Canad. Math. Bull. Vol. **30** (1), 1987

RECIPROCAL ALGEBRAIC INTEGERS WHOSE MAHLER MEASURES ARE NON-RECIPROCAL

BY
DAVID W. BOYD

ABSTRACT. The Mahler measure $M(\alpha)$ of an algebraic integer α is the product of the moduli of the conjugates of α which lie outside the unit circle. A number α is reciprocal if α^{-1} is a conjugate of α. We give two constructions of reciprocal α for which $M(\alpha)$ is non-reciprocal producing examples of any degree n of the form $2h$ with h odd and $h \geq 3$, or else of the form $\binom{2s}{s}$ with $s \geq 2$. We give explicit examples of degrees 10, 14 and 20.

Introduction. Let α be an algebraic integer of degree n with conjugates $\alpha = \alpha_1, \ldots, \alpha_n$. The Mahler measure of α is $M(\alpha) = \Pi \max(|\alpha_i|, 1)$. Clearly $\beta = M(\alpha)$ is itself an algebraic integer. We call such β *measures*.

Measures must be Perron numbers, that is they must strictly dominate all their other conjugates in absolute value. In connection with certain questions from ergodic theory, Boyle [4] was interested in finding Perron units β which are not measures. His idea was to use a result of Smyth [6] which states that if α is non-reciprocal (α^{-1} is not a conjugate of α), then $M(\alpha) \geqslant \theta_o$ where $\theta_o = 1.3247\ldots$ is the real zero of $t^3 - t - 1$. Thus any measure $\beta < \theta_o$ must be $M(\alpha)$ for a reciprocal α. Boyle thus asked whether α being reciprocal implies that $M(\alpha)$ is reciprocal.

We showed in [2] that the answer is no by giving examples of reciprocal α of degree 6 with $M(\alpha)$ being non-reciprocal. Here we will give two constructions which give examples of all degrees $n = 2h$, h odd $\geqslant 3$, and $n = \binom{2s}{s}$, $s \geqslant 2$. All our examples have $M(\alpha) \geqslant \theta_o$ however so perhaps Boyle's original idea is still viable. It would be interesting to have some examples with $M(\alpha) < \theta_o$.

With regard to the original motivation for the question, we should mention that we have recently shown that not all Perron units are measures [3]. For example, β with minimal polynomial $t^m - t - 1$ is not a measure if $m > 3$.

I wish to express my thanks to Mike Boyle for suggesting this interesting question and to Hershey Kisilevsky who enlightened me about fields with dihedral Galois groups. This research was supported in part by an operating grant from NSERC.

1. **Preliminary discussion and notation**. Let α be a reciprocal algebraic integer of degree $n = 2h$ with $\nu \leqslant h$ conjugates in $|z| > 1$. Unless stated otherwise, we assume

Received by the editors November 2, 1985.
AMS Subject Classification (1980): Primary 12A10; Secondary 12A55.

that the conjugates $\alpha_1, \ldots, \alpha_n$ are numbered so that $|\alpha_i| \geqslant |\alpha_j|$ if $i < j$ and $\alpha_i^{-1} = \alpha_{n+1-i}$. Then $\beta = M(\alpha) = u\alpha_1, \cdots, \alpha_\nu$ for some $u = \pm 1$.

We write $\text{Spl}(\alpha) = Q(\alpha_1, \ldots, \alpha_n)$ and $G = \text{Gal}(\alpha)$ for the Galois group of $\text{Spl}(\alpha)$ over Q. We write $\text{Irr}(\alpha)$ for the minimal polynomial of α. $\text{Gal}(\alpha)$ can be regarded as a transitive permutation group on the set $[1, n] = \{1, 2, \ldots, n\}$ or $\{\pm 1, \ldots, \pm h\}$. As remarked in [2], since α is reciprocal, G is a subgroup of $B_h = C_2$ wr S_h, the hyperoctahedral group consisting of all permutations and sign changes of $\{\pm 1, \ldots, \pm h\}$.

In [2], we showed that if $n = 6$, then $M(\alpha)$ is reciprocal unless $\nu = 2$ and $G = S_3$ (the regular representation of S_3), or if $\nu = 3$ and $G = A_4$ or $S_4^{(2)}$ where $S_4^{(2)}$ denotes the representation of S_4 on the cosets of the Klein group K_4. Examples of all three types were presented in [2].

For any subset I of $[1, n]$, write $\alpha(I) = \Pi\{\alpha_i : i \in I\}$, so $\beta = u\alpha([1, \nu])$. Let $\{I_1, \ldots, I_m\}$ be the orbit of $I_1 = [1, \nu]$ under G. Then $\deg \beta = m$ and the conjugates of β are $u\alpha(I_k)$, $k = 1, \ldots, m$. For, each conjugate of β appears equally often in the list $u\alpha(I_k)$, $k = 1, \ldots, m$. But β appears once only since $\beta > |\alpha(I)|$ for any set $I \neq [1, \nu]$. Thus each conjugate appears exactly once.

PROPOSITION 1. *With the above notation, each i in* $[1, n]$ *appears in the same number r, say, of the sets* $I_1, \ldots, I_m$. *In particular* $nr = m\nu$.

PROOF. This follows since G is transitive. See [3].

PROPOSITION 2. *Suppose* α *is reciprocal and* $\beta = M(\alpha)$ *is non-reciprocal. Then* $n < 2\nu^2$.

PROOF. If $\beta_k = u\alpha(I_k)$ has $|\beta_k| > 1$ then some i in $[1, \nu]$ must lie in I_k. All of $1, \ldots, \nu$ appear in I, and each such i appears in $r - 1$ other I_k hence there are at most $1 + (r - 1)\nu$ conjugates β_k with $|\beta_k| > 1$.

Similarly, there are at most $r\nu$ conjugates β_k with $|\beta_k| < 1$.

Since β is non-reciprocal, no β_k satisfies $|\beta_k| = 1$, and hence

$$m \leqslant 1 + (r - 1)\nu + r\nu < 2r\nu$$

$$\text{So } nr = m\nu < 2r\nu^2 \quad \text{and thus} \quad n < 2\nu^2.$$

PROPOSITION 3. *If* α *is reciprocal with* $\beta = M(\alpha)$ *and if* $m = \deg \beta$ *is even then* $N(\beta) = +1$.

PROOF. This follows from Proposition 1 as in [3].

REMARK. Our two constructions have $\nu = h - 1$ and $\nu = h$, respectively. In view of Prop. 2, it would be interesting to have examples with $\nu \sim h^{1/2}$.

2. **Examples with dihedral Galois group**. This construction was suggested by the case $h = 3$, $G = S_3 = D_3$ of [2].

We begin with a unit γ of odd degree h for which $\mathrm{Gal}(\gamma) = D_h$. This group can be represented on h symbols as $D_h = \langle a, b\rangle$ where, if $k = (h+1)/2$, a and b are the permutations:

$$a = (1, 2, \dots, h)$$

$$b = (2, h)(3, h-1)\dots(k, k+1)$$

Assume that γ is not totally real. Then complex conjugation is an involution in D_h which, without loss of generality, we may take to be b. Thus γ has a single real conjugate γ_1.

THEOREM 1. *Let γ be as above and let i be any fixed integer in $2 \leq i \leq k$. Let $\alpha = \gamma_1/\gamma_i$. Then α is a reciprocal algebraic integer of degree $2h$ with* $\mathrm{Gal}(\alpha) = D_h$. *Furthermore, $\beta = M(\alpha)$ is non-reciprocal with $m = \deg \beta$ a divisor of h.*

PROOF. Assume $i = 2$. The orbit of the ordered pair $(1, 2)$ under D_h consists of the $2h$ pairs, (i, j) with $j \equiv i \pm 1 \pmod h$. Hence α is reciprocal with conjugates $\alpha_1 = \gamma_1/\gamma_2, \alpha_2 = \gamma_2/\gamma_3, \dots, \alpha_h = \gamma_h/\gamma_1$ and their reciprocals. If $|\alpha_i| = 1$ for $i \leq h$ then $\gamma_i = \bar{\gamma}_{i+1}$ so $i = k$, hence only α_k and $\bar{\alpha}_k$ lie on $|z| = 1$ so $\nu = h - 1$.

Since α is totally complex, $u = +1$ and $\beta = \alpha(I)$ for some subset I of $\{1, \dots, 2h\}$ with $|I| = h - 1$. (Note that our earlier numbering of α_i in decreasing order is not used here). Since β is real, it is a fixed point of b and hence the degree m of β divides h. In particular m is odd so β is non-reciprocal.

EXAMPLE 1. *If $h = 3$ any unit γ of degree 3 which is not totally real has* $\mathrm{Gal}(\gamma) = S_3 = D_3$. *One of $\pm\gamma_1$, $\pm\gamma_1^{-1}$ is a Pisot number $\theta > 1$ and $M(\gamma_1/\gamma_2) = \theta^3$ so this reduces to Proposition 4 of [2]. Recall that a Pisot number is an algebraic integer $\theta > 1$ all of whose other conjugates lie in $|z| < 1$.*

EXAMPLE 2. *Let $d > 0$ and suppose the field $k = Q(\sqrt{-d})$ has an ideal class group which is cyclic of order h. Then the Hilbert Class field K of k has* $\mathrm{Gal}(K/Q) = D_h$. If *γ is a unit of degree h with $K =$* $\mathrm{Spl}(\gamma)$ *then Theorem 1 applies to γ. Weber [9, p. 486] shows how to construct suitable γ by means of modular invariants and Watson [8] has worked out many special cases.*

For example, if $d = 47$ then [9, p. 723] give $K = \mathrm{Spl}(\gamma)$, where

$$\mathrm{Irr}(\gamma) = 1 \quad 0 \quad -1 \quad -2 \quad -2 \quad -1$$

(using $a_0 t^k + \dots + a_k = a_0 a_1 \dots a_k$). Here $\gamma_1 \sim e^{\pi\sqrt{47}/24}/\sqrt{2} = 1.73469\dots$ is a Pisot number. Taking $\alpha = \gamma_1/\gamma_2$ gives.

$$\mathrm{Irr}(\alpha) = 1 \quad 4 \quad 5 \quad 1 \quad 6 \quad 13 \quad 6 \quad 1 \quad 5 \quad 4 \quad 1$$

and $\beta = M(\alpha) = \gamma_1^4(\gamma_3\gamma_4)^3 = 6.7964\dots$ with

$$\mathrm{Irr}(\beta) = 1 \quad -9 \quad 19 \quad -26 \quad -9 \quad -1.$$

https://doi.org/10.4153/CMB-1987-001-0 Published online by Cambridge University Press

The other choice $\alpha = \gamma_1/\gamma_3$ gives

$$\mathrm{Irr}(\alpha) = 1 \quad 1 \quad 6 \quad 3 \quad 11 \quad 3 \quad 11 \quad 3 \quad 6 \quad 1 \quad 1$$

and $\beta = M(\alpha) = \gamma_1^3\gamma_3\gamma_4 = 4.7438\ldots$ with

$$\mathrm{Irr}(\beta) = 1 \quad -2 \quad -10 \quad -13 \quad -6 \quad -1$$

Some remarks about the computation of these polynomials are made at the end of this paper.

EXAMPLE 3. *For $d = 71$, $h = 7$ we have $K = \mathrm{Spl}(\gamma)$ where, [8],*

$$\mathrm{Irr}(\gamma) = 1 \quad -2 \quad -1 \quad 1 \quad 1 \quad 1 \quad -1 \quad -1$$

There are three choices for α and $\alpha = \gamma_1/\gamma_2$ makes $\beta = M(\alpha) = 10.6247\ldots$ smallest. The corresponding polynomials are:

$$\mathrm{Irr}(\alpha) = 1 \quad 0 \quad -4 \quad -1 \quad 5 \quad 6 \quad 16 \quad 25 \quad 16 \quad 6 \quad 5 \quad -1 \quad -4 \quad 0 \quad 1$$

$$\mathrm{Irr}(\beta) = 1 \quad -6 \quad -45 \quad -46 \quad 28 \quad -67 \quad 15 \quad -1$$

REMARK. Such dihedral extensions exist for any odd h. See [10], for example.

3. **Examples with symmetric or alternating group**. Analogous to the case $h = 3$, $\nu = 3$ we now start with γ of even degree $2s$ for which $G = \mathrm{Gal}(\gamma)$ is transitive on the unordered s-subsets of $\{1, \ldots, 2s\}$. Then, by a result of Beaumont and Peterson [1], G is either A_{2s} or S_{2s} except in the case $2s = 6$ when $G = \mathrm{PGL}_2(5) \cong S_5$ is possible. The following is thus analogous to Proposition 6 of [2].

THEOREM 2. *Let γ be a Pisot number of degree $2s$ with $N(\gamma) = 1$ such that* $\mathrm{Gal}(\gamma)$ *is transitive on the s-subsets of $\{1, \ldots, 2s\}$. Let $\alpha = \gamma_1 \ldots \gamma_s$. Then α is reciprocal, $n = \deg\alpha = \binom{2s}{s}$, α has $\nu = n/2$ conjugates in $|z| > 1$ and if $t = \binom{2s-2}{s-1}$ then $M(\alpha) = \gamma^t$ is non-reciprocal of degree $m = 2s$.*

PROOF. Since γ is a Pisot number there is no nontrivial multiplicative relation between the conjugates of γ, by a result of Mignotte [5]. Thus the $\binom{2s}{s}$ numbers $\gamma(I)$, $|I| = s$ are distinct and, by the assumption on $\mathrm{Gal}(\gamma)$, are the conjugates of $\alpha = \gamma([1, s])$.

If J is the complement of I in $[1, 2s]$ then $\gamma(I)\gamma(J) = N(\gamma) = 1$ so α is reciprocal. Letting $\gamma = \gamma_1 > 1$, we have $|\gamma(I)| > 1$ exactly when I contains 1 and thus $\nu = n/2$ and

$$\beta = M(\alpha) = \gamma_1^\nu(\gamma_2 \ldots \gamma_{2s})^\mu = \gamma_1^{\nu-\mu}$$

where

$$\nu - \mu = \binom{2s-2}{s-1}.$$

Hence β is non-reciprocal and of degree $2s$.

EXAMPLE. *The construction gives some examples with* $n \equiv 0 \pmod 4$ *since* $\binom{2s}{s}$ *is of this form unless s is a power of* 2.

Take $2s = 6$ and

$$\mathrm{Irr}(\gamma) = 1 \quad -1 \quad -1 \quad 0 \quad -1 \quad 0 \quad 1.$$

Then with α as in the Theorem,

$$P = \mathrm{Irr}(\alpha) = a_0 a_1 \ldots a_{20},$$

where $a_0 \ldots a_{10} = 1 \quad 0 \quad 2 \quad -2 \quad -4 \quad -8 \quad -13 \quad -1 \quad 8 \quad 16 \quad 38$, and $\beta = \gamma_1^6 = 25.3804\ldots$ is a Pisot number of degree 6. By using the methods of Soicher and McKay [7], one can show that $\mathrm{Gal}(\gamma) = S_6$. Alternatively, one need only check that P is irreducible to insure that the conditions on $\mathrm{Gal}(\gamma)$ are met.

4. **Other constructions**. By taking γ with other Galois groups, one can produce a wide variety of further examples.

1. For instance, if $\gamma = 1/(\sqrt[5]{2} - 1)$ then γ is a Pisot unit with $\mathrm{Gal}(\gamma) = C_5 \rtimes C_4$, the Frobenius group of order $20 = \langle (12345), (2354) \rangle$.

Taking $\alpha = (\gamma_1\gamma_2)/(\gamma_3\gamma_5)$, we find that α is reciprocal of degree $n = 10$ with $\nu = 5$ and $M(\alpha) = \gamma_1^4(\gamma_3\gamma_4)^{-2}$ non-reciprocal of degree 10.

If instead $\alpha = (\gamma_1\gamma_2)/(\gamma_3\gamma_4)$ then α is reciprocal of degree 20, $\nu = 8$ while $M(\alpha) = \gamma_1^{10}$ is non-reciprocal of degree 5.

2. A product construction as in Theorem 2 can work in certain cases with a smaller group $\mathrm{Gal}(\gamma)$. For example, suppose $\deg(\gamma) = 6$ with conjugates $\gamma_{\pm i}$, $i = 1, 2, 3$ and that $\mathrm{Gal}(\gamma) = B_3$, the group of all permutations and sign changes of $\{\pm 1, \pm 2, \pm 3\}$, so $|B_3| = 48$. Then $\alpha = \gamma_1\gamma_2\gamma_3$ has degree 8 and $\alpha' = \gamma_{-1}\gamma_1\gamma_2$ has degree 12. If $N(\gamma) = 1$ then α and α' are reciprocal.

If in addition γ_1 is a Pisot number then $M(\alpha) = \gamma_1^2\gamma_{-1}^{-2}$, which is reciprocal but $M(\alpha') = \gamma_1^4\gamma_{-1}^2$, which is non-reciprocal. Since Pisot units can be found in any real number field, it is not difficult to construct such γ.

5. **Computation of the polynomials**. Given $\mathrm{Irr}(\gamma)$ for a γ satisfying the conditions of Theorem 1, we wish to compute $\mathrm{Irr}(\alpha)$ and $\mathrm{Irr}(\beta)$. The first step is compute the roots numerically and use this information to decide on an appropriate numbering of the roots so that $a = (12\ldots h)$ is in $\mathrm{Gal}(\gamma)$. One then can compute $\mathrm{Irr}(\alpha)$ numerically by computing $tr(\alpha^k)$, $1 \leqslant k \leqslant 2h$ and using Newton's formulas to determine the coefficients. To be absolutely certain that the approximate arithmetic used here has not produced the wrong coefficients one simply checks that the computed $\mathrm{Irr}(\alpha)$ divides

$$\prod_{i \neq j} (x - \gamma_i\gamma_j^{-1}) = Q.$$

There is an easy way to generate Q since its power sums satisfy

$$T_k = \Sigma\, (\gamma_i \gamma_j^{-1})^k = S_k S_{-k} - h,$$

where $S_k = \Sigma\, \gamma_i^k$ and $h = \deg \gamma$. Thus one generates the S_k, S_{-k} by an application of Newton's formulas to $\mathrm{Irr}(\gamma)$, forms T_k and then uses Newton's formulas in reverse to find the coefficients of Q.

Similarly, for Theorem 2, we must generate $\mathrm{Irr}(\gamma_1 \ldots \gamma_s)$. We observe that

$$T_k = \mathrm{tr}((\gamma_1 \ldots \gamma_s)^k) = \sigma_s(\gamma^k),$$

where σ_s denotes the elementary symmetric function of order s. Since $\sigma_s(\gamma) = P_s(S_1(\gamma), \ldots, S_s(\gamma))$ where $S_1 \ldots S_s$ are the power sums and P_s a known polynomial (from Newton's formulas!), we have

$$T_k = P_s(S_k, S_{2k}, \ldots, S_{sk}).$$

For example, if $s = 3$,

$$T_k = (S_k^2 - 3S_k S_{2k} + 2S_{3k})/6.$$

One thus must generate S_k for $1 \leqslant k \leqslant ns$, $n = \binom{2s}{s}$, compute T_k and generate $\mathrm{Irr}(\alpha)$ by Newton's Formulas.

This method of generating the coefficients of the polynomial with roots $\gamma(I)$, $|I| = s$, can be used in the algorithm of Soicher and McKay [9] who use instead the polynomials with roots $\Sigma\,\{\gamma_i : i \in I\}$, which seem more difficult to generate. The only small problem here is the exponential growth of the S_k but multiprecision arithmetic is usually sufficient to handle this.

References

1. R.A. Beaumont and R.P. Peterson, *Set-transitive permutation groups*, Canad. Jour. Math. **7** (1955), pp. 35–42.
2. D.W. Boyd, *Inverse problems for Mahler's measure*, in Diophantine Analysis, ed. J.H. Loxton and A.J. van der Poorten, Camb. Univ. Press, 1986.
3. D.W. Boyd, *Perron units which are not Mahler measures*, Ergodic Th. and Dyn. Syst., to appear.
4. M. Boyle, *Pisot, Salem and Perron numbers in ergodic theory and topological dynamics*, xeroxed notes, November 1982.
5. M. Mignotte, *Sur les conjugués des nombres de Pisot*, C.R. Acad. Sci. Paris **298** (1984), p. 21.
6. C.J. Smyth, *On the product of the conjugates outside the unit circle of an algebraic integer*, Bull. Lond. Math. Soc. **3** (1971), pp. 169–175.
7. L. Soicher and J. McKay, *Computing Galois groups over the rationals*, Jour. Number Theory **20** (1985), pp. 273–281.
8. G.N. Watson, *Singular moduli (4)*, Acta Arith. **1** (1935), pp. 284–323.
9. H. Weber, *Lehrbuch der Algebra*, Bd II, Braunschweig 1908, reprinted by Chelsea, N.Y., 1961.
10. Y. Yamamoto, *On unramified Galois extensions of quadratic number fields*, Osaka J. Math. **I** (1970), pp. 57–76.

Department of Mathematics
University of British Columbia
Vancouver, B.C., Canada
V6T 1Y4