p)\right|$ is better than the one given in

(28):

$$\left|N_{\mathbb{Q}(\alpha)/\mathbb{Q}}F(\alpha^p)\right| \leq \|F\|^d\, M(\alpha)^{p\deg(F)} = \|F\|^{dM}\, M(\alpha)^{240p}. \tag{29}$$

Therefore, the upper bound for $\left|N_{\mathbb{Q}(\alpha)/\mathbb{Q}}F(\alpha^p)\right|$ in (28) is not a good approximation of its actual value. This can occur because the polynomial constructed in the proof of Theorem 4.1 with Lemma 3.2, can have a degree smaller than N.

We calculate

$$\begin{aligned} p^{dM} &\approx 1.150217 \cdot 10^{800}, \\ \|F\|^{dM} &\approx 1.166200 \cdot 10^{186}, \\ M(\alpha)^{pN} &\approx 8.091289 \cdot 10^{2822414}, \\ \left|N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(F(\alpha^p))\right| &\approx 2.165338 \cdot 10^{169368}. \end{aligned}$$

We see that the absolute value of the norm is neither close to the lower bound, nor to the upper bound in (28). However, the bound in (29) is much sharper:

$$M(\alpha)^{240p} \approx 7.842979 \cdot 10^{169344}.$$

In general the first inequality in (29) is expected to be quite sharp: if the prime p is large enough, than the modulus of a p-th power of a conjugate of α is either approximately 0, or equal to 1, or very large. If the conjugates of α^p are not unreasonably close to zeroes of F, then $\left|N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(F(\alpha^p))\right|$ is roughly of the order $M(\alpha)^{p\deg(F)}$. ■

5 Polynomials near cyclotomic polynomials

In this chapter, we investigate whether irreducible polynomials with small Mahler measure are close to polynomials with a Mahler measure equal to 1. Furthermore, we will give a lower bound for the Mahler measure of a polynomial in terms of the distance to a product of cyclotomic polynomials. To do this, we introduce self-inversive polynomials.

5.1 Self-inversive polynomials

Definition 5.1. Let $f = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{C}[X]$. Then

$$f^* = \overline{a_n} + \overline{a_{n-1}}X + \cdots + \overline{a_0}X^n$$

is called the *conjugate reciprocal* of f. The polynomial f is called *self-inversive* if there exists a $u \in \mathbb{C}$ such that $|u| = 1$ and $f^* = uf$.

For any $f = a_0 + \cdots + a_nX^n \in \mathbb{C}[X]$ we write $\overline{f} = \overline{a_0} + \cdots + \overline{a_n}X^m$. Notice that for all $f \in \mathbb{C}[X]$ of degree n we have $f^*(X) = X^n\overline{f}(1/X)$.

Remark 5.2. Let $f_1, f_2 \in \mathbb{C}[X]$ be polynomials of degree d_1, d_2 respectively. Then $(f_1 f_2)^* = f_1^* f_2^*$:

$$(f_1 f_2)^* = X^{d_1+d_2}\overline{f_1 f_2}(1/X) = X^{d_1}\overline{f_1}(1/X) \cdot X^{d_2}\overline{f_2}(1/X) = f_1^* f_2^*.$$

We conclude that the product of self-inversive polynomials is again self-inversive: let $u_1, u_2 \in \mathbb{C}$ on the unit circle be such that $f_i^* = u f_i$ for $i = 1, 2$, then we find

$$(f_1 f_2)^* = f_1^* f_2^* = (u_1 u_2) f_1 f_2. \qquad \blacksquare$$

Definition 5.3. A non-zero algebraic number α is called *reciprocal*, if $\alpha,\ \alpha^{-1}$ are conjugates.

Lemma 5.4. *Let α be a non-zero algebraic number. Then α is reciprocal if and only if the primitive mimimal polynomial F_α of α is self-inversive (i.e., $F_\alpha^* = \pm F_\alpha$).*

Proof. If $F_\alpha^* = \pm F_\alpha$, then

$$F_\alpha(\alpha^{-1}) = \pm F_\alpha^*(\alpha^{-1}) = \pm \alpha^d F_\alpha(\alpha) = 0,$$

so indeed α is reciprocal.

Now assume α is reciprocal. We will prove $F_\alpha^* = \pm F_\alpha$. We have

$$F_\alpha^*(\alpha) = \alpha^{-d} F_\alpha(\alpha^{-1}) = 0,$$

so there exists a non-zero $x \in \mathbb{Q}$ such that $F_\alpha^* = x F_\alpha$. Write $x = a/b$ with $a, b \in \mathbb{Z}$ coprime and b non-zero. Then $b F_\alpha^* = a F_\alpha$. By definition of F_α, there is no common divisor $d \in \mathbb{Z}$ with $|d| > 1$ of all coefficients of F_α. Hence, $|a| = |b| = 1$ and we find $x \in \{\pm 1\}$. $\square$

Remark 5.5. All reciprocal algebraic units except ± 1 are of even degree. To show this, suppose α is a non-zero algebraic unit which is reciprocal and of odd degree $2n+1$. By the previous lemma, the monic minimal polynomial f_α of α satisfies $f_\alpha = \pm f_\alpha^*$. Notice that

$$f_\alpha^*(-1) = (-1)^{2n+1} f_\alpha(1/(-1)) = -f_\alpha(-1) \quad \text{and} \quad f_\alpha^*(1) = f_\alpha(1).$$

So if $f_\alpha = f_\alpha^*$, we find $2 f_\alpha(-1) = f_\alpha(-1) + f_\alpha^*(-1) = 0$. In this case, we thus have $\alpha = -1$ and $f_\alpha = X + 1$. Similarly, if $f_\alpha = -f_\alpha^*$, we find $f_\alpha(1) = 0$ and thus $\alpha = 1,\ f_\alpha = X - 1$.

In addition, this argument shows that for all non-zero reciprocal algebraic units $\alpha \neq 1$, we have $f_\alpha = f_\alpha^*$ (this does not depend on the parity of the degree). $\blacksquare$

Corollary 5.6. *Let α be reciprocal and $\|F_\alpha\| \leq 4$. Then α is a root of unity.*

Proof. By Lemma 5.4 we have $F_\alpha^* = \pm F_\alpha$. By Remark 5.5 we can assume $\deg F_\alpha = 2n$ for some positive integer n. Clearly, $\|F_\alpha\| \geq 2$. If $\|F_\alpha\| = 2$, we find $F_\alpha = X^{2n} \pm 1$, and then α is a $2n$-th or $4n$-th root of unity. If $\|F_\alpha\| = 3$,

we find $F_\alpha = X^{2n} \pm X^n + 1$, and this implies α is a $3n$-th or $6n$-th root of unity. If $\|F_\alpha\| = 4$, then there exist $\varepsilon_1, \varepsilon_2 \in \{\pm 1\}$ such that

$$F_\alpha = X^{2n} + \varepsilon_1\varepsilon_2 X^{n+m} + \varepsilon_1 X^{n-m} + \varepsilon_2.$$

But this gives $F_\alpha = (X^{n+m} + \varepsilon_1)(X^{n-m} + \varepsilon_1\varepsilon_2)$, which is reducible. Hence, $\|F_\alpha\| = 4$ cannot occur at all. □

5.2 Polynomials near cyclotomic polynomials

We will investigate whether for monic irreducible polynomials $f \in \mathbb{Z}[X]$ with small Mahler measure there exists a $g \in \mathbb{Z}[X]$ such that $M(g) = 1$ and $\|f - g\|$ is small. We will denote the n-th cyclotomic polynomial by Φ_n for all positive integers n.

Example 5.7. Consider Lehmer's polynomial

$$\mathcal{L} := X^{10} + X^9 - X^7 - X^6 - X^5 - X^4 - X^3 + X + 1.$$

We find that $M(\mathcal{L} + X^5) = 1$. In fact,

$$\mathcal{L} = \Phi_1^2\Phi_2^2\Phi_3^2\Phi_6 - X^5.$$

Since $M(\mathcal{L} - X^5) \approx 1.845$ we find that $\mathcal{L} - X^5$ is not the product of cyclotomic polynomials. ■

Remark 5.8. For monic irreducible polynomials $f \in \mathbb{Z}[X]$ with small Mahler measure yet greater than 1, and of even degree $2n$, often exactly one of the polynomials $f \pm X^n$ is the product of cyclotomic polynomials. However, this is not always the case, as we will show. We will consider monic irreducible polynomials with the smallest known Mahler measures. If $f \in \mathbb{Z}[X]$ is of degree $2n$ and reciprocal and $f = a_0 + a_1X + \cdots + a_{2n}X^{2n}$, then we denote its coefficients by $[a_0, \ldots, a_n]$. For a non-zero polynomial $f \in \mathbb{Z}[X]$, we write $\nu(f) := \#\{z \in \mathbb{C} \mid |z| > 1,\ f(z) = 0\}$ for the number of roots of f outside the unit disk.

For a polynomial $f \in \mathbb{Z}[X]$, we define

$$\begin{aligned}\mathrm{CyclDist}(f) &:= \min\{\|f - g\| \mid g \in \mathbb{Z}[X]\backslash\{0\},\ M(g) = 1\},\\ \mathrm{CyclDist}^*(f) &:= \min\{\|f - g\| \mid g \in \mathbb{Z}[X]\backslash\{0\},\ M(g) = 1,\ \deg g = \deg f\}.\end{aligned}$$

$\mathrm{CyclDist}(f) = 1$ does not hold for all monic irreducible polynomials f with integer coefficients, despite the results in Table 1. For example, f given by

$$[1, 2, 2, 2, 1, 0, -1, -2, -2, -1, 0, 1, 1, 1, 1, 1]$$

gives $\mathrm{CyclDist}(f) = 7$. Its Mahler measure is approximately $M(f) \approx 1.285$.

We use a list of Mossinghoff in [13]: it contains all polynomials $f \in \mathbb{Z}[X]$ with $1 < M(f) < 1.30$ and $\deg f \leq 44$. For computational reasons, we do not compute CyclDist but $\mathrm{CyclDist}^*$ for polynomials. A scatter plot of $\mathrm{CyclDist}^*$

coefficients f	$2n$	$M(f)$	$\nu(f)$	cycl. prod.
$[1,1,0,-1,-1,-1]$	10	1.176	1	$f+X^5$
$[1,1,1,1,0,0,-1,-1,-1,-1]$	18	1.188	1	$f-X^9$
$[1,0,0,1,-1,0,0,-1]$	14	1.200	1	$f-X^7$
$[1,1,1,0,0,-1,0,-1,0,-1]$	18	1.201	2	none
$[1,0,-1,0,0,0,0,1]$	14	1.202	1	$f-X^7$
$[1,0,1,0,0,1,-1,1,0,0,1,-1]$	22	1.205	2	none
$[1,1,1,1,0,0,0,-1,-1,-1,-1,0,0,0,1]$	28	1.208	2	$f-X^{14}$
$[1,1,0,0,1,1,0,-1,-1,-1,-1]$	20	1.213	2	none
$[1,1,1,1,1,0,-1,-1,-1,-1,-1]$	20	1.215	2	$f-X^{10}$
$[1,0,0,0,-1,1]$	10	1.216	1	$f-X^5$

Table 1: the ten monic irreducible polynomials with the smallest known Mahler measures [13]. For such a polynomial f of even degree $2n$, the table shows which of the polynomials $f \pm X^n$ is the product of cyclotomic polynomials. The Mahler measures are rounded.

of the non-zero polynomials $f \in \mathbb{Z}[X]$ with

$$1 < M(f) < 1.30, \quad \deg f \le 32, \quad \nu(f) = 1$$

is given in Figure 2.

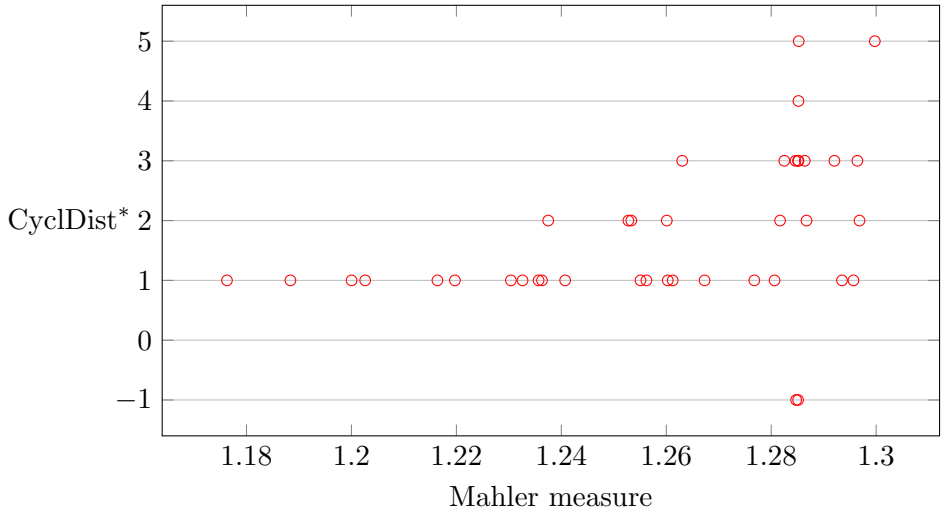

Figure 2: For all monic irreducible polynomials $f \in \mathbb{Z}[X]$ with $M(f) < 1.30$, $\nu(f) = 1$ and $\deg f \le 32$, we calculated $\mathrm{CyclDist}^*(f)$ if $\mathrm{CyclDist}^*(f) \le 6$. If $\mathrm{CyclDist}^*(f) > 6$, then -1 is plotted.

We see that not for all monic irreducible polynomials $f \in \mathbb{Z}[X]$ with $\nu(f) = 1$ we have $\mathrm{CyclDist}(f) = 1$. However, it appears that of these polynomials the ones with small Mahler measures also have a small value for $\mathrm{CyclDist}^*$. In Figure 3 the requirement $\nu(f) = 1$ of the polynomials f is dropped. In

this figure the polynomials with small Mahler measure also tend to have a smaller value for CyclDist*. These results seem to indicate that polynomials with small Mahler measure and integer coefficients are close to products of cyclotomic polynomials. In Figure 3, it also appears that CyclDist* tends to be odd.

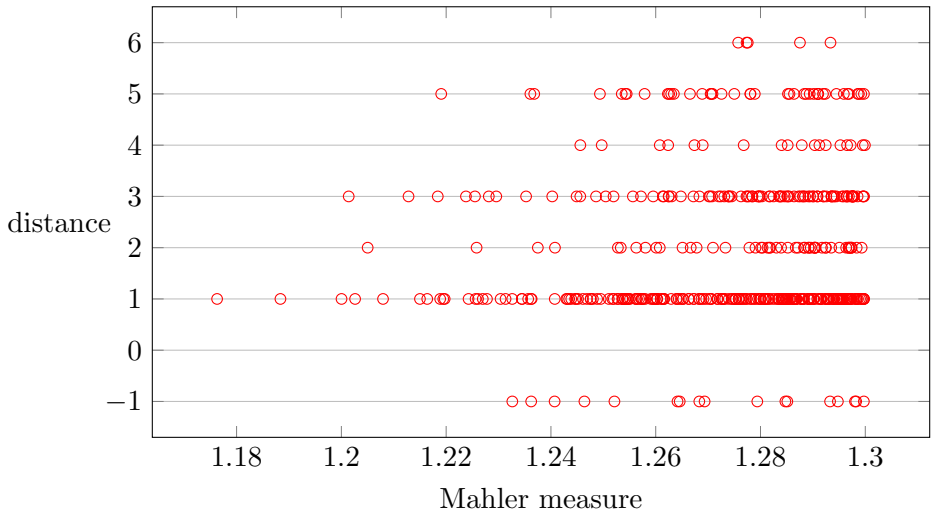

Figure 3: For all monic irreducible polynomials $f \in \mathbb{Z}[X]$ with $1 < M(f) < 1.30$ and $\deg f \leq 32$, we calculated CyclDist$^*(f)$ if CyclDist$^*(f) \leq 6$. If CyclDist$^*(f) > 6$, then -1 is plotted.

■

Conversely, it might also be interesting to investigate the following. If $M(g)$ equals 1 for some monic polynomial $g \in \mathbb{Z}[X]$, then what is the Mahler measure of polynomials $f \in \mathbb{Z}[X]$ with $\|f - g\| = 1$? If we consider $g = \Phi_{5p}$ for primes $p \neq 5$ and denote its degree by $d := 4(p-1)$, then it appears that $M(\Phi_{5p} - X^{d/2})$ is not very large: see Table 2.

p	7	11	13	17	19	23	29	31
$M(\Phi_{5p} - X^{2(p-1)})$	1.29	1.31	1.29	1.30	1.29	1.30	1.29	1.29

Table 2: The approximated Mahler measure of $M(\Phi_{5p} - X^{2(p-1)})$ for some prime numbers p.

5.3 A lower bound for the Mahler measure

We will now prove a Proposition which gives a lower bound for the Mahler measure of certain polynomials close to products of cyclotomic polynomials. First, we prove a few lemmas. For all positive integers n, let $\omega(n)$ denote the number of distinct prime divisors of n. An integer n is called squarefree if

$p^2 \nmid n$ for all primes p. Let $\mu : \mathbb{Z}_{>0} \to \mathbb{Z}$ be the Möbius-function:

$$\mu(n) = \begin{cases} (-1)^{\omega(n)} & \text{if } n \text{ is squarefree} \\ 0 & \text{if } n \text{ is not squarefree.} \end{cases}$$

By applying the Möbius inversion formula [6, Theorem 266] to the identity

$$X^n - 1 = \prod_{d|n} \Phi_d$$

we obtain

$$\Phi_n = \prod_{d|n} \left(X^{n/d} - 1\right)^{\mu(d)}. \tag{30}$$

for all integers $n > 0$.

Lemma 5.9. *Let n be a positive integer. Then there exists a product of cyclotomic polynomials $h \in \mathbb{Z}[X]\backslash\{0\}$ such that*

$$\|h\Phi_n\| \leq 2^{2^{\omega(n)-1}}, \quad \|h\| \leq 2^{2^{\omega(n)-1}} \quad \textit{and} \quad \deg h \leq n2^{\omega(n)-2}.$$

Proof. We take h to be equal to the denominator of the right hand side of (30):

$$h := \prod_{\substack{d|n \\ \mu(d)=-1}} \left(X^{n/d} - 1\right)^{-\mu(d)}.$$

All roots of h are roots of unity, so h is a product of cyclotomic polynomials. By (30) this choice of h gives

$$h\Phi_n = \prod_{\substack{d|n \\ \mu(d)=1}} \left(X^{n/d} - 1\right)^{\mu(d)}.$$

Notice that there is a bijection between the subsets of $\{1, \ldots, \omega(n)\}$ of even cardinality and the subsets of $\{1, \ldots, \omega(n)\}$ of odd cardinality: send any subset S of even cardinality to $\{1\} \cup S$ if it did not contain S, and otherwise send it to $S\backslash\{1\}$. Since there are $2^{\omega(n)}$ subsets in total, the number of odd subsets equals $2^{\omega(n)-1}$ and this equals also the number of even subsets. The number of positive divisors $d \mid n$ with $\mu(d) = -1$ equals the number of subsets of $\{1, \ldots, \omega(n)\}$ of odd cardinality, and thus it equals $2^{\omega(n)-1}$. We conclude that

$$\|h\| \leq 2^{2^{\omega(n)-1}}.$$

Similarly, we also have

$$\|h\Phi_n\| \leq 2^{2^{\omega(n)-1}}.$$

Finally, we notice that the degree of h satisfies

$$\deg h = \sum_{\substack{d|n \\ \mu(d)=-1}} \frac{n}{d} \leq \sum_{\substack{d|n \\ \mu(d)=-1}} \frac{n}{2} = \frac{n}{2} \cdot 2^{\omega(n)-1} = n2^{\omega(n)-2}. \qquad \square$$

Lemma 5.10. *Let $f, g \in \mathbb{C}[X]$ be polynomials and suppose that g is self-inversive and that $\deg g > 2 \deg f$. Then $\|f - g\| \geq \|f\|$.*

Proof. Define $m := \deg f$ and $n := \deg g$ and write $g = g_0 + \cdots + g_n X^n$. Let $g_1 := g_0 + \cdots + g_m X^m$ and $g_2 := g_{n-m} X^{n-m} + \cdots + g_n X^n$. Since $\deg g > 2 \deg f$, we have $\|g - f\| \geq \|g_1 - f\| + \|g_2\|$. Moreover, because g is self-inversive we find $\|g_2\| = \|g_1\|$. Hence, using the triangle inequality, we conclude that

$$\|f\| = \|f - g_1\| + \|g_1\| = \|g_1 - f\| + \|g_2\| \leq \|g - f\|. \qquad \square$$

Let $\varphi : \mathbb{Z}_{\geq 1} \to \mathbb{Z}_{\geq 1}$ defined by $n \mapsto \#(\mathbb{Z}/n\mathbb{Z})^\times$ be the Euler totient function.

Proposition 5.11. *Let $n_1, \ldots, n_k$ be positive integers and let α be a non-zero algebraic integer that is not a root of unity. Define*

$$D := \|f_\alpha - \Phi_{n_1} \ldots \Phi_{n_k}\| \quad \text{and} \quad s := 2^{\omega(n_1)} + \cdots + 2^{\omega(n_k)}.$$

Suppose $D < \|f_\alpha\|$. Then

$$M(\alpha) \geq 1 + \frac{\log 2}{\left(1 + \frac{1}{2}s^2\right) 2^{1+s/2}(D+1)}.$$

Proof. Write $d := \deg \alpha$. By Lemma 5.9 there exists products of cyclotomic polynomials $h_1, \ldots, h_k \in \mathbb{Z}[X]$ such that

$$\|h_i \Phi_{n_i}\| \leq 2^{2^{\omega(n_i)-1}}, \quad \|h_i\| \leq 2^{2^{\omega(n_i)-1}}, \quad \deg h_i \leq n_i 2^{\omega(n_i)-2}$$

for all $1 \leq i \leq k$. Define $h := h_1 \ldots h_k$. Then we have

$$\|h\Phi_{n_1} \ldots \Phi_{n_1}\| \leq \prod_{i=1}^{k} \|h_i \Phi_{n_i}\| \leq 2^{s/2}, \tag{31}$$

$$\|h\| \leq \prod_{i=1}^{k} \|h_i\| \leq 2^{s/2}. \tag{32}$$

Define $F := hf_\alpha$. From (32) and (31) we find

$$\begin{aligned} \|F\| &= \|h\Phi_{n_1} \ldots \Phi_{n_k} + h(f_\alpha - \Phi_{n_1} \ldots \Phi_{n_k})\| \\ &\leq \|h\Phi_{n_1} \ldots \Phi_{n_k}\| + \|h\| \, \|f_\alpha - \Phi_{n_1} \ldots \Phi_{n_k}\| \\ &\leq 2^{s/2}(D+1). \end{aligned} \tag{33}$$

Consider a prime p. Since α is not a root of unity, neither is α^p, and thus we find $h(\alpha^p) \neq 0$. Moreover, by Lemma 2.21 we have $f_\alpha(\alpha^p) \neq 0$. Hence,

$F(\alpha^p) \neq 0$. Lemma 4.4 now gives

$$\left|N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(F(\alpha^p))\right| \geq p^d, \tag{34}$$

and by equation (33) we also have

$$\left|N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(F(\alpha^p))\right| \leq \left(2^{s/2}(D+1)\right)^d M(\alpha)^{p\deg(F)}. \tag{35}$$

Write $N := \deg F$. By (34) and (35) we have

$$M(\alpha) \geq \left(\frac{p}{2^{s/2}(D+1)}\right)^{d/(pN)}. \tag{36}$$

By Bertrand's postulate (Lemma 2.19) there exists a prime p such that

$$2 \cdot 2^{s/2}(D+1) \leq p \leq 4 \cdot 2^{s/2}(D+1).$$

Now let p satisfy these inequalities. Then we find by (36) (and since the function $[2,4] \to \mathbb{R},\ x \mapsto x^{1/x}$ attains its global minima in 2 and in 4),

$$\log M(\alpha) \geq \frac{d \log 2}{2^{1+s/2}(D+1)N}. \tag{37}$$

We will now give an upper bound for $N = \deg F$. For any positive integer n we have (where p ranges over the prime numbers):

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right) \geq n 2^{-\omega(n)}. \tag{38}$$

Let $j \in \{1, \ldots, k\}$ be such that $\omega(n_j)$ is maximal among $\omega(n_1), \ldots, \omega(n_k)$. Then we have

$$\deg h = \sum_{i=1}^{k} \deg h_i \leq \sum_{i=1}^{k} n_i 2^{\omega(n_i)-2} \leq \sum_{i=1}^{k} \varphi(n_i) 2^{2\omega(n_i)-2} \leq 2^{2\omega(n_j)-2} \sum_{i=1}^{k} \varphi(n_i), \tag{39}$$

where the second inequality holds by (38). By Lemma 5.4 and Remark 5.2 we find that $\Phi_{n_1} \ldots \Phi_{n_k}$ is self-inversive. Since also $D < \|f_\alpha\|$, we have by Lemma 5.10,

$$\varphi(n_1) + \cdots + \varphi(n_k) = \deg(\Phi_{n_1} \ldots \Phi_{n_k}) \leq 2 \cdot \deg f_\alpha = 2d.$$

So from (39) we get

$$\deg h \leq 2^{2\omega(n_j)-2} \sum_{i=1}^{k} \varphi(n_i) \leq 2^{2\omega(n_j)-1} d.$$

Hence,

$$N = \deg F = \deg h + \deg f_\alpha \leq \left(2^{2\omega(n_j)-1} + 1\right) d \leq \left(\tfrac{1}{2}s^2 + 1\right) d. \tag{40}$$

We conclude by (37) and (40) that

$$\log M(\alpha) \geq \frac{\log 2}{\left(1+\frac{1}{2}s^2\right) 2^{1+s/2}(D+1)}. \qquad \square$$

We examine a specific case of the previous proposition, namely $k = 1$ and $\omega(n_1) \leq 2$.

Corollary 5.12. *Let α be a non-zero reciprocal algebraic integer and not a root of unity. Let $n \in \mathbb{Z}_{>0}$ be such that $\omega(n) \leq 2$. Suppose that*

$$\|f_\alpha - \Phi_n\| \leq 4.$$

Then $M(\alpha) \geq 1.0019$. If n is prime, then $M(\alpha) \geq 1.0115$.

Proof. Let $D := 4$. By Corollary 5.6 we have $D < \|f_\alpha\|$. The result now follows from Proposition 5.11 with $s = 4$ if $\omega(n) = 2$ and $s = 2$ if $\omega(n) = 1$. $\square$

References

[1] F. Amoroso and S. David. Le problème de Lehmer en dimension supérieure. *J. Reine Angew. Math.*, pages 145–179, 1999.

[2] P. Borwein, E. Dobrowolski, and M. J. Mossinghoff. Lehmer's problem for polynomials with odd coefficients. *Ann. of Math.*, 166:347–366, 2007.

[3] D Cantor and E Straus. On a conjecture of D. H. Lehmer. *Acta Arith.*, 42:97–100, 1982. Correction: 42:327, 1983.

[4] E. Dobrowolski. On the maximal modulus of conjugates of an algebraic integer. *Bull. Acad. Polon. Sci.*, 26:291–292, 1978.

[5] E. Dobrowolski. On a question of Lehmer and the number of irreducible factors of a polynomial. *Acta Arith.*, 34:391–401, 1979.

[6] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers.* Oxford University Press, 4 edition, 1979.

[7] M. Hindry and J. H. Silverman. *Diophantine Geometry: An Introduction*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, 1 edition, 2000.

[8] L. Kronecker. Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten. *J. Reine Angew. Math.*, 53:176–181, 1857.

[9] S. Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, 2013.

[10] D. H. Lehmer. Factorization of certain cyclotomic functions. *Ann. of Math.*, 34:461–479, 1933.

[11] R. Louboutin. Sur la mesure de Mahler d'un nombre algébrique. *C. R. Acad. Sci. Paris*, 296:707–708, 1983.

[12] K. Mahler. On some inequalities for polynomials in several variables. *J. London Math. Soc.*, 37:341–344, 1962.

[13] M. J. Mossinghoff. Mahler measure records. http://www.cecm.sfu.ca/mjm/Lehmer/records/, 2009. [Online; accessed 09-June-2016].

[14] D. G. Northcott. An inequality in the theory of arithmetic on algebraic varieties. *Proc. Camb. Philos. Soc.*, 45:502–509, 1949.

[15] T. A. Pierce. The numerical factors of the arithmetic forms $\prod_{i=1}^{n}(1-\alpha_i)$. *Ann. of Math.*, 18:53–64, 1916.

[16] B. J. Rosser and L. Schoenfeld. Approximate formulas for some functions of prime numbers. *Illinois J. of Math.*, 6:64–94, 1962.

[17] A. Schinzel and H. Zassenhaus. A refinement of two theorems of Kronecker. *Michigan Math. J.*, 12:81–85, 1965.

[18] R. Séroul. *Programming for mathematicians*. Springer-Verlag, 2012.

[19] C. Smyth. The Mahler measure of algebraic numbers: a survey. *LMS Lecture Note Series*, 352:322–349, 2008.

[20] C.J. Smyth. On the product of the conjugates outside the unit circle of an algebraic integer. *Bull. London Math. Soc.*, 3:169–175, 1971.

[21] P. Voutier. An effective lower bound for the height of algebraic numbers. *Acta Arith.*, 74:81–95, 1996.