Mahler measures, their quotients and differences

Artūras Dubickas
Vilnius University

Nijmegen 2023

Definitions

Let $\mathcal{M}$ be the set of Mahler measures of algebraic numbers, that is,

$$\mathcal{M} = \{M(\alpha) \ : \ \alpha \in \overline{\mathbb{Q}}\}.$$

By $\mathcal{M}^*$ we denote the set of Mahler measures of integer polynomials, namely,

$$\mathcal{M}^* = \{M(P) \ : \ P \in \mathbb{Z}[x]\}.$$

Here, the notation $*$ is used, because $\mathcal{M}^*$ is the multiplicative semigroup generated by $\mathcal{M}$. (This follows by the multiplicativity of Mahler's measure of polynomials.)

Pisot and Salem numbers

Recall that an algebraic integer $\alpha > 1$ is a *Pisot number* if its conjugates over $\mathbb{Q}$ (if any) all lie in $|z| < 1$. The set of Pisot numbers will be denoted by $\mathcal{P}$.

Also, an algebraic integer $\alpha > 1$ is a *Salem number* if its conjugates over $\mathbb{Q}$ all lie in $|z| \leq 1$ with at least one case of equality. Each Salem number is reciprocal. The set of Salem numbers will be denoted by $\mathcal{S}$.

We have $\mathcal{P} \subset \mathcal{M}$ and $\mathcal{S} \subset \mathcal{M}$. Also, $M(\alpha) \geq |\alpha|$, where $M(\alpha) = \alpha$ if and only if $\alpha \in \mathcal{P} \cup \mathcal{S} \cup \{1\}$.

Below, we will consider the sets $\mathcal{P} \pm \mathcal{P}$, $\mathcal{S} \pm \mathcal{S}$, $\mathcal{M} \pm \mathcal{M}$, and corresponding product and quotient sets.

The sets of Mahler's measures $\mathcal{M}$ and $\mathcal{M}^*$

The first results related to the sets $\mathcal{M}$ and $\mathcal{M}^*$ were obtained by David Boyd:

- D.W. Boyd, *Inverse problems for Mahler's measure,* in "Diophantine Analysis" (J. Loxton and A. van der Poorten, eds.), London Math. Soc. Lecture Notes, **109**, Cambridge Univ. Press, Cambridge 1986, 147–158.
- D.W. Boyd, *Perron units which are not Mahler measures,* Ergod. Theory and Dynamical Sys. **6** (1986), 485–488.
- D.W. Boyd, *Reciprocal algebraic integers whose Mahler measures are non-reciprocal,* Canad. Math. Bull. **30** (1987), 3–8.

An example of Boyd's results

Building on the very first result of this type

- R.L. Adler and B. Marcus, *Topological entropy and equivalence of dynamical systems,* Mem. Amer. Math. Soc. **20** (1979), no. 219.

Boyd showed that

Theorem

Every $\alpha \in \mathcal{M}^*$ is an algebraic integer which is a Perron number; that is, a real positive algebraic number such that every algebraic conjugate α' of α over $\mathbb{Q}$ with $\alpha' \neq \alpha$ (if any) satisfies $\alpha > |\alpha'|$. Moreover, if $\alpha \in \mathcal{M}^*$, then $|\alpha'| > \alpha^{-1}$ unless $\alpha' = \pm\alpha^{-1}$.

Further necessity criteria

Some further necessity (and some sufficiency) criteria for α to be in $\mathcal{M}$ were given in

- A. Dubickas, *On numbers which are Mahler measures,* Monatsh. Math. **141** (2004), 119–126.

  It was shown, for example, that

Theorem

If α of degree $d \geq 3$ is not a unit, not a Pisot or a Salem number, and belongs to $\mathcal{M}$, then its norm is not square-free.

Towards sufficiency:

Theorem

If a unit α is in $\mathcal{M}$ then $\alpha^m \in \mathcal{M}$ for every positive integer m.

A converse of Boyd's result

Theorem

If α is a positive algebraic number, then for some $n \in \mathbb{N}$ we have $n\alpha \in \mathcal{M}$.

Since $n \in \mathcal{M}$ (as $n = M(n)$) this implies that each positive algebraic number is a quotient of two Mahler measures.

Proof

Assume that β has minimal polynomial $P(x)$ of degree d with leading coefficient $b \in \mathbb{N}$ and with height (i.e. the maximal modulus of all coefficients of P) $H(\beta)$. Let β^* be the maximal modulus of all roots of P different from β. (If $d = 1$, set $\beta^* = 0$.) Since β is a Perron number, $\beta^* < \beta$. Clearly, there are infinitely many pairs of prime numbers $q \neq t$ for which

$$\beta^* < \frac{q}{tb} < \beta.$$

Take such a pair q, t for which $q > H(\beta)$. We claim that $n\beta$, where $n = q^{d-1}tb$, is the Mahler measure of the number $tb\beta/q$.

Proof: continuation

Indeed, $tb\beta/q$ is the root of the polynomial $P(qx/(tb))$. Furthermore, the polynomial $t^d b^{d-1} P(qx/(tb))$ has integer coefficients. Its two extreme coefficients are q^d and $t^d b^{d-1} P(0)$. By our choice of q, t, these two integers are relatively prime. Consequently, $t^d b^{d-1} P(qx/(tb))$ is an integer polynomial irreducible in $\mathbb{Z}[x]$. All its roots except for $tb\beta/q > 1$ lie in the unit circle, so

$$M(tb\beta/q) = q^d tb\beta/q = q^{d-1} tb\beta = n\beta,$$

as claimed.

Dynamical system

In that paper I also considered the iterations of the map $\alpha \to M(\alpha)$, i.e. the sequence $\alpha, M(\alpha), M(M(\alpha)), \dots$ introduced earlier in

- A. Dubickas, *Canad. Math. Bull.* **45** (2002), 196–203.

The sequence is nondecreasing and becomes constant as soon as it reaches a Pisot or a Salem number β (or 1), since then (and only then) $\beta = M(\beta)$.

This problem was further investigated by Fili, Pottmeyer and Zhang:

- P.A. Fili, L. Pottmeyer and M. Zhang, *On the behavior of Mahler's measure under iteration,* Monatsh. Math. **193** (2020), 61–86.
- P.A. Fili, L. Pottmeyer and M. Zhang, *Wandering points for the Mahler measure,* Acta Arith. **204** (2022), 225–252.

Some results of Fili, Pottmeyer and Zhang

Assume that the sequence $\alpha, M(\alpha), M(M(\alpha)), \ldots$ reaches a Pisot or a Salem number after $k \geq 0$ steps. Then, $\mathcal{O}_M(\alpha)$ is the orbit of α under M with size $|\mathcal{O}_M(\alpha)|$. The corresponding stopping time is $k = |\mathcal{O}_M(\alpha)| - 1$. It can be infinite.

I showed that for a "generic" α the stopping time is infinite, but on the other hand for each $k \geq 0$ there is an algebraic number α with stopping time k.

F-P-Z proved the following:

Theorem

For any integers $d \geq 3$, $l \neq 0, \pm 1$ and $s \geq 1$ there is an algebraic integer α degree d with norm l and $|\mathcal{O}_M(\alpha)| = s$.

Further results of Fili, Pottmeyer and Zhang

My question was to classify all number fields K such that for every $\alpha \in K$ we have $|\mathcal{O}_M(\alpha)| < \infty$.

Some results of F-P-Z towards this:

Theorem

For any α of degree $d \leq 3$ one has $|\mathcal{O}_M(\alpha)| < \infty$. For any algebraic unit α of degree $d = 4$ one has $|\mathcal{O}_M(\alpha)| \leq 2$ or $|\mathcal{O}_M(\alpha)| = \infty$.
Moreover, if $|\mathcal{O}_M(\alpha)| = \infty$, then $M(M(M(\alpha))) = M(\alpha)^2$.

Theorem

Let $[K : \mathbb{Q}] = 5$. Then, K contains a unit α satisfying $|\mathcal{O}_M(\alpha)| = \infty$.

Further results of Fili, Pottmeyer and Zhang

For units of degree $d = 4$ they also showed the following:

Theorem

If α is an algebraic unit of degree 4, then the sequence $\log M^{(n)}(\alpha)_{n\in\mathbb{N}}$ satisfies a linear homogeneous recursion.

By one of the above theorems, in the case $|\mathcal{O}_M(\alpha)| = \infty$ the recursion is

$$x_n = 2x_{n-2}.$$

Conjecture (F-P-Z). *For every algebraic unit α there is a $k \in \mathbb{N}$ such that the sequence $\log M^{(n)}(\alpha)_{n\geq k}$ satisfies a linear homogeneous recursion.*

Further results of Fili, Pottmeyer and Zhang

Theorem

If α is an algebraic unit of degree d such that the Galois group of the Galois closure of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ contains the alternating group A_d, then $|\mathcal{O}_M(\alpha)| \in \{1, 2, \infty\}$.
More precisely, if α is as above, of degree ≥ 5, and such that none of $\pm\alpha^{\pm 1}$ is conjugate to a Pisot number, then $|\mathcal{O}_M(\alpha)| = \infty$.

This explains that the "generic" case for a unit α is $|\mathcal{O}_M(\alpha)| = \infty$.

Here, in all cases the process terminates when after several iterations one gets a Pisot number.

Why not Salem?

Why not Salem number?

The reason is that the Galois group of the Galois closure of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ for a Salem number α is "small".

- F. Lalande, *Corps de nombres engendrés par un nombre de Salem,* Acta Arith **88** (1999), 191-200.
- C. Christopoulos and J. McKee, *Galois theory of Salem polynomials,* Math. Proc. Cambridge Philos. Soc. **148** (2010), 47-54.
- A. Dubickas, *Salem numbers as Mahler measures of nonreciprocal units,* Acta Arith. **176** (2016), 81–88.

Lalande showed that for each $n \geq 2$ there are Salem numbers of degree $d = 2n$ with the largest possible Galois groups $\mathbb{Z}_2^n \rtimes S_n$ of order $2^n n!$. A more precise result about which Galois groups may occur has been given by Christopoulos and McKee, and the final result by myself (by replacing the statement "only if n is odd" by "if and only if n is odd").

Further results of Fili, Pottmeyer and Zhang

Recall that my question was to classify all number fields K such that for every $\alpha \in K$ we have $|\mathcal{O}_M(\alpha)| < \infty$. The previous results imply that this is the case for $[K : \mathbb{Q}] \leq 3$.

They solved this problem for abelian number fields.

Theorem

Let K be a number field such that the Galois group of $K/\mathbb{Q}$ is abelian. Then for each $\alpha \in K$ we have $|\mathcal{O}_M(\alpha)| < \infty$ if and only if the maximal totally real subfield of K has Galois group isomorphic to C_1, C_2, C_3, or $C_2 \times C_2$, where C_n denotes the cyclic group of order n.
In all other cases, there is a unit $\alpha \in K$ satisfying $|\mathcal{O}_M(\alpha)| = \infty$.

Further developments

Some further results related to the sets $\mathcal{M}$ and $\mathcal{M}^*$ were obtained in 2004:

- J.D. Dixon and A. Dubickas, *The values of Mahler measures,* Mathematika **51** (2004), 131–148.

There, we proved, for example, that $\mathcal{M}$ is a proper subset of $\mathcal{M}^*$:

Theorem

$\mathcal{M} \neq \mathcal{M}^*$. For example, if $\alpha > 1$ and $\beta > 1$ are two quadratic units such that $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) = \mathbb{Q}$, then $\alpha\beta \in \mathcal{M}^* \setminus \mathcal{M}$.

The difficult part here is to show that $\alpha\beta \notin \mathcal{M}$.

Main result in that paper

...shows that, in principle, the problem of determining whether α is in $\mathcal{M}^*$ or not can be solved for any specified α.

Theorem

Suppose that α is an algebraic number of degree d, and F is the Galois closure of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$. If $\alpha \in \mathcal{M}^*$ then $\alpha = M(f)$ for some separable polynomial $f(X) \in \mathbb{Z}[X]$ of degree at most $\sum_{1 \le r \le d/2} \binom{d}{r}$ whose roots lie in F. Moreover, if $\alpha \in \mathcal{M}$ is a unit then $\alpha = M(\beta)$ for some unit $\beta \in F$ of degree at most $\binom{d}{\lfloor d/2 \rfloor}$.

(The second part explains how we proved that the product of two quadratic units α, β satisfying $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) = \mathbb{Q}$ is not in $\mathcal{M}$.)

We do not have a similar result for the whole set $\mathcal{M}$.

Schinzel's result

Is it true that if $\alpha \in \mathcal{M}$ then $\alpha = M(\beta)$ for some $\beta \in F$? (Recall that F is the Galois closure of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$.) In 2004 we showed that this is true for units and some other classes of numbers in $\mathcal{M}$.

However, in

- A. Schinzel, *On values of the Mahler measure in a quadratic field (solution of a problem of Dixon and Dubickas)*, Acta Arith. **113** (2004), 401–408

Schinzel constructed certain quadratic numbers α which belong to $\mathcal{M}$, but which are not expressible as $\alpha = M(\beta)$ with $\beta \in \mathbb{Q}(\alpha)$. (For quadratic numbers α, the field $\mathbb{Q}(\alpha)$ is Galois, so $F = \mathbb{Q}(\alpha)$.)

Schinzel's result

For example, by one of his theorems, $\alpha = 21 + 14\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ is the Mahler measure of the quartic irreducible polynomial

$$7X^4 + 2X^3 + 41X^2 + 22X + 7,$$

but $21 + 14\sqrt{2} \neq M(\beta)$ for any $\beta \in \mathbb{Q}(\sqrt{2})$. His results imply, for instance, that

Theorem

For all primes p we have $p^{\frac{3+\sqrt{5}}{2}} \in \mathcal{M}$ if and only if either $p \in \{2, 5\}$ or $5|(p \pm 1)$.

So the overall situation with $\mathcal{M}$ is much more complicated. It is not known, for instance, whether $1 + \sqrt{17}$ belongs to $\mathcal{M}$ or not.

Schinzel's question

Question. *Let K be a real quadratic field. Assume that $\alpha \in K$ is a primitive algebraic integer such that $\alpha \in \mathcal{M}$, and p is a prime number that splits in K. Is it true that then $p\alpha \in \mathcal{M}$?*

An algebraic integer α is called *primitive* if α/k is not an algebraic integer for every integer $k \geq 2$.

He proved that the answer is positive if at least one of the inequalities

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

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

holds. Here, α' is conjugate to α over $\mathbb{Q}$ and Δ is the discriminant of the field K.

Generalization to cubic numbers

Some results of Schinzel were extended to cubic numbers:

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

Theorem

A primitive real cubic integer β is in $\mathcal{M}$ if and only if there is a rational integer k such that $\beta > k > \max\{|\beta'|, |\beta''|\}$, $k|(\beta\beta' + \beta\beta'' + \beta'\beta'')$ and $k^2|\beta\beta'\beta''$, where β' and β'' are the conjugates of β.

An example of a cubic measure

Example

Consider $\theta > 1$ satisfying $\theta^3 - 3\theta - 1 = 0$. The field $\mathbb{Q}(\theta)$ is cyclic, so it is Galois and its normal extension is $F = \mathbb{Q}(\theta)$. Then, $\gamma = 2 + \theta$ is a root of $x^3 - 6x^2 + 9x - 3 = 0$. The polynomial

$$P(x) = 27x^6 + 27x^5 + 63x^4 + 37x^3 + 33x^2 + 9x + 3$$

is irreducible in $\mathbb{Z}[x]$ and has Mahler's measure 9γ. One of our theorems (applied to the number 9γ) implies that there is no $\beta \in \mathbb{Q}(\theta) = \mathbb{Q}(\gamma) = F$ for which $9\gamma = 18 + 9\theta = M(\beta)$, although $9\gamma \in \mathcal{M}$.

Other results

Among other results in that paper I showed that:

Theorem

If $\alpha \in \mathcal{M}$ then $\alpha^m \in \mathcal{M}$ for every positive integer m.

(Eerlier this result was proved for units.)

Question. *Is there a real number $\alpha \notin \mathbb{N}$ such that $m\alpha \in \mathcal{M}$ for every $m = 1, 2, 3, \ldots$?*

Probably, the answer is "no".

A result related to the above question

Set $\beta = (1+\sqrt{5})/2$ and $\beta' = (1-\sqrt{5})/2$. Then,

- For each positive integer m the number $m^2\beta$ belongs to $\mathcal{M}$.

We have $M(mX^2 + X + m\beta) = m\beta$ and $M(mX^2 + X + m\beta') = m$. Hence,

$$M(m^2X^4 + 2mX^3 + (m^2+1)X^2 + mX - m^2) = m^2\beta.$$

It is easy to see that the polynomial $m^2X^4 + 2mX^3 + (m^2+1)X^2 + mX - m^2$ is irreducible for every positive integer m, since it has coprime coefficients and the degree of $\sqrt{1-4m^2\beta}$ over $\mathbb{Q}$ is equal to 4. (If it would be equal to 2, then its conjugate must be $\eta\sqrt{1-4m^2\beta'}$ with $\eta = 1$ or $\eta = -1$. But their product $\eta\sqrt{1-4m^2-16m^4}$ is irrational for every $m \geq 1$, which is impossible.)

Proof of the theorem about powers

Assume that $\beta = M(\alpha)$. Fix $m \geq 2$. Suppose that the degree of α over $\mathbb{Q}$ is d, and let d_n denote the degree of α^n over $\mathbb{Q}$, so that $d_1 = d$. The quantity

$$h(\gamma) = \frac{\log M(\gamma)}{\deg \gamma}$$

is called the *Weil height* of $\gamma \in \overline{\mathbb{Q}}$. We will apply the formula

$$h(\gamma^n) = nh(\gamma)$$

to the powers of α. If $d_m = d$, then $h(\alpha^m) = mh(\alpha)$ implies immediately that

$$\beta^m = M(\alpha)^m = e^{mdh(\alpha)} = e^{mdh(\alpha^m)/m} = e^{d_m h(\alpha^m)} = M(\alpha^m),$$

so $\beta^m \in \mathcal{M}$.

Proof of the theorem about powers: continuation

We now turn to the case $d_m < d$. Set $t_1 = d/d_m$, $t_2 = d_m/d_{mt_1}$, $t_3 = d_{mt_1}/d_{mt_1t_2}$, etc. Each t_i is an integer, because $\mathbb{Q}(\alpha^u)$ is a subfield of $\mathbb{Q}(\alpha^v)$ if $v|u$.

Since

$$t_1 t_2 \dots t_k = d/d_{mt_1\dots t_{k-1}} \le d,$$

sooner or later in the sequence $t_1, t_2, t_3, \dots$ we will get an element equal to 1. Let $k \ge 2$ be the smallest positive integer for which $t_k = 1$. Using the equalities $h(\alpha^{mt_1\dots t_{k-1}}) = mt_1 \dots t_{k-1} h(\alpha)$ and

$$d/d_{mt_1\dots t_{k-1}} = t_1 \dots t_k = t_1 \dots t_{k-1},$$

we obtain

$$\beta^m = M(\alpha)^m = e^{mdh(\alpha)} = e^{dh(\alpha^{mt_1\dots t_{k-1}})/(t_1\dots t_{k-1})} =$$

$$= e^{d_{mt_1\dots t_{k-1}} h(\alpha^{mt_1\dots t_{k-1}})} = M(\alpha^{mt_1\dots t_{k-1}}) \in \mathcal{M}.$$

Additive and multiplicative groups

The first results about additive and multiplicative groups generated by $\mathcal{M}$ were obtained in

- A. Dubickas, *Mahler measures generate the largest possible groups*, Math. Res. Lett. **11** (2004), 279–283.

The multiplicative group is maximal possible: it consists of all positive algebraic numbers.

Theorem

For every positive algebraic number α there exist $\beta, \gamma \in \mathbb{Q}(\alpha)$ such that $\alpha = \frac{M(\beta)}{M(\gamma)}$.

Additive group generated by $\mathcal{M}$

Let $\mathcal{M}^+ = \{\sum k_j m_j \mid m_j \in \mathcal{M}, k_j \in \mathbb{Z}\}$ be a free additive group generated by $\mathcal{M}$. Here is an example showing that $\mathcal{M} \neq \mathcal{M} + \mathcal{M}$.

Example

Let $d \geq 4$ be an even integer. Then $\alpha > 1$ solving $x^d - x^{d-1} - \cdots - x - 1 = 0$ is a Pisot number, and so $\alpha + 1$ is in $\mathcal{M} + \mathcal{M}$, but not in $\mathcal{M}$. (Not even in $\mathcal{M}^*$.)

The proof of $\beta = \alpha + 1 \in \mathcal{M} + \mathcal{M} \setminus \mathcal{M}^*$ rests on Boyd's necessity criterion.

Proof

The fact that $x^d - x^{d-1} - \cdots - x - 1 = 0$, $d \geq 2$, defines a Pisot number α, where $1 < \alpha < 2$, is well–known and follows easily from Rouché's theorem. Thus $\beta = \alpha + 1 \in \mathcal{M} + \mathcal{M}$, since $\alpha = M(\alpha) \in \mathcal{M}$ and $1 = M(1) \in \mathcal{M}$. The number $\beta < 3$ is the largest positive root of its minimal polynomial

$$g(x) = (x-1)^d - \frac{(x-1)^d - 1}{x-2} \in \mathbb{Z}[x].$$

If $\beta \in \mathcal{M}^*$ then, by Boyd's criterion mentioned above, we would have that all conjugates of β over $\mathbb{Q}$ are greater than $1/3$ in absolute value. However, for even $d \geq 4$, we have that $g(0) = 1 > 0$ and

$$g(1/3) = \frac{8(-2/3)^d - 3}{5} \leq \frac{8 \cdot (16/81) - 3}{5} < 0.$$

So $g(x)$ has a root in the interval $(0, 1/3)$, a contradiction. Hence, $\beta = \alpha + 1 \in (\mathcal{M} + \mathcal{M}) \setminus \mathcal{M}^*$.

$\mathcal{M}^+$ is the set of all real algebraic integers

Clearly, every element of $\mathcal{M}^+$ is a real algebraic integer. The converse is also true. More precisely, we have the following:

Theorem

For every real algebraic integer α there exist four numbers $\beta, \gamma, \beta', \gamma' \in \mathbb{Q}(\alpha)$ and two positive integers b, c such that $\alpha = bM(\beta) + cM(\gamma) - bM(\beta') - cM(\gamma')$.

The set of differences $\mathcal{M} - \mathcal{M}$

The last theorem raises the question:

Question. *Is it true that every real algebraic integer belongs to the set $\mathcal{M} - \mathcal{M}$?*

In

- P. Drungilas and A. Dubickas, *Every real algebraic integer is a difference of two Mahler measures*, Canadian Math. Bull. **50** (2007), 191–195

we proved a result which implies that every real algebraic integers belongs to the set $\mathcal{M} - \mathcal{M}^*$

The set of differences $\mathcal{M} - \mathcal{M}^*$

Theorem

Every real algebraic integer α of degree d can be written as $\alpha = M(P) - M(Q)$, where $P, Q \in \mathbb{Z}[x]$, $\deg P = \deg Q = d$, P is irreducible in $\mathbb{Z}[x]$ and Q has an irreducible factor of degree d. Furthermore, if $d \leq 3$ then both P and Q can be chosen to be irreducible.

The theorem implies that $\mathcal{M} - \mathcal{M}$ contains all real algebraic integers of degree at most 3. How about degree $d \geq 4$?

The method used in the proof of the above theorem (concerning the possibility to express α in the form $M(\beta) - M(\gamma)$ for any d) leads to the diophantine equation $ax^{d-1} - by^{d-1} = 1$. Here, a, b are positive integers satisfying certain additional conditions.

The set of differences $\mathcal{M} - \mathcal{M}$ for degree $d \geq 5$

More precisely, we need the following statement: if g and d are fixed positive integers then, for every positive integer l, there is a solution of the equation $ax^{d-1} - by^{d-1} = 1$ in positive integers a, b, x and y such that $\gcd(ag, x)=\gcd(bg, y)= 1$ and $x > la$, $y > lb$. Unfortunately, there is a little hope that this statement holds for any $d \geq 5$. The point is that, for $d \geq 5$, it contradicts to the well-known *abc*-conjecture!

Indeed, suppose that there are $a, b, x, y \in \mathbb{N}$ satisfying the conditions as above. Then the *abc*-conjecture implies that

$$by^{d-1} < ax^{d-1} < C_\epsilon\Big(\prod_{p|abxy} p\Big)^{1+\epsilon} \leq C_\epsilon(abxy)^{1+\epsilon},$$

where $\epsilon > 0$ and where C_ϵ is a constant depending on ϵ only. Consequently,

$$by^{d-1}ax^{d-1} < C_\epsilon^2(abxy)^{2+2\epsilon}.$$

...continuation

Cancelling terms from both sides we deduce

$$(xy)^{d-3-2\epsilon} < C_\epsilon^2 (ab)^{1+2\epsilon}.$$

Hence, for $x > la$ and $y > lb$, we deduce that

$$l^{2d-6-4\epsilon} < C_\epsilon^2 (ab)^{4-d+4\epsilon}.$$

Note that for $d \geq 5$ and $\epsilon < 1/4$ the right hand side is less than C_ε^2. The left hand side tends to infinity as $l \to \infty$ for $d \geq 4$ and $\epsilon < 1/4$. So the above equation does not have a solution for l sufficiently large.

Of course, this only implies that possibly not all algebraic integers of degree $d \geq 5$ are expressible in the form $\mathcal{M} - \mathcal{M}$ using the construction of the abovementioned paper (Canad. Math. Bull., 2007).

Density of $\mathcal{M}$ modulo 1

By a result of Salem

- R. Salem, *Algebraic numbers and Fourier analysis,* Boston, 1963

powers of a quartic Salem number are everywhere dense in $[0,1]$, but not uniformly distributed in $[0,1]$. Thus, the set $\mathcal{S}$ modulo 1 is everywhere dense. Consequently, the set $\mathcal{M}$ modulo 1 is also everywhere dense.

How about the set

$$\mathcal{M}_K := \{M(\alpha) \ : \ \alpha \in K\},$$

where K is a fixed number field?

Not every field contains a Salem number!

Density of $\mathcal{M}_K$ modulo 1

Of course, in the case when $K = \mathbb{Q}$ each Mahler measure $M(\alpha)$, where $\alpha \in \mathbb{Q}$, is a positive integer, so the fractional part $\{M(\alpha)\}$ (that is, $M(\alpha)$ modulo 1) is equal to 0.

Similarly, if $K = \mathbb{Q}(\sqrt{-D})$, where D is a positive integer, then $\alpha \in \mathbb{Q}(\sqrt{-D})$ is either a rational number or a complex quadratic number. In the first case, $M(\alpha)$ is an integer. In the second case, α and $\overline{\alpha}$ are conjugate over $\mathbb{Q}$, so $M(\alpha)$ is a positive integer too by $\alpha\overline{\alpha} \in \mathbb{Q}$. Consequently, $\{M(\alpha)\} = 0$ for each $\alpha \in \mathbb{Q}(\sqrt{-D})$.

It turns out that for $K \neq \mathbb{Q}$ and $K \neq \mathbb{Q}(\sqrt{-D})$ the set $\mathcal{M}_K$ modulo 1 is dense in $[0, 1]$.

Density of $\mathcal{M}_K$ modulo 1

This was shown in

- A. Dubickas, *Mahler measures in a field are dense modulo 1,* Archiv der Math. **88** (2007), 29–34.

More precisely,

Theorem

Let K be a number field which is neither $\mathbb{Q}$ nor its quadratic complex extension. Then there is a number $\beta \in K$ with minimal polynomial $Q(x) \in \mathbb{Z}[x]$ such that for

$$\gamma_k := \frac{\beta + |Q(1)|k}{|Q(1)|k + 1} \in K,$$

$k = 1, 2, 3, \ldots,$ the sequence of Mahler measures $M(\gamma_1), M(\gamma_2), M(\gamma_3), \ldots$ modulo 1 is uniformly distributed in $[0, 1]$.

Sumsets of Pisot and Salem numbers

Recall that $\mathcal{P} \subset \mathcal{M}$ and $\mathcal{S} \subset \mathcal{M}$. In

- A. Dubickas, *Sumsets of Pisot and Salem numbers,* Expositiones Mathematicae **26** (2008), 85–91

the following questions were considered.

- Can m Salem numbers sum to a Salem number?
- Can m Salem numbers sum to a Pisot number?
- Can m Pisot numbers sum to a Salem number?

One 'missing' case is trivial. Since $\{2, 3, 4, \dots\} \subset \mathcal{P}$, every sum of m Pisot numbers which are positive integers greater than 1 is a Pisot number itself.

The answer to the first question is negative:

Theorem

For any integer $m \geq 2$ no sum of m Salem numbers is a Salem number.

We say that an algebraic number $\gamma > 0$ is a *Perron number* if its conjugates over $\mathbb{Q}$ different from γ itself (if any) all lie in the unit disc $|z| < \gamma$. In particular, Pisot and Salem numbers are Perron numbers.

The next result is useful for the proof of the above theorem.

Lemma

Suppose that $\gamma, \gamma_1, \ldots, \gamma_m$, where $m \in \mathbb{N}$, are Perron numbers satisfying $\gamma = \gamma_1 + \cdots + \gamma_m$. Then $\gamma_1, \ldots, \gamma_m \in \mathbb{Q}(\gamma)$.

Proof of the lemma

Let F be a normal closure of $\mathbb{Q}(\gamma, \gamma_1, \ldots, \gamma_m)$ over $\mathbb{Q}$. Suppose, for instance, that $\gamma_1 \notin \mathbb{Q}(\gamma)$. Then $\mathbb{Q}(\gamma, \gamma_1)$ is proper extension of $\mathbb{Q}(\gamma)$, so there is an automorphism $\sigma : F \mapsto F$ which maps $\gamma \mapsto \gamma$ and $\gamma_1 \mapsto \gamma'$, where $\gamma' \neq \gamma_1$ is conjugate to γ_1 over $\mathbb{Q}(\gamma)$. Hence,
$\gamma = \gamma_1 + \cdots + \gamma_m = \sigma(\gamma) = \gamma' + \sigma(\gamma_2) + \cdots + \sigma(\gamma_m)$. The right hand side here is equal to

$$\gamma = |\gamma| = |\gamma' + \sigma(\gamma_2) + \cdots + \sigma(\gamma_m)| \leq |\gamma'| + |\sigma(\gamma_2)| + \cdots + |\sigma(\gamma_m)|.$$

Clearly, $\mathbb{Q} \subseteq \mathbb{Q}(\gamma)$, so γ' is conjugate to γ_1 over the smaller field $\mathbb{Q}$. Thus $|\gamma'| < \gamma_1$. Similarly, $|\sigma(\gamma_j)| \leq \gamma_j$ for each $j \in \{2, \ldots, m\}$, because $\sigma(\gamma_j)$ and γ_j are conjugate over $\mathbb{Q}$. (This time, $\sigma(\gamma_j)$ and γ_j can be equal.) It follows that the above sum of moduli is strictly smaller than $\gamma_1 + \gamma_2 + \cdots + \gamma_m = \gamma$, a contradiction. By the same argument, we conclude that $\gamma_2, \ldots, \gamma_m \in \mathbb{Q}(\gamma)$.

Proof of the theorem

Suppose that there exist Salem numbers $\alpha, \alpha_1, \dots, \alpha_m$, where $m \geq 2$, such that $\alpha = \alpha_1 + \cdots + \alpha_m$. By the lemma, there are nonzero polynomials $f_1, \dots, f_m \in \mathbb{Q}[x]$ such that $\alpha_j = f_j(\alpha)$ for each $j = 1, \dots, m$. An automorphism of the Galois closure of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ taking $\alpha \mapsto \alpha^{-1}$ maps the equality $\alpha = f_1(\alpha) + \cdots + f_m(\alpha)$ into $\alpha^{-1} = f_1(\alpha^{-1}) + \cdots + f_m(\alpha^{-1})$. For any $j \in \{1, \dots, m\}$, the number $f_j(\alpha^{-1})$ is a real conjugate of $\alpha_j = f_j(\alpha)$ over $\mathbb{Q}$, hence $f_j(\alpha^{-1}) \in \{\alpha_j, \alpha_j^{-1}\}$. Thus, $f_j(\alpha^{-1}) > 0$ and $f_j(\alpha) f_j(\alpha^{-1}) = \alpha_j^2$ or 1. In both cases, $f_j(\alpha) f_j(\alpha^{-1}) \geq 1$. Hence,

$$1 = \alpha\alpha^{-1} = (f_1(\alpha) + \cdots + f_m(\alpha))(f_1(\alpha^{-1}) + \cdots + f_m(\alpha^{-1}))$$

$$> \sum_{j=1}^{m} f_j(\alpha) f_j(\alpha^{-1}) \geq m,$$

a contradiction.

Two remaining questions

The next two theorems imply that the answers to the second and to the third questions are positive.

Theorem

For any integer $m \geq 2$ and any Salem number α there exist infinitely many $n \in \mathbb{N}$ for which the sum $\alpha^n + \alpha^{2n} + \cdots + \alpha^{mn}$ is a Pisot number.

Theorem

For any integer $m \geq 2$ and any Salem number α there exist infinitely many $n \in \mathbb{N}$ for which there are Pisot numbers $\beta_1, \ldots, \beta_m \in \mathbb{Z}[\alpha]$ summing to the Salem number α^n, namely, $\beta_1 + \beta_2 + \cdots + \beta_m = \alpha^n$.

Our results imply that the set $m\mathcal{S} \cap \mathcal{S}$ is empty, whereas the sets $m\mathcal{S} \cap \mathcal{P}$ and $m\mathcal{P} \cap \mathcal{S}$ are nonempty for any integer $m \geq 2$.

Example

Example

Equation $x^4 - 5x^3 + 7x^2 - 5x + 1 = 0$ defines the Salem number $\alpha := (5 + \sqrt{5} + \sqrt{10\sqrt{5} + 14})/4$. Its square

$$\alpha^2 = (22+10\sqrt{5}+5\sqrt{10\sqrt{5} + 14}+\sqrt{50\sqrt{5} + 70})/8 = 10.99925\ldots$$

(which is a Salem number) is clearly expressible by the sum of

$$\beta_1 = \alpha^2 - \alpha + 1 = (20 + 8\sqrt{5} + 3\sqrt{10\sqrt{5} + 14} + \sqrt{50\sqrt{5} + 70})/8$$

and

$$\beta_2 = \alpha - 1 = (1 + \sqrt{5} + \sqrt{10\sqrt{5} + 14})/4.$$

The numbers β_1 (the root of $x^4 - 10x^3 + 12x^2 - 5x + 1 = 0$) and β_2 (the root of $x^4 - x^3 - 2x^2 - 2x - 1 = 0$) are Pisot numbers.

A difference set

Theorem

For any Salem number α, there exist infinitely many positive integers n such that $\alpha + \alpha^n$ is a Pisot number. In particular, every Salem number is expressible by a difference of a Pisot number and a Salem number.

The above theorem implies that

$$\mathcal{S} \subset \mathcal{P} - \mathcal{S}.$$

Therefore, every Salem number is a difference of two Mahler measures.

A more recent result

Recently, in

- A. Dubickas, *Mahler measures of Pisot and Salem type numbers,* Quaestiones Mathematicae **45** (2022), 1449–1458

I came back to these questions. Let

$$U := \{\alpha \in \overline{\mathbb{Q}} | \alpha > 1 \quad \text{with all conjugates} \neq \alpha \text{ over } \mathbb{Q} \text{ in } \quad |z| \leq 1\}.$$

The set U consists of $\mathcal{P} \cup \mathcal{S}$ and of all algebraic numbers which are not algebraic integers but have the same restriction on their conjugates as Pisot and Salem numbers have. Sometimes they are called generalized Pisot numbers and extended Salem numbers.

A more recent result

The set of Mahler measures of algebraic numbers from the set U will be denoted by $\mathfrak{M}$. (Each element of $\mathfrak{M}$ is the product of an element from U and a positive integer.) It is clear that

$$\mathcal{P} \cup \mathcal{S} \subset \mathfrak{M} \subset \mathcal{M} \subset [1, +\infty) \cap \overline{\mathbb{Q}}.$$

In an earlier paper (Drungilas and Dubickas), it was proved that for each real algebraic integer α there is $m \in \mathbb{N}$ such that

$$\alpha \in m\mathfrak{M} - \mathfrak{M}, \tag{1}$$

and that one can choose $m = 1$ for any α of degree $d \leq 3$.

A more recent result

Theorem

For every real quadratic algebraic integer α there are infinitely many Pisot numbers $\theta \in \mathbb{Q}(\alpha)$ such that $\alpha + \theta \in \mathfrak{M}$.

For $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{D})$, (infinitely many) Pisot numbers θ in the proof are chosen of the form $\lfloor n\sqrt{D} \rfloor + n\sqrt{D}$ with appropriate $n \in \mathbb{N}$. A key lemma in its proof:

Lemma

Let $a, b \in \mathbb{Z}$, and let $D > 1$ be a square free integer. Then, for each $Q = k^2 - D$, where $k > \sqrt{D}$ is an integer of parity different from that of D, there is an integer q in the range $0 \leq q < Q$ and infinitely many $m \in \mathbb{N}$ for which Q divides

$$(a + 2\lfloor (Qm + q)\sqrt{D} \rfloor)^2 - D(b + 2(Qm + q))^2.$$

Implication

The above theorem implies that all real quadratic algebraic integers lie in $\mathfrak{M} - \mathcal{P}$. It is not clear whether this is still the case for any real algebraic integer.

However, not every real algebraic integer α of belongs $\mathcal{P} - \mathcal{P}$, $\mathcal{P} - \mathcal{S}$, $\mathcal{S} - \mathcal{P}$ or $\mathcal{S} - \mathcal{S}$.

A more recent result

This follows from the next theorem:

Theorem

Let be $\alpha > 2$ be a real algebraic number of degree $d \geq 2$ whose other real and nonreal conjugates over $\mathbb{Q}$ all lie in the strip

$$2 < \Re(z) < \alpha.$$

Then, α is not in $U - U$.

Latest published result on this

Latest published paper on this:

- A. Dubickas, *Every Salem number is a difference of two Pisot numbers*, Proc. Edinburgh Math. Soc. **66** (2023), 862–867.

The title of the paper says that

Theorem

Every Salem number is expressible as a difference of two Pisot numbers.

In terms of difference sets, this means that

$$\mathcal{S} \subset \mathcal{P} - \mathcal{P}.$$

Latest published result on this

More explicitly, we show that

Theorem

For each Salem number α of degree $d \geq 4$ there exist infinitely many $n \in \mathbb{N}$ for which $\alpha^{2n-1} - \alpha^n + \alpha$ and $\alpha^{2n-1} - \alpha^n$ are both Pisot numbers of degree d. The smallest such n is at most $6^{d/2-1} + 1$.

Latest published result on this

Salem himself proved that every Salem number is expressible as a quotient of two Pisot numbers. On the other hand, by one of the abovemention every positive algebraic number is a quotient of two Mahler measures. The next theorem generalizes both these results:

Theorem

Every real positive algebraic number α of degree d is expressible as a quotient of two Pisot numbers of degree d from the field $\mathbb{Q}(\alpha)$.

It follows that

$$\frac{\mathcal{P}}{\mathcal{P}} = \overline{\mathbb{Q}} \cap (0, \infty).$$

A simple lemma

Lemma

Let α be a real algebraic number of degree $d \geq 2$ with conjugates $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_d$ over $\mathbb{Q}$, and let f be a nonconstant polynomial with rational coefficients such that $f(\alpha) > 0$ and $|f(\alpha_j)| < 1$ for $j = 2, \ldots, d$. If $f(\alpha) \in \mathbb{Q}(\alpha)$ is an algebraic integer, then it is a Pisot number of degree d.

Proof of the theorem

Let α be a positive algebraic number of degree d over $\mathbb{Q}$ with conjugates $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_d$. The claim is trivial for $d = 1$, since every integer $k \geq 2$ is a Pisot number and every positive rational number is a quotient of two such numbers. Assume that $d \geq 2$, and let m be a positive integer for which $m\alpha$ is an algebraic integer.

Fix a positive number $u < 1$ satisfying

$$mu \max(1, |\alpha_2|, \ldots, |\alpha_d|) < 1, \tag{2}$$

and a positive number $v > 1$ satisfying

$$mv\alpha > 1. \tag{3}$$

Proof of the theorem: continuation

Select a Pisot number $\beta \in \mathbb{Q}(\alpha)$ of degree d (this is always possible). A natural power of β is also a Pisot number of degree d, so by replacing β by its large power if necessary, we can assume that $\beta > v$ and that the other $d-1$ conjugates of β over $\mathbb{Q}$ are all in $|z| < u$.

Write this β in the form $\beta = f(\alpha)$, where $f \in \mathbb{Q}[x]$ is a nonconstant polynomial of degree at most $d-1$. Then, the numbers $\beta_j = f(\alpha_j)$, $j = 1, \dots, d$, are the conjugates of $\beta = \beta_1$ over $\mathbb{Q}$. Recall that, by the choice of β, we have

$$\beta = f(\alpha) > v \quad \text{and} \quad |\beta_j| = |f(\alpha_j)| < u \quad \text{for} \quad j = 2, \dots, d.$$

Proof of the theorem: continuation

We claim that under assumption on the constants $u \in (0,1)$ as in (2) and $v > 1$ as in (3), the numbers $m\alpha\beta \in \mathbb{Q}(\alpha)$ and $m\beta \in \mathbb{Q}(\alpha)$ are both Pisot numbers of degree d. This will complete our proof, since their quotient is α.

Firstly, $m\beta$ is a Pisot number, since it is an algebraic integer greater than $m > 1$, whose other conjugates $m\beta_j$, $j = 2, \ldots, d$, all lie in $|z| < 1$ by $|\beta_j| < u$ and (2) (which implies $mu < 1$). Of course, $m\beta \in \mathbb{Q}(\alpha)$ is of degree d over $\mathbb{Q}$, since so is β.

Proof of the theorem: continuation

Secondly, the number $m\alpha\beta = m\alpha f(\alpha) \in \mathbb{Q}(\alpha)$ is a positive algebraic integer, since so are $m\alpha$ and β. It is greater than 1 by $\beta > v$ and (3). Its other conjugates are

$$m\alpha_j f(\alpha_j) = m\alpha_j \beta_j,$$

$j = 2, \ldots, d$. They are all in $|z| < 1$ due to $|\beta_j| < u$ and (2). Hence, $m\alpha f(\alpha) \in \mathbb{Q}(\alpha)$ is a Pisot number of degree d over $\mathbb{Q}$ by the lemma applied to the polynomial $mxf(x) \in \mathbb{Q}[x]$.

Therefore, $m\alpha\beta \in \mathbb{Q}(\alpha)$ and $m\beta \in \mathbb{Q}(\alpha)$ indeed are both Pisot numbers of degree d, which finishes the proof.