Canad. Math. Bull. Vol. **50** (2), 2007 pp. 191–195

Every Real Algebraic Integer Is a Difference of Two Mahler Measures

Paulius Drungilas and Artūras Dubickas

Abstract. We prove that every real algebraic integer α is expressible by a difference of two Mahler measures of integer polynomials. Moreover, these polynomials can be chosen in such a way that they both have the same degree as that of α, say d, one of these two polynomials is irreducible and another has an irreducible factor of degree d, so that $\alpha = M(P) - bM(Q)$ with irreducible polynomials $P, Q \in \mathbb{Z}[X]$ of degree d and a positive integer b. Finally, if $d \leqslant 3$, then one can take $b = 1$.

1 Introduction

Let β be an algebraic number of degree d over the field of rational numbers $\mathbb{Q}$ with minimal polynomial $b_d X^d + \cdots + b_1 X + b_0 = b_d(X - \beta_1)\cdots(X - \beta_d) \in \mathbb{Z}[X]$. Its *Mahler measure* is defined by $M(\beta) = b_d \prod_{j=1}^{d} \max\{1, |\beta_j|\}$. It is well known that $M(\beta)$ is a real algebraic integer greater than or equal to 1 (see [1]). Likewise, the Mahler measure of $R(X) = b_d(X - \beta_1)\cdots(X - \beta_d) \in \mathbb{C}[X]$, where the numbers $\beta_i \in \mathbb{C}$ are not necessarily distinct, is defined by $M(R) = |b_d| \prod_{j=1}^{d} \max\{1, |\beta_j|\}$. Clearly, $M(RT) = M(R)M(T)$ for any polynomials $R, T \in \mathbb{C}[X]$, but the numbers $M(\beta\gamma)$ and $M(\beta)M(\gamma)$, where $\beta, \gamma \in \overline{\mathbb{Q}}$, are not necessarily equal.

Let $\mathcal{M}$ be the set of all Mahler measures of algebraic numbers, and let $\mathcal{M}^*$ be a monoid under multiplication generated by $\mathcal{M}$. By the multiplicative property of Mahler measures, $\mathcal{M}^*$ is the set of all Mahler measures of integer polynomials. Throughout, we say that α is a *Mahler measure* if $\alpha \in \mathcal{M}$. (Sometimes α is called a measure if $\alpha \in \mathcal{M}^*$, but these definitions define different sets, because $\mathcal{M} \neq \mathcal{M}^*$ [6].) Generally speaking, the structure of the sets $\mathcal{M}$ and $\mathcal{M}^*$ is not known, although the elements of $\mathcal{M}^*$ (and so of $\mathcal{M}$ too) must satisfy several necessary conditions (see [1, 3–8]).

The question whether an algebraic integer is in $\mathcal{M}^*$ or not was answered in [6]. It was proved there that if $\alpha \in \mathcal{M}^*$, then $\alpha = M(F)$ for some separable polynomial $F(X) \in \mathbb{Z}[X]$ of degree bounded by a function in $d = \deg \alpha$ only. Therefore, one can determine whether α belongs to $\mathcal{M}^*$ or not by a finite computation. However, no method is known to decide on whether a given algebraic integer α is in $\mathcal{M}$. The question remains open even for α of degree two, say for $\alpha = 1 + \sqrt{17}$. In this direction, Schinzel [16] obtained partial results for quadratic α, whereas the second named author [10] studied a corresponding question for cubic algebraic integers α.

Received by the editors February 18, 2005; revised February 17, 2006.
This research was partially supported by the Lithuanian State Science and Studies Foundation.
AMS subject classification: 11R04, 11R06, 11R09, 11R33, 11D09.
Keywords: Mahler measures, Pisot numbers, Pell equation, *abc*-conjecture.
©Canadian Mathematical Society 2007.

https://doi.org/10.4153/CMB-2007-020-0 Published online by Cambridge University Press

(See also [1,3–9] for other partial results concerning Mahler measures and the review paper [11].)

Although the structure of the sets $\mathcal{M}$ and $\mathcal{M}^*$ is not known, some derived sets are quite simple. The second named author proved in [9] that every positive algebraic number α can be written as a quotient of two elements of $\mathcal{M}$, so the smallest multiplicative group containing $\mathcal{M}$ is the multiplicative group of all positive algebraic numbers. Furthermore, it is shown in [9] that every real algebraic integer can be written as a linear form in four elements of $\mathcal{M}$ with integer coefficients: $\alpha = bM(\beta) + cM(\gamma) - bM(\beta') - cM(\gamma')$, where $\beta, \gamma, \beta', \gamma' \in \mathbb{Q}(\alpha)$ and $b, c \in \mathbb{N}$. Since $gM(\eta) \in \mathcal{M}^*$ for any $g \in \mathbb{N}$ and $\eta \in \overline{\mathbb{Q}}$, the set of measures $\mathcal{M}^*$ forms an additive basis of order at most 4 for the ring of integers of real algebraic numbers. (The set U is said to be an additive basis of order ℓ of the set V if each element of V can be written as $\pm u_1 \pm \cdots \pm u_t$, where $u_1, \ldots, u_t \in U$, $t \leqslant \ell$, and where ℓ is the smallest positive integer with this property.) In connection with this, we asked in [9] whether every algebraic integer α can be expressed by a difference of two Mahler measures. The next theorem implies that this order is equal to 2 and partially answers the above question.

Theorem 1 *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 $d \leqslant 3$ then both P and Q can be chosen to be irreducible.*

Theorem 1 implies that every real algebraic integer is expressible in the form $\widetilde{m} - m^*$ with $\widetilde{m} \in \mathcal{M}$ and $m^* \in \mathcal{M}^*$. Since $bM(T) = M(bT) \in \mathcal{M}^*$ for $b \in \mathbb{N}$ and $T \in \mathbb{Z}[X]$, Theorem 1 follows from the next result which is even more precise.

Theorem 2 *Suppose that α is a real algebraic integer of degree d. Then there exist two generalized Pisot numbers $\beta, \gamma \in \mathbb{Q}(\alpha)$ of degree d and a positive integer b such that $\alpha = M(\beta) - bM(\gamma)$. Furthermore, if $d \leqslant 3$ then we can choose $b = 1$, so that α can be expressed by a difference of two Mahler measures.*

Recall that $\alpha > 1$ is called a *Pisot number* if it is an algebraic integer whose other conjugates all lie strictly inside the unit circle. As in [9] (see also [12]) we call $\alpha > 1$ a *generalized Pisot number* if it satisfies the above definition but without assumption that α is an algebraic integer. Finally, following [13] an algebraic integer is called an *ε-Pisot number,* where $0 < \varepsilon \leqslant 1$, if its conjugates have absolute value less than ε, so that the usual Pisot numbers correspond to 1-Pisot numbers.

It is well known that in every real algebraic number field of degree d, there exist ε-Pisot numbers of degree d. One can take, for instance, a sufficiently large natural power of an arbitrary Pisot number lying in a real algebraic number field. (See [15, p. 3] or [13, Theorem 1.4] for a more subtle statement.) This fact will be used several times in the proof of Theorem 2.

https://doi.org/10.4153/CMB-2007-020-0 Published online by Cambridge University Press

2 Proof of Theorem 2

Let α be a real algebraic integer of degree d, where $d \geqslant 2$, with conjugates $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_d$, $\overline{|\alpha|} := \max_{1 \leqslant j \leqslant d} |\alpha_j| \geqslant 1$ and $N := |\operatorname{Norm}(\alpha)| \in \mathbb{N}$. Here, as usual, $\operatorname{Norm}(\alpha)$ denotes the product of conjugates of α. Fix $\varepsilon > 0$ (which is a small number to be defined later). Take an ε-Pisot number $\theta > 1$ of degree d in $\mathbb{Q}(\alpha)$. This means that its other algebraic conjugates $\theta_i \in \mathbb{Q}(\alpha_i)$, $i = 2, \ldots, d$, satisfy $|\theta_i| < \varepsilon$. Set

$$n := 1 + Nm^{d-1}, \quad b := (n^{d-1} - 1)/m^{d-1} = N(n^{d-2} + \cdots + n + 1),$$
$$\beta := \alpha/n + m(n^{d-1} - 1)\theta, \quad \gamma := \alpha/m + n^d\theta,$$

where m is a positive integer satisfying $m > 2\overline{|\alpha|}$ and $\gcd(m, N) = 1$. Clearly, $n > m$. With this choice of m, n, β and γ, we obtain that $\beta, \gamma \in \mathbb{Q}(\alpha)$ are generalized Pisot numbers if $\varepsilon < 1/(2n^d)$, because then $\beta, \gamma > 1$ (even if α is negative), and $|\beta_i|, |\gamma_i| < 1$ for each $i \geqslant 2$, because $|\theta_i| < \varepsilon < 1/(2n^d)$. Moreover, $\beta = F(\alpha)$, where $F(x) \in \mathbb{Q}[x]$, is of degree d, because otherwise we would have that $\beta = F(\alpha) = F(\alpha_i) = \beta_i$ for some $i \geqslant 2$, which is not the case, because $\beta > 1 > |\beta_i|$ for any $i \geqslant 2$. So both β and, by the same argument, γ are generalized Pisot numbers of degree d.

Next, by the choice of n, we deduce that $\gcd(n, \operatorname{Norm}(\alpha)) = 1$. It follows that $\gcd(n, \operatorname{Norm}(\alpha + m(n^d - n)\theta)) = 1$. Thus the leading coefficient of the minimal polynomial of β equals n^d and $M(\beta) = n^{d-1}(\alpha + m(n^d - n)\theta)$. Likewise, $\gcd(m, \operatorname{Norm}(\alpha)) = 1$ implies that $\gcd(m, \operatorname{Norm}(\alpha + mn^d\theta)) = 1$, so the leading coefficient of the minimal polynomial of γ equals m^d and $M(\gamma) = m^{d-1}(\alpha + n^d m\theta)$. It follows that

$$M(\beta) - bM(\gamma) = n^{d-1}(\alpha + m(n^d - n)\theta) - \frac{n^{d-1} - 1}{m^{d-1}} m^{d-1}(\alpha + n^d m\theta) = \alpha.$$

This proves the first part of the theorem for $d \geqslant 2$. The proof for $d = 1$ is trivial. Indeed, then α is a rational integer. For $\alpha \geqslant 0$, we have $\alpha = M(\alpha + 1) - M(1)$, whereas, for $\alpha < 0$, $\alpha = M(1) - M(\alpha - 1)$. This completes the proof of the first part of the theorem and proves the second part for $d = 1$.

Consider the case $d = 2$. Take a positive integer u and a real number $\varepsilon > 0$ such that $u > 2N\overline{|\alpha|}$, $\gcd(u, N) = 1$ and $\varepsilon < (2(Nu + 1)^2)^{-1}$. Now, choose an ε-Pisot number $\theta \in \mathbb{Q}(\alpha)$ of degree $d = 2$. Then the numbers $\beta = \alpha/(Nu+1) + u^2\theta \in \mathbb{Q}(\alpha)$ and $\gamma = N\alpha/u + (Nu + 1)^2\theta \in \mathbb{Q}(\alpha)$ are generalized quadratic Pisot numbers. Using $\gcd(u, N) = 1$, we deduce as above that the leading coefficient of the minimal polynomial of γ equals u^2. Thus $M(\gamma) = Nu\alpha + u^2(Nu + 1)^2\theta$. Similarly, the leading coefficient of the minimal polynomial of β is equal to $(Nu + 1)^2$. It follows that $M(\beta) = (Nu + 1)\alpha + u^2(Nu + 1)^2\theta$, giving $\alpha = M(\beta) - M(\gamma)$.

Finally, suppose that $d = 3$. Consider the Pell equation $x^2 - N(N + 2)y^2 = 1$, where $N = |\operatorname{Norm}(\alpha)|$. (See, for instance, [2] for an introduction to this equation.) Since $x_1 = N + 1$, $y_1 = 1$ is the minimal solution of this Pell equation, its other solutions x_k, y_k in positive integers are obtained from the equality

$$x_k + y_k\sqrt{N(N + 2)} := (N + 1 + \sqrt{N(N + 2)})^k.$$

https://doi.org/10.4153/CMB-2007-020-0 Published online by Cambridge University Press

Now, take a positive integer k and a real number $\varepsilon > 0$ (to be chosen later) such that $\gcd(k, N(N+2)) = 1$ and $y_k > 2N(N+2)\overline{|\alpha|}$. Once again there exists a cubic ε-Pisot number $\theta \in \mathbb{Q}(\alpha)$. Then the numbers $\beta = \alpha/x_k + y_k^3\theta \in \mathbb{Q}(\alpha)$ and $\gamma = N(N+2)\alpha/y_k + x_k^3\theta \in \mathbb{Q}(\alpha)$ are generalized cubic Pisot numbers provided that $\varepsilon < (2x_k^3)^{-1}$. On the other hand, it is easy to see that the numbers $x_k - (N+1)^k$ and $y_k - k(N+1)^{k-1}$ are divisible by $N(N+2)$. In particular, N divides $x_k - 1$, so $\gcd(x_k, N) = 1$. Moreover, by the choice of k, we have $\gcd(k(N+1)^{k-1}, N(N+2)) = 1$, so $\gcd(y_k, N(N+2)) = 1$. Hence the leading coefficients of the minimal polynomials of β and γ are x_k^3 and y_k^3, respectively. Thus $M(\beta) = x_k^2\alpha + x_k^3y_k^3\theta$ and $M(\gamma) = N(N+2)y_k^2\alpha + x_k^3y_k^3\theta$. This yields $M(\beta) - M(\gamma) = (x_k^2 - N(N+2)y_k^2)\alpha = \alpha$. The proof of Theorem 2 is now complete.

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. 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 little hope that this statement holds for any $d > 4$. The point is that, for $d > 4$, it contradicts to the well-known *abc*-conjecture. (See, for instance, [14].) Indeed, suppose that there are $a, b, x, y \in \mathbb{N}$ satisfying $ax^{d-1} - by^{d-1} = 1$ and other conditions as above. Then the *abc*-conjecture implies that $by^{d-1} < ax^{d-1} < C_\epsilon(\prod_{p|abxy} p)^{1+\epsilon} \leq C_\epsilon(abxy)^{1+\epsilon}$, where $\epsilon > 0$ and where C_ϵ is a constant depending on ϵ only. Consequently, $(xy)^{d-3-2\epsilon} < C_\epsilon^2(ab)^{1+2\epsilon}$. Hence, for $x > la$ and $y > lb$, we deduce that $l^{2d-6-4\epsilon} < C_\epsilon^2(ab)^{4-d+4\epsilon}$ which is impossible for l sufficiently large if $d \geqslant 5$ and $\epsilon < 1/4$.

Acknowledgements We thank Michael Bennett for pointing out the connection with the *abc*-conjecture.

References

[1] R. L. Adler and B. Marcus, *Topological entropy and equivalence of dynamical systems.* Mem. Amer. Math. Soc. **20**(1979), no. 219.
[2] E. J. Barbeau, *Pell's equation.* Springer-Verlag, New York, 2003.
[3] D. W. Boyd, *Inverse problems for Mahler's measure.* In: Diophantine Analysis. London Math. Soc. Lecture Note Ser. 109, Cambridge University Press, Cambridge, 1986, pp. 147–158.
[4] ———, *Perron units which are not Mahler measures.* Ergodic Theory Dynam. Systems **6**(1986), no. 4, 485–488.
[5] ———, *Reciprocal algebraic integers whose Mahler measures are non-reciprocal.* Canad. Math. Bull. **30**(1987), no. 1, 3–8.
[6] J. D. Dixon and A. Dubickas, *The values of Mahler measures.* Mathematika **51**(2004), no. 1-2, 131–148.
[7] A. Dubickas, *Mahler measures close to an integer.* Canad. Math. Bull. **45**(2002), no. 2, 196–203.
[8] ———, *On numbers which are Mahler measures.* Monatsh. Math. **141**(2004), no. 2, 119–126.
[9] ———, *Mahler measures generate the largest possible groups.* Math. Res. Lett. **11**(2004), no. 2-3, 279–283.
[10] ———, *Mahler measures in a cubic field.* Czechoslovak Math. J. **56**(2006), no. 3, 949–956.
[11] ———, *Algebraic, arithmetic and geometric properties of Mahler measures.* Proc. Inst. Math. (Nat. Acad. Sc. Belarus) **13**(2005), 70–74.

https://doi.org/10.4153/CMB-2007-020-0 Published online by Cambridge University Press

[12] 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. **44**(2001), no. 1, 1–17.
[13] A.-H. Fan and J. Schmeling, *ε-Pisot numbers in any real algebraic number field are relatively dense.* J. Algebra **272**(2004), no. 2, 470–475.
[14] A. Granville and T. J. Tucker, *It's as easy as abc.* Notices Amer. Math. Soc. **49**(2002), no. 10, 1224–1231.
[15] R. Salem, *Algebraic numbers and Fourier analysis.* D. C. Heath, Boston, MA, 1963.
[16] A. Schinzel, *On values of the Mahler measure in quadratic field (solution of a problem of Dixon and Dubickas).* Acta Arith. **113**(2004), no. 4, 401–408.

Department of Mathematics and Informatics
Vilnius University
Naugarduko 24
LT-03225 Vilnius
and
Institute of Mathematics and Informatics
Akademijos 4
LT-08663 Vilnius
Lithuania
e-mail: pdrungilas@gmail.com

Department of Mathematics and Informatics
Vilnius University
Naugarduko 24
LT-03225 Vilnius
Lithuania
e-mail: arturas.dubickas@maf.vu.lt

https://doi.org/10.4153/CMB-2007-020-0 Published online by Cambridge University Press