ACTA ARITHMETICA
176.1 (2016)

Salem numbers as Mahler measures of nonreciprocal units

by

ARTŪRAS DUBICKAS (Vilnius)

1. Introduction. Recall that for a polynomial

$$f(x) = a(x - \alpha_1) \dots (x - \alpha_n) \in \mathbb{C}[x], \qquad \text{where } a \neq 0,$$

its *Mahler measure* is defined by $M(f) := |a| \prod_{j=1}^{n} \max\{1, |\alpha_j|\}$. If $f(x) = (x - \alpha_1) \dots (x - \alpha_n) \in \mathbb{Q}[x]$ is irreducible over the field $\mathbb{Q}$, we denote by K_f its splitting field $\mathbb{Q}(\alpha_1, \dots, \alpha_n)$ and by $G_f = \mathrm{Gal}(K_f/\mathbb{Q})$ its Galois group. Also, the polynomial f is called *reciprocal* if the set $\{\alpha_1, \dots, \alpha_n\}$ of its roots is equal to $\{\alpha_1^{-1}, \dots, \alpha_n^{-1}\}$, i.e. $f(x) = \pm x^n f(x^{-1})$, and *nonreciprocal* otherwise. A root $\alpha > 1$ of a monic irreducible polynomial f in $\mathbb{Z}[x]$ of degree $2n \geq 4$ is called a *Salem number* if f is reciprocal and has $2n - 2$ roots on the unit circle $|z| = 1$.

Let L_0 be the set of all possible Mahler measures of nonreciprocal (but not necessarily irreducible) polynomials in $\mathbb{Z}[x]$. Various aspects of the set of all Mahler measures

$$L := \{M(f) : f \in \mathbb{Z}[x]\}$$

and of its subset of nonreciprocal measures

$$L_0 := \{M(f) : f \in \mathbb{Z}[x],\ f \text{ nonreciprocal}\}$$

have been investigated in the papers of Adler and Marcus [1], Boyd [2], [3], [4], Dixon and Dubickas [6], Dubickas [8], and Schinzel [12]. One of the problems from the recent BIRS workshop "The Geometry, Algebra and Analysis of Algebraic Numbers" held in 2015 in Banff (Canada) suggested by David Boyd, 7(c), is the following:

- Does L_0 contain any Salem numbers?

2010 *Mathematics Subject Classification*: Primary 11R09; Secondary 11R06, 11R32.
Key words and phrases: Salem number, Mahler measure, nonreciprocal algebraic number, Galois group of a Salem polynomial.
Received 8 January 2016.
Published online 10 October 2016.

DOI: 10.4064/aa8407-8-2016

The problem, as stated, was actually solved in [6] by Dixon and the present author (see also [7]). Selecting, for instance, the nonreciprocal quartic polynomial $x^4 - x + 1$ whose Galois group is isomorphic to S_4 and whose Mahler measure is equal to the product

$$|\beta|^2 = \beta\beta' = 1.40126\ldots \in L_0$$

of two complex conjugate roots β and $\beta' = \overline{\beta}$ of $x^4 - x + 1$ that are outside the unit circle, we see that $\alpha = \beta\beta'$ must be of degree 6 over $\mathbb{Q}$, and thus it is a Salem number (in this case, with minimal polynomial $x^6 - x^4 - x^3 - x^2 + 1$). This is true for any totally complex nonreciprocal quartic unit β whose Galois group is doubly transitive: each such Mahler measure $M(\beta)$ belongs to the set L_0 and at the same time it is a Salem number of degree 6.

This construction seems, however, an accidental one. So one may ask a more general question:

- Are there Salem numbers of other degrees in the set L_0?

In this note we will show that

THEOREM 1.1. *The set L_0 of nonreciprocal Mahler measures contains infinitely many Salem numbers of degree $d = 4$ and also of each degree $d = 4\ell + 2$, where $\ell \in \mathbb{N}$.*

The proofs for $d = 4$ and for $d = 4\ell + 2$ are different. The quartic Salem numbers are given by a straightforward (although not easy to find!) construction arising from quartic nonreciprocal totally complex units. More precisely, we will use the nonreciprocal polynomial $Q(x) := x^4 + (kx - 1)^2$ with $k \in \mathbb{N}$ (see Section 3).

The construction of Salem numbers of degree $d = 4\ell + 2$ lying in the set L_0 is more subtle (at least when $\ell > 1$ and the result does not follow from the above construction). In particular, as one of our main tools, we use the results of Christopoulos and McKee [5]. In order to formulate those results we need to recall the notion of a trace polynomial. Let $f \in \mathbb{Z}[x]$ be a monic irreducible reciprocal polynomial of degree $d = 2n$ with roots $\alpha_1, \ldots, \alpha_n, \alpha_1^{-1}, \ldots, \alpha_n^{-1}$. Then the corresponding *trace polynomial* g of degree n is the monic polynomial whose roots are $\alpha_1 + \alpha_1^{-1}, \ldots, \alpha_n + \alpha_n^{-1}$. With this notation, [5, Theorem 1.1] asserts the following:

THEOREM 1.2. *Let f be a Salem polynomial of degree $d = 2n$, $n \geq 2$, with roots $\alpha_1, \ldots, \alpha_n, \alpha_1^{-1}, \ldots, \alpha_n^{-1}$ and trace polynomial g, and let G_f, G_g be the Galois groups of f and g. Then G_f is isomorphic either to the semidirect product $\mathbb{Z}_2^n \rtimes G_g$ or to $\mathbb{Z}_2^{n-1} \rtimes G_g$, with the latter possible only if n is odd.*

Furthermore, in [5, Proposition 2.3] the following has been shown:

Theorem 1.3. *In Theorem 1.2, the group* $\mathbb{Z}_2^n$ *of order* 2^n *is generated by all transpositions of the form* $(\alpha_i, \alpha_i^{-1})$, $i = 1, \dots, n$, *whereas* $\mathbb{Z}_2^{n-1}$ *of order* 2^{n-1} *is generated by all the products* $(\alpha_i, \alpha_i^{-1})(\alpha_j, \alpha_j^{-1})$ *of two transpositions, where* $1 \le i < j \le n$. *This latter case occurs if and only if* n *is odd and the discriminant of* f *is a square in the splitting field* K_g *of* g.

In [10], Lalande proved that for each $n \ge 2$ there are Salem numbers of degree $2n$ with the largest possible Galois groups $\mathbb{Z}_2^n \rtimes S_n$ of order $2^n n!$ (see also [11]). The example

$$x^{10} - 2x^9 - 6x^8 - 10x^7 - 10x^6 - 10x^5 - 10x^4 - 10x^3 - 6x^3 - 2x + 1$$

given in [5] illustrates that the second possibility in Theorem 1.2 may occur for $n = 5$.

Our next result shows that the second possibility may occur for every odd $n \ge 3$, so one can replace in Theorem 1.2 "only if n is odd" by "if and only if n is odd".

Theorem 1.4. *For each odd* $n \ge 3$ *there is a Salem polynomial* f *of degree* $d = 2n$ *with Galois group* $G_f = \mathbb{Z}_2^{n-1} \rtimes G_g$, *where* G_g *is the Galois group of the trace polynomial* g *of* f.

The key result in the proof of Theorem 1.4 is the following lemma:

Lemma 1.5. *For each odd* $n \ge 3$ *there exists an irreducible monic polynomial* $P \in \mathbb{Z}[x]$ *of degree* n *which has* $n-1$ *real roots in the interval* $(-2, 2)$, *one real root greater than* 2, *and satisfies* $P(-2) = P(2)$.

For instance, for $n = 3$ the procedure described below (with $T = 20$ and $N = 1$) produces the polynomial $P(x) = x^3 - 12x^2 - 4x + 22$.

In the next section, we shall prove Lemma 1.5 and Theorem 1.4. Then, in Section 3, we prove Theorem 1.1 for $d = 4$. Finally, in Section 4, using Theorem 1.4 and the construction of so-called Salem half-norms used in [9], we shall prove Theorem 1.1 for each d of the form $4\ell + 2$.

2. Proofs of Lemma 1.5 and Theorem 1.4

Proof of Lemma 1.5. Let

$$r_1 := -2 < r_2 < \cdots < r_{n-1} < r_n := 2$$

be n fixed rational numbers. Set

$$h(x) := b_0 + b_1 x + \cdots + b_{n-1} x^{n-1}.$$

Then the n equations

$$h(r_1) = -T - 2^{n+1} - r_1^n \quad \text{and} \quad h(r_j) = (-1)^j T - r_j^n \quad \text{for } j = 2, \dots, n$$

form a linear system in n unknowns $b_0, b_1, \dots, b_{n-1}$. The Vandermonde determinant of this linear system is a nonzero rational number. Thus, for each

$T \in \mathbb{N}$ this linear system has a unique real solution $(b_0, \dots, b_{n-1}) \in \mathbb{Q}^n$. On multiplying all equalities by some (large) positive integer N and setting

$$H(X) := Nh(x) = B_0 + B_1 x + \cdots + B_{n-1} x^{n-1}$$

we can further assume that all the coefficients B_j of the polynomial H are integers divisible by 4. Here, by the above,

$$H(r_1) = -N(T + 2^{n+1} + r_1^n), \tag{2.1}$$

$$H(r_j) = N((-1)^j T - r_j^n) \quad \text{for } j = 2, \dots, n. \tag{2.2}$$

Set

$$\begin{aligned} P(x) &:= H(x) + 2 - 2^{n-1}x + x^n \\ &= B_0 + 2 + (B_1 - 2^{n-1})x + B_2 x^2 + \cdots + B_{n-1}x^{n-1} + x^n. \end{aligned}$$

By construction, all the coefficients of the monic polynomial $P \in \mathbb{Z}[x]$ for x^j $(0 \le j \le n-1)$ are even and the constant coefficient $B_0 + 2$ is not divisible by 4. Hence, by Eisenstein's criterion with respect to the prime $p = 2$, the polynomial P is irreducible.

Now, we will show that for every $T > 2^{n+1}$ the polynomial P satisfies other required properties. Firstly, using (2.1), $r_1 = -2$, and the fact that n is odd, we obtain

$$P(-2) = H(-2) + 2 = -N(T + 2^{n+1} + (-2)^n) + 2 = -N(T + 2^n) + 2.$$

Similarly, from (2.2) it follows that

$$P(r_j) = H(r_j) + 2 - 2^{n-1}r_j + r_j^n = N((-1)^j T - r_j^n) + 2 - 2^{n-1}r_j + r_j^n$$

for $j = 2, \dots, n$. In particular, since $r_n = 2$, taking $j = n$ we obtain

$$P(2) = N(-T - 2^n) + 2 - 2^n + 2^n = -N(T + 2^n) + 2.$$

Therefore, $P(-2) = P(2)$, as claimed.

Next, observe that $P(r_1) = P(-2) < 0$ (for any $T, N \in \mathbb{N}$). Furthermore, the condition $T > 2^{n+1}$ implies that for j even

$$\begin{aligned} P(r_j) &= N((-1)^j T - r_j^n) + 2 - 2^{n-1}r_j + r_j^n \\ &\ge T - r_j^n + 2 - 2^{n-1}r_j + r_j^n > T - 2^{n-1}r_j > T - 2^n > 0. \end{aligned}$$

Similarly, for j odd we have

$$P(r_j) \le -T - r_j^n + 2 - 2^{n-1}r_j + r_j^n < -T + 2 + 2^n < 0.$$

Thus, P has a real root in each of the $n-1$ intervals (r_j, r_{j+1}) for $j = 1, \dots, n-1$. Finally, in view of $P(2) < 0$ its nth root must lie in $(2, \infty)$, as claimed. ∎

In fact, P depends on the choice of T and N. Evidently, there are infinitely many choices of T. Also, for each T there are infinitely many possibilities to choose N. So, we have infinitely many irreducible polynomials P satisfying the conditions of Lemma 1.5.

Proof of Theorem 1.4. As observed in [5], the discriminants Δ_f of an irreducible reciprocal polynomial

$$f(x) = \prod_{j=1}^{n}(x-\alpha_j)(x-\alpha_j^{-1}) \tag{2.3}$$

of degree $n \ge 2$ and Δ_g of its trace polynomial

$$g(x) = \prod_{j=1}^{n}(x-\alpha_j-\alpha_j^{-1}) \tag{2.4}$$

are related by the formula

$$\Delta_f = \Delta_g^2 \prod_{i=1}^{n}(\alpha_j-\alpha_j^{-1})^2. \tag{2.5}$$

Indeed, using

$$\begin{aligned}\Delta_g &= \prod_{1\le i<j\le n}(\alpha_i+\alpha_i^{-1}-\alpha_j-\alpha_j^{-1})^2 = \prod_{1\le i<j\le n}(\alpha_i-\alpha_j)^2(1-\alpha_i^{-1}\alpha_j^{-1})^2\\ &= \prod_{1\le i<j\le n}(\alpha_i-\alpha_j)^2(\alpha_i\alpha_j-1)^2\prod_{i=1}^{n}\alpha_i^{2-2n},\end{aligned}$$

we deduce that

$$\begin{aligned}\Delta_f &= \prod_{1\le i<j\le n}(\alpha_i-\alpha_j)^2(\alpha_i^{-1}-\alpha_j^{-1})^2\prod_{1\le i,j\le n}(\alpha_i-\alpha_j^{-1})^2\\ &= \prod_{1\le i<j\le n}(\alpha_i-\alpha_j)^4\prod_{1\le i,j\le n}(\alpha_i\alpha_j-1)^2\prod_{i=1}^{n}\alpha_i^{2-4n}\\ &= \prod_{1\le i<j\le n}(\alpha_i-\alpha_j)^4(\alpha_i\alpha_j-1)^4\prod_{i=1}^{n}(\alpha_i^2-1)^2\alpha_i^{2-4n}\\ &= \Delta_g^2\prod_{i=1}^{n}(\alpha_i^2-1)^2\alpha_i^{-2} = \Delta_g^2\prod_{i=1}^{n}(\alpha_i-\alpha_i^{-1})^2.\end{aligned}$$

Since

$$(-2-y-y^{-1})(2-y-y^{-1}) = -4+y^2+y^{-2}+2 = (y-y^{-1})^2,$$

from (2.4) it follows that

$$\prod_{j=1}^{n}(\alpha_j-\alpha_j^{-1})^2 = g(-2)g(2).$$

Combining this with (2.5) yields $\Delta_f = \Delta_g^2 g(-2)g(2)$.

Now, for an odd $n \geq 3$, selecting $g(x) = P(x)$ as in Lemma 1.5, we see that the corresponding $f(x) = x^n P(x + x^{-1})$ in (2.3) will be a Salem polynomial of degree $d = 2n$ whose discriminant $\Delta_f = \Delta_P^2 P(-2)P(2)$ is a square of the positive integer $|\Delta_P P(2)|$. By Theorem 1.3, this completes the proof. ∎

3. Quartic Salem numbers. Consider the polynomial

$$Q(x) = x^4 + (kx-1)^2,$$

where $k \in \mathbb{N}$. Clearly, it has no real roots, so it is not a product of cubic and linear integer polynomials. If it were a product of two monic quadratic integer polynomials, say $x^2 + a_1 x + b_1$ and $x^2 + a_2 x + b_2$, then $a_1 + a_2 = 0$ and $b_1 b_2 = 1$. Thus, $a_2 = -a_1$ and $b_1 = b_2 = \pm 1$. However, the product of $x^2 + a_1 x \pm 1$ and $x^2 - a_1 x \pm 1$ is equal to $(x^2 \pm 1)^2 - a_1^2 x^2$, which is distinct from $Q(x)$, a contradiction. Hence, Q is irreducible.

Since

$$Q(x) = \big(x^2 + (kx-1)\sqrt{-1}\big)\big(x - (kx-1)\sqrt{-1}\big),$$

it has the following four roots:

$$\beta_1 := \frac{1}{2}\bigg(-\sqrt{\frac{-k^2 + \sqrt{k^4+16}}{2}} + \bigg(\sqrt{\frac{k^2 + \sqrt{k^4+16}}{2}} + k\bigg)\sqrt{-1}\bigg), \tag{3.1}$$

$$\beta_3 := \frac{1}{2}\bigg(\sqrt{\frac{-k^2 + \sqrt{k^4+16}}{2}} + \bigg(\sqrt{\frac{k^2 + \sqrt{k^4+16}}{2}} - k\bigg)\sqrt{-1}\bigg), \tag{3.2}$$

$$\beta_2 := \overline{\beta}_1 \quad \text{and} \quad \beta_4 = \overline{\beta}_3. \tag{3.3}$$

Hence, $\beta_1\beta_4 = \sqrt{-1}$, $\beta_1 + \beta_4 = k\sqrt{-1}$ and $\beta_2\beta_3 = -\sqrt{-1}$, $\beta_2 + \beta_3 = -k\sqrt{-1}$. Also, $|\beta_1| > 1$ and $|\beta_3| = |\beta_1|^{-1} < 1$.

Therefore,

$$\alpha := M(\beta_1) = \beta_1\overline{\beta}_1 = \frac{1}{4}\Big(k^2 + \sqrt{k^4+16} + k\sqrt{2k^2 + 2\sqrt{k^4+16}}\Big)$$

is a Salem number with conjugates $\beta_3\overline{\beta}_3 = \alpha^{-1}, \beta_1\beta_3, \overline{\beta}_1\overline{\beta}_3$ whose minimal polynomial is $x^4 - k^2x^3 - 2x^2 - k^2x + 1$.

4. Proof of Theorem 1.1 for $d = 4\ell+2$. Let $d = 2n$, where $n = 2\ell+1$, $\ell \in \mathbb{N}$. Consider the Salem half-norm (as defined in [9])

$$\beta := \alpha_1 \ldots \alpha_n,$$

where $\alpha = \alpha_1$ is a Salem number of degree $2n$ as in Theorem 1.4 with conjugates $\alpha_1, \ldots, \alpha_n, \alpha_1^{-1}, \ldots, \alpha_n^{-1}$ and Galois group $G_f = \mathbb{Z}_2^{n-1} \rtimes G_g$. Corollary 4.8 in [9] asserts that the 2^n numbers

$$\alpha_1^{\delta_1} \dots \alpha_n^{\delta_n}, \quad \text{where } \delta_j \in \{-1, 1\}, \tag{4.1}$$

are all distinct. We will show that the degree of β is 2^{n-1} and that β is nonreciprocal, that is, $\beta^{-1} = \alpha_1^{-1} \dots \alpha_n^{-1}$ is not conjugate to β over $\mathbb{Q}$.

Indeed, if β were reciprocal then there is an automorphism of the Galois group G_f that maps β to β^{-1}. However, by Theorem 1.3, each $\sigma \in G_f$ maps the product $\alpha_1 \dots \alpha_n$ into $\alpha_1^{\delta_1} \dots \alpha_n^{\delta_n}$, where $\delta_j \in \{-1, 1\}$, and where the number of j's with $\delta_j = 1$ is odd, since n is odd. The number $\beta^{-1} = \alpha_1^{-1} \dots \alpha_n^{-1}$ has zero j's with $\delta_j = 1$. Hence, $\sigma(\beta) \neq \beta^{-1}$ for each $\sigma \in G_f$.

In fact, we have two sets of conjugate algebraic numbers: those 2^{n-1} of the form (4.1) that have an odd number of δ_j equal to 1 are all conjugate to β, whereas the remaining 2^{n-1} such products (4.1), with an even number of δ_j equal to 1, are all conjugate to β^{-1}. In particular, $M(\beta) = \alpha^{2^{n-2}}$, since 2^{n-2} conjugates of β lie on the circle $|z| = \alpha$ and 2^{n-2} other conjugates lie on the circle $|z| = \alpha^{-1}$. This completes the proof of the theorem, since $M(\beta) \in L_0$ and every positive integer power α^m of a Salem number α is a Salem number itself (here, $m = 2^{n-2} \geq 2$).

References

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

[2] D. W. Boyd, *Inverse problems for Mahler's measure*, in: Diophantine Analysis, J. H. Loxton and A. J. van der Poorten (eds.), London Math. Soc. Lecture Note Ser. 109, Cambridge Univ. Press, Cambridge, 1986, 147–158.

[3] D. W. Boyd, *Perron units which are not Mahler measures*, Ergodic Theory Dynam. Systems 6 (1986), 485–488.

[4] D. W. Boyd, *Reciprocal algebraic integers whose Mahler measures are non-reciprocal*, Canad. Math. Bull. 30 (1987), 3–8.

[5] C. Christopoulos and J. McKee, *Galois theory of Salem polynomials*, Math. Proc. Cambridge Philos. Soc. 148 (2010), 47–54.

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

[7] A. Dubickas, *Algebraic, arithmetic and geometric properties of Mahler measures*, Proc. Inst. Math. (Nat. Acad. Sci. Belarus) 13 (2005), 70–74.

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

[9] 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), 1–17.

[10] F. Lalande, *Corps de nombres engendrés par un nombre de Salem*, Acta Arith. 88 (1999), 191–200.

[11] F. Lalande, *Réalisation de produits en couronne comme groupe de Galois de polynômes réciproques et construction de polynômes génériques* (with an appendix by J. Oesterlé), Acta Arith. 103 (2002), 9–20.

[12] 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.

Artūras Dubickas
Department of Mathematics and Informatics
Vilnius University
Naugarduko 24
Vilnius LT-03225, Lithuania
E-mail: arturas.dubickas@mif.vu.lt