

MAHLER MEASURES CLOSE TO AN INTEGER

Artūras Dubickas

Abstract. We prove that the Mahler measure of an algebraic number cannot be too close to an integer, unless we have equality. The examples of certain Pisot numbers show that the respective inequality is sharp up to a constant. All cases when the measure is equal to the integer are described in terms of the minimal polynomials.

1 Introduction

Let α be an algebraic number of degree d with minimal polynomial

$$a_d z^d + \dots + a_1 z + a_0 \in \mathbb{Z}[z],$$

and conjugates $\alpha_1, \alpha_2, \dots, \alpha_d$ (with α one of these) labelled so that

$$|\alpha_1| \geq |\alpha_2| \geq \dots \geq |\alpha_k| > 1 \geq |\alpha_{k+1}| \geq \dots \geq |\alpha_d|.$$

Here, $k \in \{0, 1, 2, \dots, d\}$ with $k = 0$ if the house of α , namely $\overline{|\alpha|} = \max_{1 \leq j \leq d} |\alpha_j|$, is less than or equal to 1. Which values can the Mahler measure of α ,

$$M(\alpha) = a_d \prod_{j=1}^k |\alpha_j|,$$

take? Clearly,

$$\beta = M(\alpha) = \pm a_d \alpha_1 \alpha_2 \dots \alpha_k$$

is a real algebraic integer greater than or equal to 1. By Kronecker's theorem [12], $\beta = 1$ if and only if α is a root of unity. Lehmer [13] asked whether β is bounded away from 1 if α is not a root of unity.

Theorem A (d'après Boyd [4]). *If $\beta = M(\alpha)$ then every conjugate of β (other than β itself) either lies in the annulus $\beta^{-1} < |z| < \beta$ or is equal to $\pm\beta^{-1}$.*

In Boyd's theorem [4] there is an additional requirement for α to be an algebraic integer, but his proof remains the same for an arbitrary algebraic number.

Proof Let θ be an automorphism of a suitable normal extension of \mathbb{Q} containing all conjugates of α (and so those of β) which maps $\beta \rightarrow \beta'$. Then

$$\beta' = \theta(\beta) = \theta(\pm a_d \alpha_1 \dots \alpha_k) = \pm a_d \alpha'_1 \dots \alpha'_k.$$

AMS subject classification: Primary: 11R04, 11R06; secondary: 11R09, 11J68.

Keywords: Mahler measure, PV numbers, Salem numbers.

The modulus of the right-hand side in the above equality is strictly less than β , because the sets $\{\alpha'_1, \dots, \alpha'_k\}$ and $\{\alpha_1, \dots, \alpha_k\}$ are distinct. Thus, $|\beta'| \geq \beta$. This part of the theorem was also proved by Adler and Marcus [1].

On the other hand, we have

$$|\beta'| = a_d |\alpha'_1 \dots \alpha'_k| = \left| \frac{a_d a_0}{a_d \alpha'_{k+1} \dots \alpha'_d} \right| \geq \frac{a_d |a_0|}{M(\alpha)} \geq \beta^{-1}.$$

The inequalities are equalities if $\{\alpha'_{k+1}, \dots, \alpha'_d\} = \{\alpha_1, \dots, \alpha_k\}$ and $a_d = |a_0| = 1$. Thus, there is no more than one β' on the circle $|z| = \beta^{-1}$. Furthermore, if there is just one then it is real. The proof of Theorem A is now completed. ■

Except for Theorem A, which gives necessary, but not sufficient condition on a number to be a measure, not too much is known about the set of measures $\beta = M(\alpha)$. The exception here are the lower bounds on $M(\alpha)$, where α is a non-cyclotomic, in terms of d (see e.g. the older reviews of Boyd [3], Waldschmidt [22], and the new books of Everest and Ward [11] and of Waldschmidt [23] for such and some other results). In addition to these, Boyd [5] showed that $\beta = M(\alpha)$ can be non-reciprocal for reciprocal α . For example, if α is a root of $z^6 + z^5 + 2z^4 + 3z^3 + 2z^2 + z + 1$ then $\beta = M(\alpha)$ is non-reciprocal, as it has minimal polynomial $z^3 - z^2 - z - 1$.

In Sections 2 and 3, we investigate how close $M(\alpha)$ can be to a real algebraic number $\gamma \geq 1$. The straightforward estimates on the resultant give sharp bounds for the distance between the integer and the measure. In our final Section 4, we give some examples where for quadratic numbers γ the equation $M(\alpha) = \gamma$ has some unexpected solutions (in α).

2 Results

Let α be an algebraic number of degree d . Suppose $\beta = M(\alpha)$ is of degree D , and let γ be an algebraic number of degree n with c_n as the leading coefficient of its minimal polynomial. Set

$$r(\gamma) = \log(2^n c_n |\gamma|^n).$$

With this notation, we can give our first statement.

Theorem 1 *For any real algebraic number $\gamma \geq 1$ and any algebraic number α , we have $M(\alpha) = \gamma$ or*

$$\log |M(\alpha) - \gamma| > -Dr(\gamma).$$

Taking $\gamma = 1$, and using the bound $D < 2^d$, Theorem 1 gives only the weak lower bound $M(\alpha) > 1 + 2^{-2^d}$ in Lehmer's problem. For Salem numbers, we have $D = d$, and so this gives a stronger bound $\alpha > 1 + 2^{-d}$, which is still very weak compared to the best known logarithmic bounds [7], [14], [21]. Recall that a Salem number is a reciprocal algebraic integer $\sigma > 1$ such that its conjugates, except for two, namely σ

itself and $1/\sigma$, are all on the unit circle $|z| = 1$. For other integers $\gamma = m$, where $m \in \{2, 3, \dots\}$, we have the following statement, elucidating the equality $M(\alpha) = m$.

Theorem 2 Suppose $m \geq 2$ is a positive integer, and let α be an algebraic number such that $M(\alpha)$ is of degree D . Then either $M(\alpha) = m$, and so one of the following is true:

- (i) the extreme coefficients of the minimal polynomial of α are m and $\pm m$, and its roots are all on $|z| = 1$;
- (ii) the extreme coefficients of the minimal polynomial of α are q (where q is one of the numbers $1, 2, \dots, m-1$) and $\pm m$, and its roots are all in $|z| > 1$;
- (iii) α^{-1} is as in (ii),

or we have the inequality $\log|M(\alpha) - m| > -D \log(2m)$.

The inequality of Theorem 2 is sharp up to a constant. To show this, we first recall an old result of Perron [16].

Theorem B The integer polynomial $f(z) = z^d + a_{d-1}z^{d-1} + \dots + a_1z + a_0$, $a_0 \neq 0$, is irreducible if $|a_{d-1}| > 1 + |a_{d-2}| + \dots + |a_1| + |a_0|$.

In modern terms, one can easily show that this is the case, since $f(z)$ defines a \pm Pisot number. Recall that an algebraic integer $\sigma > 1$ is a Pisot number if its remaining conjugates (if any) are all strictly inside the unit circle.

Proof On the unit circle $|z| = 1$ we have $|z^d + a_{d-2}z^{d-2} + \dots + a_1z + a_0| < |-a_{d-1}z^{d-1}|$. By Rouché's Theorem, $f(z)$ has $d-1$ zeros strictly inside the unit circle $|z| < 1$. As the product of all roots is equal to $(-1)^d a_0$, the remaining root is outside the unit circle $|z| > 1$, and is, therefore, real. Thus, $f(z)$ is irreducible for otherwise it has a monic integral factor all of whose roots lie inside the unit circle, which is impossible. ■

Selmer [17] noted that Perron's result of 1907 can sometimes be extended if in Theorem B we have equality. If, for instance, $a_{d-1} = 1 + a_{d-2} + \dots + a_1 + a_0$ then $f(z)/(z-1)$ is irreducible.

Set

$$P(d, m; z) = z^d - (m-1)(z^{d-1} + z^{d-2} \dots + z + 1).$$

We proved in [9] that among all integer polynomials of height at most m and of degree at most d the polynomial $P(d, m+1; z)$ has a root closest to an integer. We now show that $P(d, m; z)$ is also irreducible and defines a Pisot number. Because $P(d, m; z)(z-1) = z^{d+1} - mz^d + m-1$, we will deduce the irreducibility as in Theorem B.

Theorem 3 For every pair of integers d, m , where $d, m \geq 2$, the polynomial $P(d, m; z)$ is irreducible and defines a Pisot number $\sigma(d, m)$ such that

$$m - \frac{m-1}{m^{d-1}} < \sigma(d, m) < m - \frac{m-1}{m^d}.$$

Note that for $\sigma = \sigma(d, m)$ we have $M(\sigma) = \sigma$ and $D = d$. Thus, by Theorem 3, the lower bound $-D \log(2m)$ in Theorem 2 cannot be replaced by $-(D - 2) \log m$.

3 Proofs

Proof of Theorem 1 The resultant of $\beta = M(\alpha)$ and γ ,

$$R(\beta, \gamma) = c_n^D \prod (\beta_u - \gamma_v),$$

where the product is taken over every pair (u, v) with $1 \leq u \leq D$, $1 \leq v \leq n$, is at least 1 in absolute value if $\beta \neq \gamma$. Every term in the product is bounded above, by Theorem A, as follows:

$$|\beta_u - \gamma_v| \leq |\beta_u| + |\gamma_v| \leq \beta + \overline{|\gamma|}.$$

Using this bound for all but one pair (u, v) , we obtain the inequality

$$1 \leq |\beta - \gamma| c_n^D (\beta + \overline{|\gamma|})^{Dn-1}.$$

In case $\beta \leq \overline{|\gamma|}$ the right-hand side here is less than $|\beta - \gamma| \exp\{Dr(\gamma)\}$, and Theorem 1 follows immediately.

Assume $\overline{|\gamma|} < \beta$ and $|\beta - \gamma| \leq \exp\{-Dr(\gamma)\}$. It follows that

$$\beta \leq |\gamma| + \exp\{-Dr(\gamma)\} \leq \overline{|\gamma|} + \exp\{-Dr(\gamma)\}.$$

Then

$$1 \leq \exp\{-Dr(\gamma)\} c_n^D (2\overline{|\gamma|} + \exp\{-Dr(\gamma)\})^{Dn-1} = \frac{1}{2\overline{|\gamma|}} \left(1 + \frac{1}{2\overline{|\gamma|} \exp\{Dr(\gamma)\}}\right)^{Dn-1}.$$

To obtain a contradiction, it suffices to show that

$$\left(1 + \frac{1}{2\overline{|\gamma|} \exp\{Dr(\gamma)\}}\right)^{Dn-1} < 2\overline{|\gamma|}.$$

As $Dn - 1 < 2^{Dn} \leq \exp\{Dr(\gamma)\}$, the left-hand side here is at most $\exp\{1/(2\overline{|\gamma|})\}$. The latter is less than $2\overline{|\gamma|}$ in the range $\overline{|\gamma|} \geq \gamma \geq 1$, which completes the proof of Theorem 1. \blacksquare

Proof of Theorem 2 Note that $r(m) = \log(2m)$ if m is a positive integer. If $M(\alpha) \neq m$, the inequality $\log|M(\alpha) - m| > -D \log(2m)$ follows from Theorem 1. So it suffices to show that if $M(\alpha) = m$ then one of the alternatives (i)–(iii) takes place.

Suppose now that $M(\alpha) = m$, where α is of degree d , with k conjugates outside the unit circle, and $a_d = q$ as the leading coefficient of its minimal polynomial. We have

$$\alpha_1 \alpha_2 \dots \alpha_k = \pm m/q.$$

Let us map α_1 to the conjugate α'_1 of the minimal absolute value (the Galois group of $\mathbb{Q}(\alpha_1, \dots, \alpha_d)$ is transitive). We then obtain the equality

$$\alpha'_1 \alpha'_2 \dots \alpha'_k = \pm m/q.$$

If, however, $0 < k < d$ then the modulus of the left-hand side here is smaller than m/q , a contradiction. Thus $k = 0$ or $k = d$. In the first case, $q = m$ and all conjugates of α are in the circle $|z| \leq 1$. Suppose we have at least one on the unit circle, say $|\alpha_1| = 1$. Then α is reciprocal, thus all conjugates of α are on the unit circle, and we have the alternative (i). If all conjugates are smaller than 1 in absolute value, we obtain the alternative (iii).

In the second case, namely if $k = d$, the product on the left-hand $\alpha_1 \dots \alpha_d$ is the norm of α . It is equal to $(-1)^d a_0/q$. Thus $a_0 = \pm m$. Since all conjugates are now strictly outside the unit circle, the alternative (ii) takes place. ■

An alternative way to prove Theorem 2 is to use the inequality on the Weil logarithmic height $h(\alpha_1 \alpha_2) \leq h(\alpha_1) + h(\alpha_2)$ (see e.g. Property 3.3 and Lemma 3.10 in [23]). Recall that $h(\alpha) = (1/d) \log M(\alpha)$.

Proof of Theorem 3 We will consider the polynomial $f(z) = P(d, m; z)(z - 1) = z^{d+1} - mz^d + m - 1$, or, more precisely, its reciprocal

$$g(z) = z^{d+1} f(1/z) = (m - 1)z^{d+1} - mz + 1.$$

As $m < (m - 1)(d + 1)$, for every sufficiently small positive number ε , the inequality $|(m - 1)z^{d+1} + 1| < |mz|$ is true on the circle $|z| = 1 - \varepsilon$. The polynomial $g(z)$, therefore, has exactly one root strictly inside the unit circle $|z| < 1$.

Suppose α is a root of $g(z)$ on the unit circle. From the equality of the moduli $|(m - 1)\alpha^{d+1} + 1| = |m\alpha| = m$, we deduce that $\alpha = \exp\{2\pi i u/(d + 1)\}$ with an integer u . Then $\alpha = ((m - 1)\alpha^{d+1} + 1)/m = 1$, and so $\alpha = 1$ is the only root of $g(z)$ on the unit circle. The remaining $d - 1$ roots of $g(z)$, therefore, are all strictly outside the unit circle. We deduce from all this that $g(z)/(z - 1)$ is irreducible, for otherwise its factor $g_1(z)$ has all roots outside the unit circle, which is impossible. Thus, $P(d, m; z)$ is irreducible and defines a Pisot number up to a sign. It is, in fact, the Pisot number, because $P(d, m; 1) < 0$ and $P(d, m; m) > 0$, so $P(d, m; z)$ has a root in the interval $(1, m)$.

It remains to prove that this root σ in $(1, m)$ is in the smaller interval, as claimed in Theorem 3. Indeed, note first that the sign of $P(d, m; z)$ and that of $f(z) = (z - m)z^d + m - 1$ are the same for every real $z > 1$. We have

$$f(m - (m - 1)m^{-d}) = (m - 1)(1 - (1 - (m - 1)m^{-d-1})^d) > 0.$$

Also,

$$f(m - (m - 1)m^{1-d}) = -(m - 1)(m(1 - (m - 1)m^{-d})^d - 1).$$

It is negative if

$$\frac{1}{m^{1/d}} + \frac{m - 1}{m^d} < 1.$$

The latter is equivalent to $(m^{1/d} - 1)/m^{1/d} > (m - 1)/m^d$. Since $m^{1/d} > 1$, this follows from

$$m^d > dm > \sum_{u=1}^d m^{u/d} = \frac{m^{1/d}(m - 1)}{m^{1/d} - 1}.$$

The proof of Theorem 3 is now completed, because $P(d, m; z)$ has a root in the interval $(m - (m - 1)m^{1-d}, m - (m - 1)m^{-d})$. ■

4 Examples

Suppose we are given a real algebraic integer β , of degree D , with conjugates as in Theorem A, such that the set of solutions of the equation

$$M(\alpha) = \beta$$

(in α) is non-empty. The problem of describing all solutions of this equation seems to be very difficult. There is almost nothing known about this except for Kronecker's theorem [12] stating that the only cyclotomic numbers are the solutions to $M(\alpha) = 1$. In case $D = 1$, $M(\alpha) \neq r$ for the rational non-integer numbers r , by Theorem A. Clearly, this is also the case with r non-positive. If, however, $\beta = m > 1$, the alternatives (i)–(iii) in Theorem 2 yield a kind of a semisolution to this problem. Even the simplest alternative (i) does not give too much information about the solutions, as the set of unit-circular numbers was not extensively studied. In [10] we call unit-circular those algebraic numbers with norm ± 1 . These are the only numbers with m as the leading coefficient of their minimal polynomials, which satisfy (i).

Problem Suppose $\beta > 1$ is a real quadratic algebraic number. Find all α such that $M(\alpha) = \beta$.

For a given algebraic number α , we consider the following sequence:

$$\overline{|\alpha|} \leq M(\alpha) \leq M(M(\alpha)) \leq M(M(M(\alpha))) \leq \dots,$$

where $A_0 = \overline{|\alpha|}$, $A_1 = M(\alpha)$, and $A_{n+1} = M(A_n)$ for $n \in \{1, 2, 3, \dots\}$. Suppose that α is neither zero nor a root of unity. For a “generic” algebraic number α the sequence A_n tends to ∞ as $n \rightarrow \infty$. For some α , say for every α of degree at most 3, the sequence is bounded. Clearly, if $A_{n+1} = A_n$ with $n \geq 0$ then A_n is either a Pisot or a Salem number, and so the A_m with $m \geq n$ are all equal to A_n . As in the famous $3x + 1$ problem, we say that α has the stopping time n if n is the smallest non-negative integer so that $A_m = A_n$ for $m \geq n$.

Fact If α has stopping time zero then it is either a root of unity or a conjugate of a Pisot or Salem number.

It is not at all clear how to describe all algebraic numbers with stopping time one. Note first that the numbers $(\pm\sigma)^{1/u}$ with σ a Pisot or Salem number and with an

integer u such that $|u| \geq 2$ all belong to this set. Clearly, this set also contains every algebraic number with $m \geq 2$ described by alternatives (i)–(iii). It also contains the algebraic integers with conjugates on two circles described by the author and Smyth in [10], as the measures of these are either Pisot or Salem numbers. In case of Salem numbers we called them Salem half-norms. For example, the measure of the Salem half-norm with minimal polynomial

$$z^{16} + 2z^{15} + z^{14} - 2z^{13} - 4z^{12} - 2z^{11} + 3z^{10} + 5z^9 + 3z^8 + z^7 - z^5 - z^4 - z^3 + z^2 + z + 1$$

is equal to $\sigma_0^4 = 1.91445\dots$, where $\sigma_0 = 1.17628\dots$ solves the Lehmer equation $z^{10} + z^9 - z^7 - z^6 - z^5 - z^4 - z^3 + z + 1 = 0$. Boyd [5], Theorem 2, showed that there are some other reciprocal numbers with the Pisot numbers as their Mahler measures. These are constructed by taking a product of half conjugates of a Pisot unit and are, therefore, in this sense Pisot half-norms.

In the latter two cases the Pisot or Salem numbers obtained are natural powers of other Pisot and Salem numbers. Is there a Salem (or a Pisot) number σ of degree ≥ 2 which is not a natural power of another Salem (Pisot) number, and such that $M(\alpha) = \sigma$ has some other solutions in α as those described above? In his thesis [20], Smyth showed that if σ_1 solves $z^3 = z + 1$ then the only non-reciprocal solutions of $M(\alpha) = \sigma_1$ are $\alpha = (\pm\sigma_1)^{1/u}$. The number σ_1 is the smallest Pisot number (Siegel [18]) and the smallest measure for non-reciprocal algebraic numbers (Smyth [19]). If, however, α is a non-reciprocal which is not of this form then $M(\alpha) > \sigma_1 + 10^{-4}$ (Smyth [19]). This was later improved by the author [8] to $M(\alpha) > \sigma_1 + 10^{-3}$. The computations of Boyd [2], [6] and of Mossinghoff [15] show that there no other solutions to the equation $M(\alpha) = \sigma_0$, except for $\alpha = (\pm\sigma_0)^{1/u}$, in α of degree at most 64.

If σ is a reciprocal quadratic unit, and so a Pisot number, then $M(\alpha) = \sigma$ has some other solutions than those described above. These, for example, can be the totally real quartic units. Let us take, for instance, $\alpha = ((11 + 2\sqrt{30})(2 + \sqrt{3}))^{1/2}$. Its Mahler measure is $11 + 2\sqrt{30}$. This is not a natural power of any other Pisot number. More generally, a solution of the equation

$$z^4 + 1 + (2 + u + v)z^2 = \sqrt{(u + 2)(v + 2)}(z^3 + 1),$$

where u, v are two positive integers such that say $u > v > 2$ and $(u + 2)(v + 2)$ is a perfect square, has the Mahler measure $(u + \sqrt{u^2 - 4})/2$, which is a reciprocal quadratic unit. We conclude with the following question.

Question Suppose $n \geq 2$. Is there an algebraic number α with stopping time n ?

Acknowledgements The author wishes to thank the anonymous referee for careful reading of the manuscript and the Department of Mathematics at Bielefeld University, where the paper was written, for the invitation. The research was partially supported by the Lithuanian State Science and Studies Foundation.

References

- [1] R.L. Adler and B. Marcus, *Topological entropy and equivalence of dynamical systems*. Mem. Amer. Math. Soc. **20**(1979), no.219.
- [2] D.W. Boyd, *Reciprocal polynomials having small measure*. Math. Comp. **35**(1980), 1361–1377.
- [3] ———, *Speculations concerning the range of the Mahler measure*. Canad. Math. Bull. **24**(1981), 453–469.
- [4] ———, *Perron units which are not Mahler measures*. Ergod. Th. and Dynam. Sys. **6**(1986), 485–488.
- [5] ———, *Reciprocal algebraic integers whose Mahler measures are non-reciprocal*. Canad. Math. Bull. **30**(1987), 3–8.
- [6] ———, *Reciprocal polynomials having small measure. II*. Math. Comp. **53**(1989), 355–357.
- [7] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*. Acta Arith. **34**(1979), 391–401.
- [8] A. Dubickas, *Algebraic conjugates outside the unit circle*. In: New Trends in Probability and Statistics Vol. 4: Analytic and Probabilistic Methods in Number Theory, Palanga, 1996, (eds., A. Laurinćikas et al.), TEV Vilnius, VSP Utrecht, 1997, 11–21.
- [9] ———, *Polynomials with a root close to an integer*. Liet. Matem. Rink. **39**(1999), 310–316.
- [10] A. Dubickas and C.J. Smyth, *On the Remak height, the Mahler measure, and conjugate sets of algebraic numbers lying on two circles*. Proc. Edinburgh Math. Soc. (to appear).
- [11] G. Everest and T. Ward, *Heights of polynomials and entropy in algebraic dynamics*. Springer, London, 1999.
- [12] L. Kronecker, *Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten*. J. für die Reine Angew. Math. **53**(1857), 173–175.
- [13] D.H. Lehmer, *Factorization of certain cyclotomic functions*. Ann. of Math. **34**(1933), 461–479.
- [14] R. Louboutin, *Sur la mesure de Mahler d'un nombre algébrique*. C. R. Acad. Sci., Paris **296**(1983), 707–708.
- [15] M.J. Mossinghoff, *Polynomials with small Mahler measure*. Math. Comp. **67**(1998), 1697–1705.
- [16] O. Perron, *Neue Kriterien für die Irreduzibilität algebraischer Gleichungen*. J. für die Reine Angew. Math. **132**(1907), 288–307.
- [17] E.S. Selmer, *On the irreducibility of certain trinomials*. Math. Scand. **4**(1956), 287–302.
- [18] C.L. Siegel, *Algebraic integers whose conjugates lie in the unit circle*. Duke Math. J. **11**(1944), 597–602.
- [19] C.J. Smyth, *On the product of conjugates outside the unit circle of an algebraic integer*. Bull. London Math. Soc. **3**(1971), 169–175.
- [20] C.J. Smyth, *Topics in the theory of numbers*. PhD Thesis, University of Cambridge, 1972.
- [21] P. Voutier, *An effective lower bound for the height of algebraic numbers*. Acta Arith. **74**(1996), 81–95.
- [22] M. Waldschmidt, *Sur le produit des conjugués extérieurs au cercle unité d'un entier algébrique*. L'Enseign. Math. (2) **26**(1980), 201–209.
- [23] ———, *Diophantine approximation on linear algebraic groups*. Grundlehren der mathematischen Wissenschaften series **326**, Springer, Berlin–Heidelberg, 2000.

Department of Mathematics and Informatics
Vilnius University
Naugarduko 24

2600 Vilnius, Lithuania

website: http://www.mif.vu.lt/ttsk/bylos/da/da_a.html

e-mail: arturas.dubickas@maf.vu.lt