Canad. Math. Bull. Vol. **54** (4), 2011 pp. 739–747
doi:10.4153/CMB-2011-028-x

The Infimum in the Metric Mahler Measure

Charles L. Samuels

Abstract. Dubickas and Smyth defined the metric Mahler measure on the multiplicative group of non-zero algebraic numbers. The definition involves taking an infimum over representations of an algebraic number α by other algebraic numbers. We verify their conjecture that the infimum in its definition is always achieved, and we establish its analog for the ultrametric Mahler measure.

1 Introduction

Let K be a number field, and let v be a place of K dividing the place p of $\mathbb{Q}$. Let K_v and $\mathbb{Q}_p$ denote the respective completions. We write $\|\cdot\|_v$ for the unique absolute value on K_v extending the p-adic absolute value on $\mathbb{Q}_p$ and define

$$|\alpha|_v = \|\alpha\|_v^{[K_v:\mathbb{Q}_p]/[K:\mathbb{Q}]}$$

for all $\alpha \in K$. Define the *Weil height* of $\alpha \in K$ by

$$H(\alpha) = \prod_v \max\{1, |\alpha|_v\},$$

where the product is taken over all places v of K. Given this normalization of our absolute values, the above definition does not depend on K, and therefore, H is a well-defined function on $\overline{\mathbb{Q}}$. Clearly $H(\alpha) \geq 1$, and by Kronecker's Theorem, we have equality precisely when α is zero or a root of unity. It is obvious that if ζ is a root of unity, then

$$H(\alpha) = H(\zeta\alpha), \tag{1.1}$$

and further, if n is an integer then it is well known that

$$H(\alpha^n) = H(\alpha)^{|n|}. \tag{1.2}$$

Also, if $\alpha, \beta \in \overline{\mathbb{Q}}^\times$, then $H(\alpha\beta) \leq H(\alpha)H(\beta)$.

We further define the *Mahler measure* of an algebraic number α by $M(\alpha) = H(\alpha)^{[\mathbb{Q}(\alpha):\mathbb{Q}]}$. Since H is invariant under Galois conjugation over $\mathbb{Q}$, we obtain immediately $M(\alpha) = \prod_{n=1}^N H(\alpha_n)$, where $\alpha_1, \dots, \alpha_N$ are the conjugates of α over $\mathbb{Q}$. Further, it is well known that

$$M(\alpha) = |A| \cdot \prod_{n=1}^N \max\{1, |\alpha_n|\}, \tag{1.3}$$

Received by the editors October 18, 2008; revised December 29, 2008.
Published electronically March 5, 2011.
This research was carried out while the author was a visiting scientist at the Max-Planck-Institut für Mathematik in Bonn, Germany.
AMS subject classification: **11R04**, 11R09.
Keywords: Weil height, Mahler measure, metric Mahler measure, Lehmer's problem.

where $|\cdot|$ denotes the usual absolute value on $\mathbb{C}$. While the right hand side of (1.3) appears initially to depend upon a particular embedding of $\overline{\mathbb{Q}}$ into $\mathbb{C}$, any change of embedding simply permutes the images of the points $\{\alpha_n\}$ so that (1.3) remains unchanged.

It follows, again from Kronecker's Theorem, that $M(\alpha) = 1$ if and only if α is zero or a root of unity. As part of an algorithm for computing large primes, D. H. Lehmer ([5]) asked whether there exists a constant $c > 1$ such that $M(\alpha) \geq c$ in all other cases. The smallest known Mahler measure greater than 1 occurs at a root of

$$\ell(x) = x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1,$$

which has Mahler measure $1.17\cdots$. Although an affirmative answer to Lehmer's problem has been given in many special cases, the general case remains open. The best known universal lower bound on $M(\alpha)$ is due to Dobrowolski ([1]), who proved that

$$\log M(\alpha) \gg \Big(\frac{\log\log\deg\alpha}{\log\deg\alpha}\Big)^3$$

whenever α is not a root of unity.

Recently, Dubickas, and Smyth ([2]) defined the *metric Mahler measure* of an algebraic number α by

$$M_1(\alpha) = \inf\Big\{\prod_{n=1}^{N} M(\alpha_n) : N \in \mathbb{N},\ \alpha_n \in \overline{\mathbb{Q}}^\times,\ \alpha = \prod_{n=1}^{N}\alpha_n\Big\}. \tag{1.4}$$

Here, the infimum is taken over all ways to represent α as a product of elements in $\overline{\mathbb{Q}}^\times$. It is easily verified that $M_1(\alpha\beta) \leq M_1(\alpha)M_1(\beta)$ for all $\alpha, \beta \in \overline{\mathbb{Q}}^\times$, and further, M_1 is well defined on the quotient group $\mathcal{G} = \overline{\mathbb{Q}}^\times / \operatorname{Tor}(\overline{\mathbb{Q}}^\times)$. This implies that the map $(\alpha, \beta) \mapsto \log M_1(\alpha\beta^{-1})$ defines a metric on $\mathcal{G}$ that induces the discrete topology if and only if there is an affirmative answer to Lehmer's problem.

Also in [2], Dubickas and Smyth conjecture that the infimum in the definition of M_1 is always achieved. We verify this conjecture as well as explicitly determine a set in which the infimum must occur.

If K is any number field, let

$$\operatorname{Rad}(K) = \big\{\alpha \in \overline{\mathbb{Q}} : \alpha^r \in K \text{ for some } r \in \mathbb{N}\big\},$$

the set of all roots of points in K. Also, we write K_α for the Galois closure of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$.

Theorem 1.1 *If α is a non-zero algebraic number, then there exist $\alpha_1, \ldots, \alpha_N \in \operatorname{Rad}(K_\alpha)$ such that $\alpha = \alpha_1 \cdots \alpha_N$ and $M_1(\alpha) = M(\alpha_1)\cdots M(\alpha_N)$.*

Motivated by the work of Dubickas and Smyth, Fili and the author ([4]) defined a non-Archimedean version of M_1 by replacing the product in (1.4) by a maximum. That is, define the *ultrametric Mahler measure* by

$$M_\infty(\alpha) = \inf\Big\{\max_{1\leq n\leq N} M(\alpha_n) : N \in \mathbb{N},\ \alpha_n \in \overline{\mathbb{Q}}^\times,\ \alpha = \prod_{n=1}^{N}\alpha_n\Big\}.$$

https://doi.org/10.4153/CMB-2011-028-x Published online by Cambridge University Press

It easily verified that M_∞ satisfies the strong triangle inequality

$$M_\infty(\alpha\beta) \le \max\{M_\infty(\alpha), M_\infty(\beta)\}$$

for all non-zero algebraic numbers α and β. It is further shown in [4] that M_∞ is well defined on the quotient group $\mathcal{G}$. We can now establish the obvious analog of Theorem 1.1 for M_∞.

Theorem 1.2 *If α is a non-zero algebraic number, then there exist $\alpha_1, \dots, \alpha_N \in \mathrm{Rad}(K_\alpha)$ such that $\alpha = \alpha_1 \cdots \alpha_N$ and $M_\infty(\alpha) = \max\{M(\alpha_1), \dots, M(\alpha_N)\}$.*

The remainder of this paper is organized in the following way. Section 2 contains the core of our argument in which we show that computing $M_1(\alpha)$ and $M_\infty(\alpha)$ requires only the use of elements in $\mathrm{Rad}(K_\alpha)$. In Section 3, we finish the proofs of Theorems 1.1 and 1.2 by showing, essentially, that there are only finitely many values for the Mahler measure in $\mathrm{Rad}(K_\alpha)$. Finally, Section 4 contains some applications of these results, giving the location of the algebraic numbers $M_1(\alpha)$ and $M_\infty(\alpha)$.

2 Reducing to Simpler Representations

The main idea in both proofs involves a method for replacing an arbitrary representation of α by a potentially smaller representation containing only points in $\mathrm{Rad}(K_\alpha)$. This technique is summarized by the following result.

Theorem 2.1 *If $\alpha, \alpha_1, \dots, \alpha_N$ are non-zero algebraic numbers with $\alpha = \alpha_1 \cdots \alpha_N$, then there exists a root of unity ζ and algebraic numbers $\beta_1, \dots, \beta_N$ satisfying*

(i) $\alpha = \zeta\beta_1 \cdots \beta_N$,
(ii) $\beta_n \in \mathrm{Rad}(K_\alpha)$ *for all n,*
(iii) $M(\beta_n) \le M(\alpha_n)$ *for all n.*

The proof of Theorem 2.1 is based on the following lemma.

Lemma 2.2 *Suppose that K is Galois over $\mathbb{Q}$. If γ is an algebraic number, then*

$$[K(\gamma) : K] = [\mathbb{Q}(\gamma) : K \cap \mathbb{Q}(\gamma)]. \tag{2.1}$$

Moreover, we have that $\prod_{n=1}^{N} \gamma_n \in K \cap \mathbb{Q}(\gamma)$, where $\gamma_1, \dots, \gamma_N$ are the conjugates of γ over K.

Proof We see clearly that $K(\gamma)$ is the compositum of K and $\mathbb{Q}(\gamma)$. Since K is Galois over $\mathbb{Q}$, it follows (see [3, p. 505, Prop. 19]) that $[K(\gamma) : K] = [\mathbb{Q}(\gamma) : K \cap \mathbb{Q}(\gamma)]$, verifying (2.1). We also observe that

$$(K \cap \mathbb{Q}(\gamma))(\gamma) \subseteq (\mathbb{Q}(\gamma))(\gamma) = \mathbb{Q}(\gamma) \subseteq (K \cap \mathbb{Q}(\gamma))(\gamma),$$

so we conclude from (2.1) that

$$[K(\gamma) : K] = [(K \cap \mathbb{Q}(\gamma))(\gamma) : K \cap \mathbb{Q}(\gamma)]. \tag{2.2}$$

Let f be the monic minimal polynomial of γ over $K \cap \mathbb{Q}(\gamma)$ so that f has degree D equal to both sides of (2.2). Now write $f(x) = x^D + \cdots + a_1 x + a_0$ and note that f is, of course, a polynomial over K. In fact, f is the monic minimal polynomial of γ over K, because it vanishes at γ and has degree $[K(\gamma) : K]$. Since $\gamma_1, \ldots, \gamma_N$ are the conjugates of γ over K, we conclude that $\prod_{n=1}^N \gamma_n = \pm a_0$, which belongs to $K \cap \mathbb{Q}(\gamma)$. ■

It is worth observing that if $\mathbb{Q}(\gamma)$ is Galois over $\mathbb{Q}$, then Lemma 2.2 becomes trivial. Indeed, $\gamma_1 \cdots \gamma_N$ certainly belongs to K by definition. But also, if $\mathbb{Q}(\gamma)$ is Galois, then $\mathbb{Q}(\gamma)$ contains all conjugates of γ over $\mathbb{Q}$. In particular, it contains γ_n for all n, so it contains their product as well. Of course, the proof of Theorem 2.1 does not permit such a hypothesis, so we require the above lemma.

Additionally, we cannot omit the hypothesis that K be Galois over $\mathbb{Q}$. For example, let γ_1, γ_2, and γ_3 be the roots of a third degree, irreducible polynomial over $\mathbb{Q}$ having Galois group S_3. This means that $\mathbb{Q}(\gamma_1) \cap \mathbb{Q}(\gamma_2) = \mathbb{Q}$. Further, we observe that γ_2 must have degree 2 over $\mathbb{Q}(\gamma_1)$ implying that its conjugates over this field are γ_2 and γ_3. But if $\gamma_2 \cdot \gamma_3 \in \mathbb{Q}(\gamma_2)$, then $\gamma_1 \in \mathbb{Q}(\gamma_2)$, a contradiction.

Proof of Theorem 2.1 Suppose that $\alpha = \alpha_1 \cdots \alpha_N$, and let E be a Galois extension of K_α containing α_n for all n. Let $G = \mathrm{Gal}(E/K_\alpha)$, $G_n = \mathrm{Gal}(E/K_\alpha(\alpha_n))$ and S_n a set of left coset representatives of G_n in G. We have that

$$\alpha^{[E:K_\alpha]} = \mathrm{Norm}_{E/K_\alpha}(\alpha) = \prod_{n=1}^N \mathrm{Norm}_{E/K_\alpha}(\alpha_n) = \prod_{n=1}^N \prod_{\sigma \in G} \sigma(\alpha_n)$$
$$= \prod_{n=1}^N \prod_{\sigma \in S_n} \prod_{\tau \in G_n} \sigma(\tau(\alpha_n)) = \prod_{n=1}^N \prod_{\sigma \in S_n} \sigma(\alpha_n)^{|G_n|},$$

so we conclude that

$$\alpha^{[E:K_\alpha]} = \prod_{n=1}^N \Big(\prod_{\sigma \in S_n} \sigma(\alpha_n) \Big)^{[E:K_\alpha(\alpha_n)]}. \tag{2.3}$$

For each n, we select an element $\beta_n \in \overline{\mathbb{Q}}$ such that

$$\beta_n^{[K_\alpha(\alpha_n):K_\alpha]} = \prod_{\sigma \in S_n} \sigma(\alpha_n), \tag{2.4}$$

so that, in view of (2.3), we obtain $\alpha^{[E:K_\alpha]} = \prod_{n=1}^N \beta_n^{[E:K_\alpha]}$. This implies the existence of a root of unity ζ such that $\alpha = \zeta \beta_1 \cdots \beta_N$. Furthermore, the set $\{\sigma(\alpha_n) : \sigma \in S_n\}$ is precisely the set of conjugates of α_n over K_α so that $\prod_{\sigma \in S_n} \sigma(\alpha_n) \in K_\alpha$. It then follows from (2.4) that $\beta_n \in \mathrm{Rad}(K_\alpha)$ for each n as well.

It remains to show that $M(\beta_n) \le M(\alpha_n)$ for all n. To see this, we note that (2.4) yields immediately

$$\deg(\beta_n) \le [K_\alpha(\alpha_n) : K_\alpha] \cdot \deg\Big(\prod_{\sigma \in S_n} \sigma(\alpha_n) \Big). \tag{2.5}$$

https://doi.org/10.4153/CMB-2011-028-x Published online by Cambridge University Press

Once again, the elements $\sigma(\alpha_n)$ for $\sigma \in S_n$ are precisely the conjugates of α_n over K_α. Hence, we may apply Lemma 2.2 to find that

$$\prod_{\sigma \in S_n} \sigma(\alpha_n) \in K_\alpha \cap \mathbb{Q}(\alpha_n).$$

Combining this with (2.5), we obtain

$$\deg(\beta_n) \leq [K_\alpha(\alpha_n) : K_\alpha] \cdot [K_\alpha \cap \mathbb{Q}(\alpha_n) : \mathbb{Q}].$$

Then we find that

$$\begin{aligned} M(\beta_n) &\leq H(\beta_n)^{[K_\alpha(\alpha_n):K_\alpha]\cdot[K_\alpha \cap \mathbb{Q}(\alpha_n):\mathbb{Q}]} = H\Big(\prod_{\sigma \in S_n} \sigma(\alpha_n)\Big)^{[K_\alpha \cap \mathbb{Q}(\alpha_n):\mathbb{Q}]} \\ &\leq H(\alpha_n)^{[K_\alpha(\alpha_n):K_\alpha]\cdot[K_\alpha \cap \mathbb{Q}(\alpha_n):\mathbb{Q}]}, \end{aligned}$$

where the last inequality follows, since the Weil height is invariant under Galois conjugation and satisfies the triangle inequality. Also $K_\alpha(\alpha_n)$ is the compositum of K_α and $\mathbb{Q}(\alpha_n)$, so that $[K_\alpha(\alpha_n) : K_\alpha] = [\mathbb{Q}(\alpha_n) : K_\alpha \cap \mathbb{Q}(\alpha_n)]$ by (2.1). This yields

$$M(\beta_n) \leq H(\alpha_n)^{[\mathbb{Q}(\alpha_n):K_\alpha \cap \mathbb{Q}(\alpha_n)]\cdot[K_\alpha \cap \mathbb{Q}(\alpha_n):\mathbb{Q}]} = M(\alpha_n),$$

which completes the proof. ∎

3 Proofs of Theorems 1.1 and 1.2

In view of Theorem 2.1, it is enough, in the definitions of M_1 and M_∞, to consider only representations $\alpha = \alpha_1 \cdots \alpha_N$ having $\alpha_n \in \mathrm{Rad}(K_\alpha)$ for all n. Any representation that fails to have this property may simply be replaced by a smaller representation that does. The remainder of our proofs of both Theorem 1.1 and 1.2 require us to show that such representations yield only finitely many different values for $\max_{1 \leq n \leq N} M(\alpha_n)$ and $\prod_{n=1}^{N} M(\alpha_n)$. The following lemma provides the starting point for this argument.

Lemma 3.1 *Let K be a Galois extension of $\mathbb{Q}$. If $\gamma \in \mathrm{Rad}(K)$, then there exists a root of unity ζ and $L, S \in \mathbb{N}$ such that $\zeta\gamma^L \in K$ and $M(\gamma) = M(\zeta\gamma^L)^S$. In particular, the set $\{M(\gamma) : \gamma \in \mathrm{Rad}(K),\ M(\gamma) \leq B\}$ is finite for every $B \geq 1$.*

Proof Suppose that $\gamma^r \in K$, so that each conjugate of γ over K must be a root of $x^r - \gamma^r \in K[x]$. Therefore, we may assume that γ has conjugates $\zeta_1\gamma, \ldots, \zeta_L\gamma$ over K for some roots of unity $\zeta_1, \ldots, \zeta_L$. By Lemma 2.2 we conclude that

$$\zeta_1 \cdots \zeta_L \gamma^L = \zeta_1\gamma \cdots \zeta_L\gamma \in K \cap \mathbb{Q}(\gamma). \tag{3.1}$$

Since K is Galois, Lemma 2.2 also implies that $L = [K(\gamma) : K] = [\mathbb{Q}(\gamma) : K \cap \mathbb{Q}(\gamma)]$. Hence, we find that

$$M(\gamma) = H(\gamma)^{[\mathbb{Q}(\gamma):\mathbb{Q}]} = H(\gamma)^{[\mathbb{Q}(\gamma):K\cap\mathbb{Q}(\gamma)]\cdot[K\cap\mathbb{Q}(\gamma):\mathbb{Q}]} = H(\gamma)^{L\cdot[K\cap\mathbb{Q}(\gamma):\mathbb{Q}]}.$$

https://doi.org/10.4153/CMB-2011-028-x Published online by Cambridge University Press

Since L is a positive integer and $\zeta_1 \cdots \zeta_L$ is a root of unity, we conclude from (1.1) and (1.2) that

$$M(\gamma) = H(\zeta_1 \cdots \zeta_L \gamma^L)^{[K \cap \mathbb{Q}(\gamma):\mathbb{Q}]}. \tag{3.2}$$

By (3.1) we know that there exists a positive integer S such that

$$[K \cap \mathbb{Q}(\gamma) : \mathbb{Q}] = S \cdot [\mathbb{Q}(\zeta_1 \cdots \zeta_L \gamma^L) : \mathbb{Q}],$$

and so (3.2) yields

$$M(\gamma) = H(\zeta_1 \cdots \zeta_L \gamma^L)^{S \cdot [\mathbb{Q}(\zeta_1 \cdots \zeta_L \gamma^L):\mathbb{Q}]} = M(\zeta_1 \cdots \zeta_L \gamma^L)^S.$$

Taking $\zeta = \zeta_1 \cdots \zeta_L$, we have that $\zeta\gamma^L \in K$ by (3.1) and $M(\gamma) = M(\zeta\gamma^L)^S$, which establishes the first statement of the lemma.

Further, we note that (3.2) implies that $M(\gamma) = H((\zeta\gamma^L)^{[K \cap \mathbb{Q}(\gamma):\mathbb{Q}]})$, but $(\zeta\gamma^L)^{[K \cap \mathbb{Q}(\gamma):\mathbb{Q}]} \in K$, implying that

$$\{M(\gamma) : \gamma \in \mathrm{Rad}(K),\ M(\gamma) \leq B\} \subseteq \{H(\alpha) : \alpha \in K^{\times},\ H(\alpha) \leq B\}. \tag{3.3}$$

It follows from Northcott's Theorem ([6]) that the right-hand side of (3.3) is finite, completing the proof. ■

The proof of Theorem 1.2 is somewhat simpler than that of Theorem 1.1, so we include it here first.

Proof of Theorem 1.2 There exists $\varepsilon > 0$ such that if $\alpha = \alpha_1 \cdots \alpha_N$ with $\alpha_n \in \mathrm{Rad}(K_\alpha)$ and

$$M_\infty(\alpha) \leq \max\{M(\alpha_1), \dots, M(\alpha_N)\} \leq M_\infty(\alpha) + \varepsilon,$$

then $M_\infty(\alpha) = \max\{M(\alpha_1), \dots, M(\alpha_N)\}$. Otherwise, we get a sequence $\{x_m\} \subseteq \mathrm{Rad}(K_\alpha)$ such that $\{M(x_m)\}$ is strictly decreasing, contradicting Lemma 3.1.

By definition, there exists a representation $\alpha = \gamma_1 \cdots \gamma_N$ with

$$M_\infty(\alpha) \leq \max\{M(\gamma_1), \dots, M(\gamma_N)\} \leq M_\infty(\alpha) + \varepsilon.$$

By Theorem 2.1, there exists a representation $\alpha = \zeta\alpha_1 \cdots \alpha_N$ such that ζ is a root of unity, $\alpha_n \in \mathrm{Rad}(K_\alpha)$ and $M(\alpha_n) \leq M(\gamma_n)$ for all n. This yields

$$M_\infty(\alpha) \leq \max\{M(\alpha_1), \dots, M(\alpha_N)\} \leq M_\infty(\alpha) + \varepsilon,$$

so that $M_\infty(\alpha) = \max\{M(\alpha_1), \dots, M(\alpha_N)\}$ by our earlier remarks. ■

We note that the above proof is not sufficient to establish Theorem 1.1. Indeed, Lemma 3.1 does not prevent the product $M(\alpha_1) \cdots M(\alpha_N)$ from having infinitely many values between $M_1(\alpha)$ and $M_1(\alpha) + \varepsilon$ unless we can bound N uniformly from above by a function of α.

In order to do this, we introduce an additional definition. For $B \geq 1$, we say that a representation $\alpha = \alpha_1 \cdots \alpha_N$ is *B-restricted* if the following three conditions hold:

https://doi.org/10.4153/CMB-2011-028-x Published online by Cambridge University Press

(i) $M(\alpha_1)\cdots M(\alpha_N) \le B$,
(ii) $\alpha_n \in \mathrm{Rad}(K_\alpha)$ for all n,
(iii) At most one element α_n is a root of unity.

We write $R_B(\alpha)$ to denote the set of all N-tuples, for all $N \in \mathbb{N}$, of non-zero algebraic numbers that form B-restricted representations of α. Further, set

$$q(\alpha) = \inf\big\{ H(x) : x \in K_\alpha^\times \setminus \mathrm{Tor}(\overline{\mathbb{Q}}^\times)\big\}$$

and note that, by Northcott's Theorem ([6]), this quantity is always strictly greater than 1. Using these definitions, we obtain the result we need to finish the proof of Theorem 1.1.

Lemma 3.2 *Let α be a non-zero algebraic number and $B \ge 1$. If $\alpha = \alpha_1 \cdots \alpha_N$ is an B-restricted representation of α, then $N \le 1 + \frac{\log B}{\log q(\alpha)}$. Moreover, the set*

$$\Big\{ \prod_{n=1}^{N} M(\alpha_n) : N \in \mathbb{N},\ (\alpha_1, \dots, \alpha_N) \in R_B(\alpha)\Big\}$$

is finite.

Proof Suppose that $\alpha = \alpha_1 \cdots \alpha_N$ is a B-restricted representation. By assumption, at least $N-1$ of the terms α_n in our representation are not roots of unity. Assume α_n is one such element. Lemma 3.1 implies that there exists a point $\gamma_n \in K_\alpha$, not a root of unity, such that

$$M(\alpha_n) \ge H(\gamma_n).$$

Therefore, we find that $M(\alpha_n) \ge q(\alpha)$ for $N-1$ of the terms belonging to $\{\alpha_1, \dots, \alpha_N\}$. This yields

$$B \ge M(\alpha_1)\cdots M(\alpha_N) \ge q(\alpha)^{N-1}.$$

We know that $q(\alpha) > 1$, so that we may divide by $\log q(\alpha)$ to obtain $N \le 1 + \frac{\log B}{\log q(\alpha)}$, verifying the first statement of the lemma. We now find that

$$\begin{aligned}
&\Big\{ \prod_{n=1}^{N} M(\alpha_n) : N \in \mathbb{N}, (\alpha_1, \dots, \alpha_N) \in R_B(\alpha)\Big\} \\
&\quad = \Big\{ \prod_{n=1}^{N} M(\alpha_n) : (\alpha_1, \dots, \alpha_N) \in R_B(\alpha), N \le 1 + \frac{\log B}{\log q(\alpha)}\Big\} \\
&\quad \subseteq \Big\{ \prod_{n=1}^{N} M(\alpha_n) : N \le 1 + \frac{\log B}{\log q(\alpha)}, M(\alpha_n) \le B, \alpha_n \in \mathrm{Rad}(K_\alpha)\Big\},
\end{aligned}$$

which is finite by Lemma 3.1. ■

https://doi.org/10.4153/CMB-2011-028-x Published online by Cambridge University Press

Proof of Theorem 1.1 By Lemma 3.2, we may select $B > M_1(\alpha)$ such that

$$(M_1(\alpha), B) \cap \Big\{ \prod_{n=1}^{N} M(\alpha_n) : N \in \mathbb{N},\ (\alpha_1, \dots, \alpha_N) \in R_{M_1(\alpha)+1}(\alpha) \Big\} = \varnothing.$$

Of course, we may choose $B \le M_1(\alpha) + 1$, which gives

$$\Big\{ \prod_{n=1}^{N} M(\alpha_n) : N \in \mathbb{N}, (\alpha_1, \dots, \alpha_N) \in R_B(\alpha) \Big\} \subseteq \Big\{ \prod_{n=1}^{N} M(\alpha_n) : N \in \mathbb{N}, (\alpha_1, \dots, \alpha_N) \in R_{M_1(\alpha)+1}(\alpha) \Big\},$$

and therefore,

$$(M_1(\alpha), B) \cap \Big\{ \prod_{n=1}^{N} M(\alpha_n) : N \in \mathbb{N},\ (\alpha_1, \dots, \alpha_N) \in R_B(\alpha) \Big\} = \varnothing. \tag{3.4}$$

By the definition of M_1, there exists a representation $\alpha = \gamma_1 \cdots \gamma_L$ such that

$$M_1(\alpha) \le M(\gamma_1) \cdots M(\gamma_L) < B.$$

Theorem 2.1 implies that there exists a representation $\alpha = \zeta\beta_1 \cdots \beta_L$ with ζ a root of unity, each element β_ℓ belonging to $\operatorname{Rad}(K_\alpha)$ and $M(\beta_\ell) \le M(\gamma_\ell)$ for all ℓ. This yields

$$M_1(\alpha) \le M(\zeta)M(\beta_1) \cdots M(\beta_L) < B.$$

By combining all roots of unity in the representation into a single element, we obtain a new representation $\alpha = \alpha_1 \cdots \alpha_N$ having $\alpha_n \in \operatorname{Rad}(K_\alpha)$, at most one root of unity, and

$$M(\alpha_1) \cdots M(\alpha_N) = M(\beta_1) \cdots M(\beta_L).$$

Therefore, we see that

$$M_1(\alpha) \le M(\alpha_1) \cdots M(\alpha_N) < B, \tag{3.5}$$

which implies, in particular, that $(\alpha_1, \dots, \alpha_N) \in R_B(\alpha)$. Then by (3.4) we get that

$$M(\alpha_1) \cdots M(\alpha_N) \notin (M_1(\alpha), B). \tag{3.6}$$

Finally, combining (3.5) and (3.6) we obtain $M_1(\alpha) = M(\alpha_1) \cdots M(\alpha_N)$. ■

4 The Location of $M_1(\alpha)$ and $M_\infty(\alpha)$

We now apply Theorems 1.1 and 1.2 in order to show that $M_1(\alpha)$ and $M_\infty(\alpha)$ belong to K_α. We begin with M_∞ in which case we are able to prove a slightly stronger result.

Theorem 4.1 *If α is an algebraic number, then there exists $\beta \in K_\alpha$ such that $M_\infty(\alpha) = M(\beta)$. In particular, $M_\infty(\alpha) \in K_\alpha$.*

https://doi.org/10.4153/CMB-2011-028-x Published online by Cambridge University Press

Proof By Theorem 1.2 there exist $\alpha_1, \dots, \alpha_N \in \operatorname{Rad}(K_\alpha)$ such that $\alpha = \alpha_1 \cdots \alpha_N$ and $M_\infty(\alpha) = \max\{M(\alpha_1), \dots, M(\alpha_N)\}$. For each n, Lemma 3.1 implies that there exists a root of unity ζ_n and $L_n, S_n \in \mathbb{N}$ such that $M(\alpha_n) = M(\zeta_n \alpha_n^{L_n})^{S_n}$ and $\zeta_n \alpha_n^{L_n} \in K_\alpha$. For simplicity, we write $L = \prod_{n=1}^N L_n$ and $J_n = \prod_{k \neq n} L_k$, so that $L = L_n J_n$ for all n. Then we obtain immediately $\alpha^L = \prod_{n=1}^N \alpha_n^{L_n J_n}$, so there exists a root of unity ζ such that $\zeta\alpha^L = \prod_{n=1}^N (\zeta_n \alpha_n^{L_n})^{J_n}$. By [4, Theorem 1.3] we obtain that

$$
\begin{aligned}
M_\infty(\alpha) = M_\infty(\zeta\alpha^L) &\leq \max_{1 \leq n \leq N} \{M(\zeta_n \alpha_n^{L_n})\} \leq \max_{1 \leq n \leq N} \{M(\zeta_n \alpha_n^{L_n})^{S_n}\} \\
&= \max_{1 \leq n \leq N} \{M(\alpha_n)\} = M_\infty(\alpha).
\end{aligned}
$$

Therefore, we have that $M_\infty(\alpha) = \max_{1 \leq n \leq N}\{M(\zeta_n \alpha_n^{L_n})\}$. As we have noted, each element $\zeta_n \alpha_n^{L_n}$ belongs to K_α completing the proof of the first statement.

Now we have that $M_\infty(\alpha) = M(\beta)$ for some $\beta \in K_\alpha$. Since K_α is Galois, it must contain all conjugates of β over $\mathbb{Q}$, and therefore, it contains the product of all roots outside the unit circle. This product is a real number, so K_α must contain its absolute value. Hence we get that $M_\infty(\alpha) \in K_\alpha$. ∎

In the case of M_1, we cannot establish a result as strong as Theorem 4.1, but we can prove an analog of its second statement.

Theorem 4.2 *If α is an algebraic number, then $M_1(\alpha) \in K_\alpha$.*

Proof By Theorem 1.1, we know that there exist $\alpha_1, \dots, \alpha_N \in \operatorname{Rad}(K_\alpha)$ such that $\alpha = \alpha_1 \cdots \alpha_N$ and $M_1(\alpha) = M(\alpha_1) \cdots M(\alpha_N)$. According to Lemma 3.1, for each n there exists an algebraic number $\gamma_n \in K_\alpha$ and a positive integer S_n such that $M(\alpha_n) = M(\gamma_n)^{S_n}$. Each conjugate of γ over $\mathbb{Q}$ must belong to the Galois extension K_α, which implies that $M(\gamma_n) \in K_\alpha$ for all n. It follows that $M_1(\alpha) \in K_\alpha$. ∎

References

[1] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial.* Acta Arith. **34**(1979), no. 4, 391–401.

[2] A. Dubickas and C. J. Smyth, *On the metric Mahler measure.* J. Number Theory **86**(2001), no. 2, 368–387. doi:10.1006/jnth.2000.2579

[3] D. S. Dummit and R. M. Foote, *Abstract algebra*, Prentice Hall, Englewood Cliffs, NJ, 1991.

[4] P. Fili and C. L. Samuels, *On the non-Archimedean metric Mahler measure.* J. Number Theory **129**(2009), no. 7, 1698–1708. doi:10.1016/j.jnt.2008.12.009

[5] D. H. Lehmer, *Factorization of certain cyclotomic functions.* Ann. of Math. **34**(1933), no. 3, 461–479. doi:10.2307/1968172

[6] D. G. Northcott, *An inequality on the theory of arithmetic on algebraic varieties.* Proc. Cambridge Philos. Soc. **45**(1949), 502–509. doi:10.1017/S0305004100025202

Simon Fraser University, Department of Mathematics, Burnaby, BC V5A 1S6

and

University of British Columbia, Department of Mathematics, Vancouver, BC V6T 1Z2
e-mail: csamuels@sfu.ca