On the behavior of Mahler's measure under iteration

Paul A. Fili[1] · Lukas Pottmeyer[2] · Mingming Zhang[1]

Abstract

For an algebraic number α we denote by $M(\alpha)$ the Mahler measure of α. As $M(\alpha)$ is again an algebraic number (indeed, an algebraic integer), $M(\cdot)$ is a self-map on $\overline{\mathbb{Q}}$, and therefore defines a dynamical system. The *orbit size* of α, denoted $\#\mathcal{O}_M(\alpha)$, is the cardinality of the forward orbit of α under M. We prove that for every degree at least 3 and every non-unit norm, there exist algebraic numbers of every orbit size. We then prove that for algebraic units of degree 4, the orbit size must be 1, 2, or infinity. We also show that there exist algebraic units of larger degree with arbitrarily large but finite orbit size.

1 Introduction

The *Mahler measure* of an algebraic number α with minimal polynomial $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$, is defined as:

✉ Lukas Pottmeyer
lukas.pottmeyer@uni-due.de

Paul A. Fili
paul.fili@okstate.edu

Mingming Zhang
mingmiz@okstate.edu

1 Oklahoma State University, Stillwater, OK 74078, USA

2 Universität Duisberg-Essen, 45117 Essen, Germany

$$M(\alpha) = |a_n| \prod_{i=1}^{n} \max\{1, |\alpha_i|\} = \pm a_n \prod_{\substack{i=1 \\ |\alpha_i|>1}}^{n} \alpha_i,$$

where $\alpha_1, \ldots, \alpha_n$ are the distinct roots of $f(x)$; i.e. $f(x) = a_n \prod_{i=1}^{n}(x - \alpha_i) \in \mathbb{C}[x]$. It is clear that $M(\alpha) \geq 1$ is a real algebraic integer, and it follows from Kronecker's theorem that $M(\alpha) = 1$ if and only if α is a root of unity. Moreover, we will freely use the facts that $M(\alpha) = M(\beta)$ whenever α and β have the same minimal polynomial, and that $M(\alpha) = M(\alpha^{-1})$. Lehmer [12] famously asked in 1933 if the Mahler measure for an algebraic number which is not a root of unity can be arbitrarily close to 1. This question became known as *Lehmer's problem*, and (somewhat inaccurately) the statement that an absolute constant $c > 1$ exists such that $M(\alpha) > 1$ implies $M(\alpha) \geq c$ became known as *Lehmer's conjecture*, despite the fact that Lehmer himself did not conjecture this and merely asked if one could find smaller values of the Mahler measure than he found. It is often suggested that the minimal value of c is a Salem number, namely $\tau = 1.17\ldots$, which is the largest real root of the polynomial $f(x) = x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$, discovered by Lehmer in his 1933 paper.

Although there has been much computational work performed in order to find irreducible polynomials of small Mahler measure (we refer the reader to M. Mossinghoff's website [15] for the latest tables of known polynomials, as well as the papers by Mossinghoff [16] and Mossinghoff et al. [17]), remarkably, no polynomial of smaller nontrivial Mahler measure has been found since Lehmer's original 1933 work. Since that time, the best asymptotic bound towards Lehmer's problem was discovered by Dobrowolski [8]. It is clear that in considering the problem, one can reduce to considering the Mahler measure of algebraic units. Smyth [19] proved that in fact, non-reciprocal units have a minimal Mahler measure $\theta_0 = M(\theta_0)$, where θ_0 is the smallest Pisot-Vijayaraghavan number and is given by the positive root of $x^3 - x - 1$. In another direction, Borwein et al. [3] proved the Lehmer conjecture for polynomials with only odd coefficients.

The study of iteration of the Mahler measure began with questions about which algebraic numbers are themselves Mahler measures. Adler and Marcus [1] proved that every Mahler measure is a Perron number and asked if the Perron numbers given by the positive roots of $x^n - x - 1$ are also values of the Mahler measure for any $n > 3$. Recall that α is a Perron number if and only $\alpha > 1$ is a real algebraic integer such that all conjugates of α over $\mathbb{Q}$ have absolute value $< \alpha$. This notion of 'Perron number' was introduced by Lind [13] who also proved several properties of the class of Perron numbers in [14], including that they are closed under addition and multiplication and are dense in the real interval $[1, \infty)$. Boyd [4] proved that the positive roots of $x^n - x - 1$ for $n > 3$ were not values of the Mahler measure, but Dubickas [10] showed that for every Perron number β, there exists a natural number n such that $n\beta$ is a value of the Mahler measure. Dixon and Dubickas [7] and Dubickas [11] established further results on which numbers are in the value set of M. However, the question whether a given number is a Mahler measure of an algebraic number is very hard to answer in general. For instance, it is an open question of Schinzel [18] whether or not $\sqrt{17} + 1$ is the Mahler measure of an algebraic number.

Dubickas [9] appears to have been the first to pose questions on the Mahler measure as a dynamical system, introducing the concept of the *stopping time* of an algebraic number under M, defined as the number of iterations required to reach a fixed point. We note that the stopping time is one less than the cardinality of the forward orbit of the number under iteration of M, which we will call the *orbit size*. Specifically, we set $M^{(0)}(\alpha) = \alpha$ and let $M^{(n)}(\alpha) = M \circ \cdots \circ M(\alpha)$ denote the nth iteration of M. We define the *orbit of α under M* to be the set:

$$\mathcal{O}_M(\alpha) = \{M^{(n)}(\alpha) : n \geq 0\}. \tag{1}$$

Then the orbit size of α is $\#\mathcal{O}_M(\alpha)$, while the stopping time is $\#\mathcal{O}_M(\alpha) - 1$. It is easy to see that for any algebraic number α, $M(\alpha) \leq M^{(2)}(\alpha)$, so M is nondecreasing after at least one iteration, and thus, the Mahler measure either grows, or is fixed.

In fact, by Northcott's theorem, it is easy to see that if α is a wandering point of M, then $M^{(n)}(\alpha) \to \infty$, as the degree of $M^{(n)}(\alpha)$ can never be larger than the degree of the Galois closure of the field $\mathbb{Q}(\alpha)$. In particular, there are no cycles of length greater than 1; each number α either wanders (that is, the orbit under M is infinite), or it is preperiodic and ends in a fixed point of M. Dubickas claimed in [9] that 'generically' $M^{(n)}(\alpha) \to \infty$, however, he did not give an example or a proof of this. The first explicit results in this direction appear to have been by Zhang [21], who proved that if $[\mathbb{Q}(\alpha) : \mathbb{Q}] \leq 3$, then $\#\mathcal{O}_M(\alpha) < \infty$, and also found an algebraic number α of degree 4 with minimal polynomial $x^4 + 5x^2 + x - 1$ such that $M^{(2n)}(\alpha) = M^{(2)}(\alpha)^{2^{n-1}}$, proving that $M^{(n)}(\alpha) \to \infty$ for this example.

Further, it is trivial to see that the fixed points of M correspond to natural numbers, Pisot-Vijayaraghavan numbers, and Salem numbers. This raises several natural questions: for example, can one show that the Lehmer problem could be reduced to the study of fixed points of M? The answer to such a question might help establish the long held folklore conjecture that Salem numbers are indeed minimal for Lehmer's problem. The fixed points for the dynamical system induced by the multiplicative Weil-height have recently been classified by Dill [6].

Dubickas posed several questions in [9], including whether one could classify all numbers of stopping time 1 (that is, numbers which are not fixed by M, but for which $M(\alpha)$ is fixed), and whether algebraic numbers of arbitrary stopping time existed. In a later paper [10], he established, among other things, that for every $k \in \mathbb{N}$, there exists a cubic algebraic integer of norm 2 with stopping time k.

In this paper, we will prove several other results regarding the stopping time of algebraic numbers. Our first result is a direct generalization of Dubickas's result:

Theorem 1 *For any $d \geq 3$, $l \in \mathbb{Z}\backslash\{\pm 1, 0\}$ and $k \in \mathbb{N}$ there is an algebraic integer α of degree d, $N(\alpha) = l$ and $\#\mathcal{O}_M(\alpha) = k$.*

The proof of Theorem 1 will be given in Sect. 2 below. To study the possible behaviour of algebraic units under iteration of M is more delicate. It is clear that $\#\mathcal{O}_M(\alpha) \leq 2$ for all algebraic units of degree at most 3, and this result is (non-trivially) also true if the degree is 4:

Theorem 2 *Let α be an algebraic unit of degree 4. Then either $\#\mathcal{O}_M(\alpha) \leq 2$ or $\#\mathcal{O}_M(\alpha) = \infty$. Moreover, if $\#\mathcal{O}_M(\alpha) = \infty$, then $M^{(3)}(\alpha) = M(\alpha)^2$.*

The first algebraic unit α with $\#\mathcal{O}_M(\alpha) \geq 3$ we found has degree 6 and orbit size 5. It is given by any root of $x^6 - x^5 - 4x^4 - 2x^2 - 4x - 1$. Despite an extensive search, we did not find any unit of degree 5 of orbit size ≥ 3, nor a unit of degree 6 of finite orbit size ≥ 6.

It will follow from the proof of Theorem 2 that we have the following corollary:

Corollary 1 *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.*

The proofs of Theorem 2 and Corollary 1 are given in Sect. 3. We note that, in the example of a degree 4 wandering point given by Zhang [21], the sequence $(\log M^{(n)}(\alpha))_{n \in \mathbb{N}}$ satisfied the recursion relation $x_n = 2x_{n-2}$ for $n \geq 3$. Based on the above corollary and further experimental data, we make the following conjecture:

Conjecture 1 *For every algebraic unit α, there exists a constant k such that the sequence $(\log(M^{(n)}(\alpha)))_{n \geq k}$ satisfies a linear homogeneous recursion.*

We note that, in the case of a large Galois group, the behavior of units is particularly simple. We prove that, if the Galois group contains the alternating group, then the orbit of a unit must either stop after at most one iteration, or the unit wanders. Specifically, we prove in Sect. 4 the following theorem:

Theorem 3 *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 $\#\mathcal{O}_M(\alpha) = \infty$.

One might be led by Theorems 2 and 3 to suspect that, in fact, algebraic units cannot have arbitrarily large but finite orbits under M. However, we prove that this is not the case.

Theorem 4 *Let $S \in \mathbb{N}$ be arbitrary, and let $d \geq 12$ be divisible by 4. Then there exist algebraic units of degree d whose orbit size is finite but greater than S.*

The proof is given in Sect. 5. It would be interesting to know whether there are large finite orbits of algebraic units in any degree less than 12.

2 Arbitrary orbit size for non-units and proof of Theorem 1

In [10], Dubickas proved the case $d = 3$ and $l = 2$ (and k arbitrary). In order to prove Theorem 1, we will start with a few examples.

Example 1 Since there are Pisot-Vijayaraghavan numbers of any degree and norm, we know that for any $d \in \mathbb{N}$ and any $l \in \mathbb{Z}\backslash\{\pm 1, 0\}$ there are algebraic numbers α of

degree d, norm l and orbit size 1. By Perron's criterion, we may take the largest root of $x^d + l^2x^{d-1} + l$.

Similarly, the polynomial $x^d + l^dx + l$ has precisely one root β inside the unit circle and all other roots are of absolute value $> |l|$. Hence, the polynomial is irreducible. Let α be the largest root of this polynomial. Then $M(\alpha) = |l/\beta|$, which is a Pisot number. Thus, α has norm l, degree d and orbit size 2.

Example 2 For any $l \in \mathbb{Z}\setminus\{\pm 1, 0\}$ we consider $f(x) = x^3 - l^2x + l$. Let $\alpha_1, \alpha_2, \alpha_3$ be the roots of f ordered so that $|\alpha_1| \geq |\alpha_2| \geq |\alpha_3|$.

If $l \geq 2$ we have

$$\begin{array}{ll} f(-l-1) = -2l^2 - 2l - 1 < 0, & f(-l) = l > 0 \\ f(l-1) = -2l^2 + 4l - 1 < 0, & f(l) = l > 0 \\ f(1) = 1 - l^2 + l < 0, & f\left(\dfrac{1}{l}\right) = \dfrac{1}{l^3} > 0 \end{array}$$

Hence, the three roots are real and none of them is an integer. If f is reducible, then one of the factors must be linear, this is a contradiction since f is monic. Hence, f is irreducible and it follows that

$$\alpha_1 \in (-l-1, -l), \quad \alpha_2 \in (l-1, l), \quad \alpha_3 \in \left(\frac{1}{l}, 1\right).$$

Therefore we find $M^{(0)}(\alpha_1) = \alpha_1$, $M^{(1)}(\alpha_1) = -\alpha_1\alpha_2 = l/\alpha_3$,

$$M^{(2)}(\alpha_1) = M\left(\frac{l}{\alpha_3}\right) = \frac{l^2}{\alpha_2\alpha_3} = -\alpha_1 l,$$

and

$$M^{(3)}(\alpha_1) = M(-\alpha_1 l) = \alpha_1 l\alpha_2 l\alpha_3 l = l^4 \in \mathbb{Z}.$$

These are all elements in the orbit of α_1 under iteration of M. Hence, α_1 is an algebraic integer of degree 3, $N(\alpha_1) = l$ and $\#\mathcal{O}_M(\alpha_1) = 4$. Moreover $-\alpha_1$ is an algebraic integer of degree 3, $N(-\alpha_1) = -l$ and $\#\mathcal{O}_M(-\alpha_1) = 4$.

In the same fashion one can prove that any root of the polynomial $x^3 + lx^2 - l$ is of degree 3, norm $-l$ and orbit size 3.

Example 3 Again let $l \in \mathbb{Z}\setminus\{\pm 1, 0\}$ be arbitrary and consider $f(x) = x^4 - l^2x^2 + (l^2 - l)x + l$. The four roots of f are ordered as $|\alpha_1| \geq |\alpha_2| \geq |\alpha_3| \geq |\alpha_4|$. A direct computation shows that f is irreducible and $\#\mathcal{O}_M(\alpha_1) = 4$ if $l \in \{-3, -2, -4\}$. If $l \notin \{-3, -2 - 1, 0, 1, 2\}$, then we show as in the last example that

$$\alpha_1 \in (-l-1, -l), \quad \alpha_2 \in (l-1, l), \quad \alpha_3 \in (1, 2), \quad \alpha_4 \in \left(-1, -\frac{1}{l^2}\right)$$

if $l > 0$, and

$$\alpha_1 \in (-l-1, -l), \quad \alpha_2 \in (l-1, l), \quad \alpha_3 \in (1, 2), \quad \alpha_4 \in \left(1, \frac{1}{l^2}\right)$$

if $l < 0$. Obviously f has no linear factor. Moreover, α_4 and α_1 must be Galois conjugates, since the norm of α_1 has to be a divisor of l. Hence, if f is not irreducible it factors into $g(x) = (x - \alpha_1)(x - \alpha_4)$ and $h(x) = (x - \alpha_2)(x - \alpha_3)$. This can only occur if g and h are in $\mathbb{Z}[x]$. Comparing the size of the roots, the only possibilities are $g(x) = x^2 + (l+1)x + 1$ and $h(x) = x^2 - (l+1)x + l$. However, multiplying these two polynomials does not give f. Hence, f is irreducible.

Now we calculate the orbit size of α_1. We have

- $M^{(1)}(\alpha_1) = -l/\alpha_4$
- $M^{(2)}(\alpha_1) = \pm l^2 \alpha_1$
- $M^{(3)}(\alpha_1) = \pm l^9$

and hence $\#\mathcal{O}_M(\alpha_1) = 4$. We have shown, that any root α of f is an algebraic integer of degree 4, norm l and orbit size 4.

Example 4 One can show with similar methods as above, that any root of $x^d - l^{d-2}x + l$ has orbit size 3, for all $d \geq 4$ and $l \in \mathbb{Z}\setminus\{\pm 1, 0\}$: To this end, we note

$$|-l^{d-2}z| = |l|^{d-2} > |l| + 1 \geq |z^d + l| \quad \forall z \in \mathbb{C}, \ |z| = 1, \tag{2}$$

and

$$|z^d| = |l|^d > |l|^{d-1} + |l| \geq |-l^{d-2}z + l| \quad \forall z \in \mathbb{C}, \ |z| = |l|. \tag{3}$$

Now we apply Rouché's theorem. Then (2) tells us that $x^d - l^{d-2}x + l$ has precisely one root α_d inside the unit circle, and (3) tells us that all roots $\alpha_1, \ldots, \alpha_d$ of $x^d - l^{d-2}x + l$ have absolute value $< |l|$.

Before we proceed with calculating the orbit size of one of these roots, we need to show that $x^d - l^{d-2}x + l$ is irreducible. This is obviously the case if $|l|$ is a prime number. So in particular, we can assume that $|l| \geq 4$. Using this assumption and $d \geq 4$, the same calculation as in (2) proves that there is precisely one root of $x^d - l^{d-2}x + l$ of absolute value $\leq \sqrt{|l|}$ (necessarily α_d).

It follows that no product of two or more of the elements $\alpha_1, \ldots, \alpha_{d-1}$ can be a divisor of l. Hence, the only possibility for $x^d - l^{d-2}x + l$ to be reducible is, if it has a root $a \in \mathbb{Z}$. This a must be a divisor of $|l|$ and it must satisfy $a^d = l^{d-2}a - l$. Hence, $a^{d-1} \mid l$ which implies $|a|^{d-1} \leq |l|$. This is not possible, as we have just seen that $|a| \geq \sqrt{|l|}$. It follows that $x^d - l^{d-2}x + l$ is indeed irreducible, and α_1 is an algebraic integer of degree d, and norm l.

We then have:

- $M^{(1)}(\alpha_1) = \alpha_1 \cdots \alpha_{d-1} = l/|\alpha_d| \notin \mathbb{Z}$, and
- $M^{(2)}(\alpha_1) = M(\pm\frac{l}{\alpha_d}) = \pm \prod_{i=1}^{d} \frac{l}{\alpha_i} \in \mathbb{Z}$.

Hence α_1 has orbit size 3.

Proposition 1 *Let $d \geq 3$ be an integer and let $\alpha_1, \ldots, \alpha_d$ be a full set of Galois conjugates of an algebraic integer α. Assume the following conditions:*

(i) $|\alpha_1| > |\alpha_2| \geq \cdots \geq |\alpha_{d-1}| > 1 > |\alpha_d|$, *and*
(ii) $|\alpha_i| \leq |N(\alpha)|$ *for all* $i \in \{2, \ldots, d\}$.

Then α is a pre-periodic point of M. More precisely, if we let

$$c(\alpha) = \min\{\min\{k \in \mathbb{N} : 2 \mid k \text{ and } |\alpha_d \cdot N(\alpha)^{b_k}| > 1\},$$
$$\min\{k \in \mathbb{N} : 2 \nmid k \text{ and } |\alpha_1| < |N(\alpha)^{b_k}|\}\},$$

where we define $b_1 = 1$, and $b_n = b_{n-1} \cdot (d-1) + (-1)^{n-1}$ for all $n \geq 2$, then $\#\mathcal{O}_M(\alpha) = c(\alpha) + 2$.

Proof First we note that α cannot be an algebraic unit. Hence, $|N(\alpha)| \geq 2$ and $b_k \geq 1$ for all k. We claim that $b_k \to \infty$. To see this, notice that $b_1 = 1, b_2 = d - 2 \geq 1$, and we want to show that for $n \geq 3$, $b_n \geq (d-2)(d-1)^{n-2} + 1$. Now, this is true for $n = 3$, since $b_3 = (d-2)(d-1) + 1$. By induction, suppose $b_{n-1} \geq (d-2)(d-1)^{n-3} + 1$, then

$$b_n \geq ((d-2)(d-1)^{n-3} + 1)(d-1) + (-1)^{n-1}$$
$$= (d-2)(d-1)^{n-2} + (d-1) + (-1)^{n-1}$$
$$\geq (d-2)(d-1)^{n-2} + 1,$$

as desired. Therefore, $b_n \geq 1$ for all n, and $b_n \to \infty$.

So the integer $c := c(\alpha)$ does indeed exist. We claim that for all $k \leq c$ we have

$$M^{(k)}(\alpha) = \begin{cases} \pm N(\alpha)^{b_k}/\alpha_d & \text{if } 2 \nmid k \\ \pm N(\alpha)^{b_k} \cdot \alpha_1 & \text{if } 2 \mid k \end{cases} \tag{4}$$

Note that $\alpha_1, \alpha_d \in \mathbb{R}$, since there is no other conjugate of the same absolute value. Therefore, the sign in (4) has to be chosen such that the value is positive. We prove the claim by induction.

For $k = 1$, we calculate

$$M^{(1)}(\alpha) = M(\alpha) = \pm \alpha_1 \cdot \ldots \cdot \alpha_{d-1} = \pm \frac{N(\alpha)}{\alpha_d} = \pm \frac{N(\alpha)^{b_1}}{\alpha_d},$$

by assumption (i). Now, assume that (4) is correct for a fixed $k < c$. If k is even, then by assumption (i) we have

$$M^{(k+1)}(\alpha) = M(\pm N(\alpha)^{b_k} \cdot \alpha_1) = \pm N(\alpha)^{b_k \cdot (d-1)} \cdot \alpha_1 \cdot \ldots \cdot \alpha_{d-1}$$
$$= \pm \frac{N(\alpha)^{b_k \cdot (d-1)+1}}{\alpha_d} = \pm \frac{N(\alpha)^{b_{k+1}}}{\alpha_d}.$$

Here we have used that $k < c$ and hence $|N(\alpha)^{b_k} \cdot \alpha_d| < 1$.

If k is odd, then by assumption (ii) we have

$$M^{(k+1)}(\alpha) = M\left(\pm \frac{N(\alpha)^{b_k}}{\alpha_d}\right) = \pm \frac{N(\alpha)^{b_k}}{\alpha_d} \cdot \frac{N(\alpha)^{b_k}}{\alpha_{d-1}} \cdot \ldots \cdot \frac{N(\alpha)^{b_k}}{\alpha_2}$$

$$= \pm \frac{N(\alpha)^{b_k \cdot (d-1)}}{\alpha_2 \cdot \ldots \cdot \alpha_{d-1}} = \pm N(\alpha)^{b_k \cdot (d-1)-1} \cdot \alpha_1 = \pm N(\alpha)^{b_{k+1}} \cdot \alpha_1.$$

Here we have used that $k < c$ and hence $|\frac{N(\alpha)^{b_k}}{\alpha_1}| < 1$. This proves the claim. Moreover, the proof of the claim shows that $M^{(k+1)}(\alpha) > M^{(k)}(\alpha_1)$ for all $k \in \{0, \ldots, c-1\}$.

Now, we calculate $M^{(c+1)}(\alpha)$. By definition of c, every conjugate of $M^{(c)}(\alpha)$ is greater than 1 in absolute value. Therefore, $M^{(c+1)}(\alpha) \in \mathbb{N}$. It follows, that $M^{(c+2)}(\alpha) = M^{(c+1)}(\alpha)$. Hence, $\#\mathcal{O}_M(\alpha_1) = c+2$ as claimed. $\square$

It remains to prove the existence of an algebraic number of degree d satisfying the assumptions of Proposition 1 for an arbitrary c.

The strategy is as follows: We will prove the locations of the roots of a class of irreducible polynomials satisfying assumptions (i) and (ii) from Proposition 1, then by Proposition 1, show that any root of one of the polynomials in the class will have desired degree, norm and orbit size.

We fix for the rest of this section arbitrary integers $d \geq 3, c \geq 2$ and $l \in \mathbb{Z}\setminus\{\pm 1, 0\}$. Moreover, we define

$$f_n(x) = x \cdot (x^{d-2} - 2) \cdot (x - n) + l$$

and denote the roots of f_n by $\alpha_1^{(n)}, \ldots, \alpha_d^{(n)}$ ordered such that

$$|\alpha_1^{(n)}| \geq |\alpha_2^{(n)}| \geq \cdots \geq |\alpha_d^{(n)}|.$$

Lemma 1 *Let $n \geq |l| + 3$ be an integer. With the notation from above we have*

$$\alpha_1^{(n)} \in \left(n - \frac{1}{n}, n + \frac{1}{n}\right), \quad \alpha_d^{(n)} \in \left(-\frac{|l|}{n}, -\frac{1}{2n}\right) \cup \left(\frac{1}{2n}, \frac{|l|}{n}\right),$$

$$|\alpha_i^{(n)}| \in \left(1, \sqrt[d-2]{3 - \frac{1}{d}}\right)$$

for all $i \in \{2, \ldots, d-1\}$. Moreover, $\alpha_d^{(n)}$ is negative if and only if $\alpha_1^{(n)} < n$.

Proof We apply Rouché's theorem and first prove the location of $\alpha_1^{(n)}$. Let z be any complex number with $|z| = n + 1/n$. Then

$$|z \cdot (z^{d-2} - 2) \cdot (z - n)|$$

$$\geq \left| n + \frac{1}{n} \right| \cdot \left| \left(n + \frac{1}{n} \right)^{d-2} - 2 \right| \cdot \frac{1}{n}$$

$$= \left| 1 + \frac{1}{n^2} \right| \cdot \left| \left(n + \frac{1}{n} \right)^{d-2} - 2 \right|$$

$$> |l|.$$

Hence by Rouché's theorem, f_n has exactly as many roots of absolute value $< n + 1/n$ as $x \cdot (x^{d-2} - 2) \cdot (x - n)$, so f_n has d roots of absolute value $< n + 1/n$. Now, let z be any complex number with $|z| = n - 1/n$, suppose that $n = |l| + m$ where $m \geq 3$. Then

$$\left| z \cdot (z^{d-2} - 2) \cdot (z - n) \right| \geq \left| n - \frac{1}{n} \right| \cdot \left| \left(n - \frac{1}{n} \right)^{d-2} - 2 \right| \cdot \frac{1}{n}$$

$$\geq \left| n - \frac{1}{n} \right| \cdot \left| \left(n - \frac{1}{n} \right) - 2 \right| \cdot \frac{1}{n}$$

$$= \left(|l| + m - \frac{1}{|l| + m} \right) \left(|l| + m - \frac{1}{|l| + m} - 2 \right) \cdot \frac{1}{|l| + m}$$

$$= \left(1 - \frac{1}{(|l| + m)^2} \right) \left(|l| - \frac{1}{|l| + m} + m - 2 \right)$$

$$= |l| - \frac{|l|}{(|l| + m)^2} - \frac{1}{|l| + m} + (m - 2) + \frac{1}{(|l| + m)^3}$$

$$- \frac{m}{(|l| + m)^2} + \frac{2}{(|l| + m)^2}$$

$$> |l|,$$

since $m \geq 3$. Again by Rouché's theorem, f_n has $d - 1$ roots of absolute value $< n - 1/n$. Since f_n has no roots on the circle $|z| = n - 1/n$, f_n has a single root in

$(-n - 1/n, -n + 1/n) \cup (n - 1/n, n + 1/n)$. Now,

$$\left| \left(-n - \frac{1}{n} \right) \left(\left(-n - \frac{1}{n} \right)^{d-2} - 2 \right) \left(-2n - \frac{1}{n} \right) \right|$$

$$\geq (|l| + 2) \left| \left(n + \frac{1}{n} \right)^{d-2} - 2 \right| \left(2n + \frac{1}{n} \right)$$

$$\geq (|l| + 2) |l| (2(|l| + 2))$$

$$\geq (|l| + 2) |l| (2|l| + 4)$$

$$\geq |l|^2 > |l|.$$

Similarly,

$$\left| \left(-n + \frac{1}{n} \right) \left(\left(-n + \frac{1}{n} \right)^{d-2} - 2 \right) \left(-2n + \frac{1}{n} \right) \right| \geq 2|l|^2 > |l|.$$

Since

$$\left(-n - \frac{1}{n} \right) \left(\left(-n - \frac{1}{n} \right)^{d-2} - 2 \right) \left(-2n - \frac{1}{n} \right)$$

has the same sign as

$$\left(-n + \frac{1}{n} \right) \left(\left(-n + \frac{1}{n} \right)^{d-2} - 2 \right) \left(-2n + \frac{1}{n} \right),$$

$f_n(-n + 1/n)$ has the same sign as $f_n(-n - 1/n)$. Therefore, since there is only one root in the annulus $|z| \in (n - 1/n, n + 1/n)$, which is necessarily real, f_n cannot have any root in the interval $(-n - 1/n, -n + 1/n)$, thus f_n has a single root in the interval $(n - 1/n, n + 1/n)$.

To prove the location of $\alpha_d^{(n)}$, let z be any complex number with $|z| = |l|/n$. Then,

$$|z \cdot (z^{d-2} - 2) \cdot (z - n)| \geq \frac{|l|}{n} \cdot \left(2 - \frac{|l|}{n} \right) \cdot \left(n - \frac{|l|}{n} \right)$$

$$= 2|l| - 2\frac{|l|^2}{n^2} - \frac{|l|^2}{n} + \frac{|l|^3}{n^3} > 2|l| - 2\frac{|l|^2}{n^2} - \frac{|l|^2}{n}$$

$$\geq 2|l| - |l|\frac{|l|^2 + 4|l|}{(|l| + 2)^2} > |l|.$$

By Rouché's theorem, f_n has exactly as many roots of absolute value $< |l|/n$ as the polynomial $x \cdot (x^{d-2} - 2) \cdot (x - n)$. This is, f_n has exactly one root of absolute value $< |l|/n$. This root is necessarily real. A straightforward computation shows

that $f_n(\pm 1/(2n))$ have the same sign as $f_n(0)$. Hence f_n cannot have any root in the interval $(-1/(2n), 1/(2n))$.

To show the location of $\alpha_i^{(n)}$ for all $i \in \{2, \ldots, d-1\}$, let z be any complex number with $|z| = 1$. Then,

$$|z \cdot (z^{d-2} - 2) \cdot (z - n)| = |z^{d-2} - 2| \cdot |z - n|$$
$$\geq n - 1 > |l|,$$

so f_n has a single root of absolute value < 1. The argument above also shows that f_n has no roots on the circle $|z| = 1$. Now, let z be any complex number with $|z| = \sqrt[d-2]{3 - 1/d}$. Then,

$$|z \cdot (z^{d-2} - 2) \cdot (z - n)|$$
$$\geq \left(3 - \frac{1}{d}\right)^{\frac{1}{d-2}} \cdot \left(1 - \frac{1}{d}\right) \cdot \left(n - (3 - \frac{1}{d})^{\frac{1}{d-2}}\right).$$

By elementary calculus,

$$\left(3 - \frac{1}{d}\right)\left(1 - \frac{1}{d}\right)^{d-2} > 1 \quad \forall\, d \geq 3,$$

which gives

$$|z \cdot (z^{d-2} - 2) \cdot (z - n)| \geq n - \left(3 - \frac{1}{d}\right)^{\frac{1}{d-2}} > |l|,$$

where the last inequality follows from the assumption $n \geq |l| + 3$. Hence, by Rouché's theorem, f_n has $d - 1$ roots of absolute value less than $\sqrt[d-2]{3 - 1/d}$. Therefore, f_n has exactly $d - 2$ roots with absolute values in the interval $(1, \sqrt[d-2]{3 - 1/d})$.

The last part of the lemma is obvious, since $x \cdot (x^{d-2} - 2) \cdot (x - n)$ changes the sign at 0 and at n in the same way. $\qquad\square$

Lemma 2 *Let $n \geq |l| + 3$. Then f_n is irreducible in $\mathbb{Q}[x]$ whenever l is odd.*

Proof From Lemma 1 we know $\alpha_1^{(n)} > |l|$. Hence, $\alpha_1^{(n)}$ must be a conjugate of the only root of f_n which is less than 1 in absolute value. If f_n would be reducible, then some product of the elements $\alpha_2^{(n)}, \ldots, \alpha_{d-1}^{(n)}$ must be a divisor of l. But every such product lies strictly between 1 and 3. Since 2 is no divisor of l by assumption, f_n is necessarily irreducible. $\qquad\square$

Lemma 3 *Let p be a prime and let $f = x^d + a_{d-1}x^{d-1} + \cdots + a_2 x^2 + a_1 x + a_0 \in \mathbb{Z}[x]$ be such that $p \mid a_i$ for all $i \in \{0, \ldots, d-1\}$ and $p^2 \nmid a_2$. Then either f has a divisor of degree ≤ 2 or f is irreducible.*

Proof This follows exactly as the classical Eisenstein criterion. Assume, that $f = g \cdot h$, where

$$g(x) = x^r + g_{r-1}x^{r-1} + \cdots + g_0 \quad \text{and} \quad h(x) = x^s + h_{s-1}x^{s-1} + \cdots + h_0 \in \mathbb{Z}[x]$$

with $r, s \geq 3$. Since the reduction of $g \cdot h$ modulo p is equal to $x^d \in \mathbb{Z}/p\mathbb{Z}[x]$ and $\mathbb{Z}/p\mathbb{Z}[x]$ is an integral domain, we know that each coefficient of g and h is divisible by p. It follows $p^2 \mid g_0h_2 + g_1h_1 + g_2h_0 = a_2$, which is a contradiction. □

Lemma 4 *Let $n \geq |l| + 3$ and $|l|$ both be even. Then f_n is irreducible.*

Proof We first note that f_n does not have a factor of degree 1. Otherwise, some divisor a of l would be a root of f_n. But $|a(a - n)| \geq n - 1 \geq |l| + 1$. Hence, in particular, $f_n(a) \neq 0$ for all $a \mid l$. It follows, that f_n is irreducible for $d = 3$. From now on we assume $d \geq 4$.

If l and n are even, then

$$f_n(x) = x(x^{d-2} - 2)(x - n) + l = x^d - nx^{d-1} - 2x^2 + 2nx + l$$

is—by Lemma 3—irreducible if it does not have a factor of degree 2.

Since $\alpha_1^{(n)}$ is larger than $|l|$ (which is the absolute value of the product of all roots of f_n), it must be conjugate to $\alpha_d^{(n)}$ which is the only root of absolute value ≤ 1. If $\alpha_d^{(n)}$ would be the only conjugate of $\alpha_1^{(n)}$, then $\alpha_1^{(n)} + \alpha_d^{(n)} \in \mathbb{Z}$. This is not possible by Lemma 1. This means, that there is no factor of degree 2, having $\alpha_1^{(n)}$ or $\alpha_d^{(n)}$ as a root. This proves that f_n is irreducible for $d = 4$. For $d \geq 5$ the only possibility of a divisor of degree 2 is $x^2 - (\alpha_i^{(n)} + \alpha_j^{(n)})x + \alpha_i^{(n)}\alpha_j^{(n)}$, for $i \neq j \in \{2, \ldots, d - 1\}$. By Lemma 1, we have

$$|\alpha_i^{(n)}\alpha_j^{(n)}| > 1 \quad \text{and} \quad |\alpha_i^{(n)}\alpha_j^{(n)}| < \sqrt[d-2]{3 - \frac{1}{d}}^2 < 2.$$

Hence, such polynomial is not in $\mathbb{Z}[x]$. We conclude that f_n does not have a factor of degree ≤ 2 and therefore f_n is irreducible. □

Theorem 5 *Let $d \geq 3$ and $l \in \mathbb{Z}\backslash\{\pm 1, 0\}$ such that $(d, l) \notin \{(3, 2), (3, -2)\}$. Moreover, let $b_1, b_2, \ldots$ be the sequence from Proposition 1 and $c \geq 2$ be an integer with $c \neq 2$ if $d \in \{3, 4\}$. Then any root α of*

$$f_{|l|^{b_c-1}}(x) = x(x^{d-2} - 2)(x - |l|^{b_c-1}) + l$$

is an algebraic integer of degree d, norm l, and orbit size $c + 2$.

Proof The cases we have to exclude, are those which violate assumption (ii) in Proposition 1 or satisfy $|l^{b_c-1}| < |l| + 3$.

In Lemmas 2 and 4, we proved that α has degree d. Moreover, by Lemma 1, α satisfies assumptions (i) and (ii) from Proposition 1. As usual we denote with $\alpha_1, \ldots, \alpha_d$

the full set of conjugates of α. Then by Lemma 1, we achieve $|\alpha_d l^{b_c}| > |l|/2 \geq 1$ and $|\alpha_1| < |l^{b_c-1}| + 1 \leq |l^{b_c}|$.

Furthermore, we know that

$$|\alpha_1| > |l|^{b_c-1} - 1 \geq |l|^{b_c-1} \quad \text{and} \quad |\alpha_d l^{b_c-1}| < \frac{|l|^{b_c-1+1}}{|l|^{b_c-1}} < 1.$$

Again from Lemma 1 we also have $|\alpha_d l^{b_c-2}| < 1$ and $|\alpha_1| > l^{b_c-2}$, if $c \geq 3$.

What we have shown is, that in the notation from Proposition 1, we have $c(\alpha) = c$, and hence $\#\mathcal{O}_M(\alpha) = c + 2$. □

Remark 1 A closed formula for the recursion $b_1, b_2, \ldots$ is

$$b_n = \frac{1}{d}((d-1)^n + (-1)^{n-1}).$$

So Theorem 5 is fairly effective.

Corollary 2 *For any triple (d, l, k) of integers, with $d \geq 3$, $l \notin \{\pm 1, 0\}$, and $1 \leq k$, there are algebraic integers α with $[\mathbb{Q}(\alpha) : \mathbb{Q}] = d$, $N(\alpha) = l$ and $\#\mathcal{O}_M(\alpha) = k$.*

Proof For $(3, 2, k)$ and $(3, -2, k)$ this is due to Dubickas [10] (note that he states the case $N(\alpha) = 2$, but then $-\alpha$ does the job in the case of negative norm). Together with Theorem 5 and the examples at the beginning of this note, we conclude the corollary. □

3 Behavior of degree 4 units and proof of Theorem 2

In light of Theorem 1, one might ask if arbitrarily long but finite orbits occur for algebraic units. In this section we will prove Theorem 2, which states that the orbit size of an algebraic unit of degree 4 must be 1, 2, or ∞.

Let α be an algebraic unit of degree 4. If α is a root of unity, a Pisot number, a Salem number or an inverse of such number we surely have $\#\mathcal{O}_M(\alpha) \leq 2$. Hence, we may and will assume for the rest of this section that the conjugates of α satisfy

$$|\alpha_1| \geq |\alpha_2| > 1 > |\alpha_3| \geq |\alpha_4|.$$

Denote the Galois group of $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)/\mathbb{Q}$ by G_α. The Galois orbit of any $\beta \in \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ is denoted by $G_\alpha \cdot \beta$.

Then $M(\alpha) = \pm \alpha_1 \alpha_2$ and

$$G_\alpha \cdot (\alpha_1 \alpha_2) \subseteq \{\alpha_1 \alpha_2, \alpha_1 \alpha_3, \alpha_1 \alpha_4, \alpha_2 \alpha_3, \alpha_2 \alpha_4, \alpha_3 \alpha_4\}.$$

Lemma 5 *If $|\alpha_1 \alpha_4| = 1$ or $|\alpha_1 \alpha_3| = 1$, then we have either $\#\mathcal{O}_M(\alpha) = 2$ or $\#\mathcal{O}_M(\alpha) = \infty$.*

Proof If $|\alpha_1\alpha_4| = 1$, then also $|\alpha_2\alpha_3| = 1$, and if $|\alpha_1\alpha_3| = 1$, then also $|\alpha_2\alpha_4| = 1$. In both cases we see that

$$|\alpha_1| = |\alpha_2| \iff |\alpha_3| = |\alpha_4|. \tag{5}$$

We first assume that $\alpha_1 \notin \mathbb{R}$. Then $\alpha_2 = \overline{\alpha_1}$ and hence $|\alpha_1| = |\alpha_2|$. Obviously it is $M(\alpha_1) = \alpha_1\alpha_2$. By our assumptions and (5), all values $|\alpha_1\alpha_3|$, $|\alpha_1\alpha_4|$, $|\alpha_2\alpha_3|$, $|\alpha_2\alpha_4|$, $|\alpha_3\alpha_4|$ are less or equal to 1. Hence $M^{(2)}(\alpha_1) = M(\alpha_1\alpha_2) = \alpha_1\alpha_2$. Therefore, $\#\mathcal{O}_M(\alpha_1) = 2$.

If $\alpha_1 \in \mathbb{R}$ and $|\alpha_1| = |\alpha_2|$, then $\alpha_2 = -\alpha_1$ and $\alpha_4 = -\alpha_3$. Hence, the only nontrivial Galois conjugate of $M(\alpha_1) = \alpha_1^2$ is α_3^2 and lies inside the unit circle. Therefore, $M^{(2)}(\alpha_1) = \alpha_1^2$ and $\#\mathcal{O}_M(\alpha_1) = 2$.

From now on we assume that $|\alpha_1| \neq |\alpha_2|$. Then, by (5), we have

$$|\alpha_1| > |\alpha_2| > 1 > |\alpha_3| > |\alpha_4|$$

and α_1 must be totally real. Moreover, we see that

$$\alpha_1^n, \alpha_2^n, \alpha_3^n, \alpha_4^n \quad \text{are pairwise distinct for all } n \in \mathbb{N}, \tag{6}$$

and

$$(\alpha_1\alpha_2)^n, (\alpha_3\alpha_4)^n, (\alpha_1\alpha_3)^n, (\alpha_2\alpha_4)^n \quad \text{are pairwise distinct for all } n \in \mathbb{N}. \tag{7}$$

We notice that in this situation it is not possible that $|\alpha_1\alpha_3| = 1$, since otherwise $|\alpha_2\alpha_4| < 1$ which contradicts $1 = |\alpha_1\alpha_2\alpha_3\alpha_4|$. Therefore, $|\alpha_1\alpha_4| = 1$, and $\alpha_4 = \pm\alpha_1^{-1}$. It follows that also $\alpha_3 = \pm\alpha_2^{-1}$. This gives natural constraints on the Galois group G_α, namely

$$G_\alpha \subseteq \{\mathrm{id}, (12)(34), (13)(24), (14)(23), (14), (23), (1342), (1243)\} \subseteq S_4.$$

In particular, since G_α is a transitive subgroup of S_4 with order divisible by 4,

$$G_\alpha = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\} \text{ or } \{\mathrm{id}, (1342), (14)(23), (1243)\} \subseteq G_\alpha.$$

In the first case, $G_\alpha \cdot (\alpha_1\alpha_2) = \{\alpha_1\alpha_2, \alpha_3\alpha_4\}$, which implies that $\alpha_1\alpha_2$ is a quadratic unit. Hence $\#\mathcal{O}_M(\alpha) = \#\mathcal{O}_M(\alpha_1\alpha_2) + 1 = 2$.

In the second case, $G_\alpha \cdot (\alpha_1\alpha_2) = \{\alpha_1\alpha_2, \alpha_3\alpha_4, \alpha_1\alpha_3, \alpha_2\alpha_4\}$. Note that $\alpha_1\alpha_2$ is still of degree 4 by (7). Hence $M^{(2)}(\alpha_1) = M(\alpha_1\alpha_2) = \pm\alpha_1^2\alpha_2\alpha_3 = \alpha_1^2$. By (6) it follows that $M^{(3)}(\alpha) = M(\alpha_1^2) = (\alpha_1\alpha_2)^2 = M(\alpha)^2$. Now, by induction and (7) and (6), it follows that $M^{(n)}(\alpha_1) = \alpha_1^{2^n}$ for all even $n \in \mathbb{N}$. Hence $\#\mathcal{O}_M(\alpha_1) = \infty$. $\square$

From now on, we assume:

$$|\alpha_1\alpha_4| \neq 1 \neq |\alpha_1\alpha_3|. \tag{8}$$

Lemma 6 *Assuming* (8), *if* $\alpha_1^n = \alpha_2^n$ *or* $\alpha_3^n = \alpha_4^n$ *for some* $n \in \mathbb{N}$, *then* $\#\mathcal{O}_M(\alpha_1) = 2$.

Proof If $\alpha_1^n = \alpha_2^n$ for some $n \in \mathbb{N}$, then α_1/α_2 is a root of unity. Since none of the elements α_1/α_3, α_1/α_4, α_2/α_3, α_2/α_4, α_3/α_1, α_3/α_2, α_4/α_1, α_4/α_2 lies on the unit circle, we have

$$G_\alpha \cdot \left(\frac{\alpha_1}{\alpha_2}\right) \subseteq \left\{\frac{\alpha_1}{\alpha_2}, \frac{\alpha_2}{\alpha_1}, \frac{\alpha_3}{\alpha_4}, \frac{\alpha_4}{\alpha_3}\right\}.$$

Hence

$$G_\alpha \subseteq \{\text{id}, (12), (12)(34), (13)(24), (14)(23), (1324), (1423)\}.$$

This implies

$$M^{(2)}(\alpha_1) = M(\pm\alpha_1\alpha_2) = \pm\alpha_1\alpha_2 = M(\alpha_1),$$

and hence $\#\mathcal{O}_M(\alpha_1) = 2$. The same proof applies if $\alpha_3^n = \alpha_4^n$. $\quad\square$

Lemma 7 *Assuming* (8) *and* $\#\mathcal{O}_M(\alpha_1) > 2$, *we have*

(a) $|\alpha_1\alpha_2| > 1$, $|\alpha_1\alpha_3| > 1$.
(b) $|\alpha_3\alpha_4| < 1$, $|\alpha_2\alpha_4| < 1$.
(c) *One of the values* $|\alpha_1\alpha_4|$ *and* $|\alpha_2\alpha_3|$ *is* < 1 *and the other is* > 1.
(d) α_1^n, α_2^n, α_3^n, α_4^n *are pairwise distinct for all* $n \in \mathbb{N}$.
(e) $(\alpha_1\alpha_2)^n$, $(\alpha_3\alpha_4)^n$, $(\alpha_1\alpha_3)^n$, $(\alpha_2\alpha_4)^n$ *are pairwise distinct for all* $n \in \mathbb{N}$.

Proof Obviously $|\alpha_1\alpha_2| > 1$ and $|\alpha_3\alpha_4| < 1$. Moreover, $1 \neq |\alpha_1\alpha_3| \geq |\alpha_2\alpha_4|$ and $|\alpha_1\alpha_3| \cdot |\alpha_2\alpha_4| = 1$. This means $|\alpha_1\alpha_3| > 1$ and $|\alpha_2\alpha_4| < 1$, proving parts (a) and (b).

Since $|\alpha_1\alpha_4| \cdot |\alpha_2\alpha_3| = 1$ and $|\alpha_1\alpha_4| \neq 1$, part (c) follows.

The elements α_1 and α_2 lie outside the unit circle, and α_3 and α_4 lie inside or on the unit circle. Hence, the only possibilities for (d) to fail are $\alpha_1^n = \alpha_2^n$ or $\alpha_3^n = \alpha_4^n$ for some $n \in \mathbb{N}$. By the previous lemma, both implies $\#\mathcal{O}_M(\alpha_1) = 2$, which is excluded by our assumptions.

Part (e) follows immediately from (a), (b) and (d). $\quad\square$

Lemma 8 *If* $M^{(3)}(\alpha_1) = M(\alpha_1)^2$ *and* $\#\mathcal{O}_M(\alpha_1) > 2$, *then* $\#\mathcal{O}_M(\alpha_1) = \infty$.

Proof This is true if assumption (8) is not satisfied, by Lemma 5. If we assume (8), then by Lemma 7 (d) and (e), we are in the same situation as at the end of the proof of Lemma 5. Hence, an easy induction proves the claim. $\quad\square$

We now complete the proof of the statement that $\#\mathcal{O}_M(\alpha_1) \in \{1, 2, \infty\}$. It suffices to prove this under the assumption (8). From now on we assume $\#\mathcal{O}_M(\alpha) > 2$ and show that this implies $\#\mathcal{O}_M(\alpha) = \infty$. By Lemma 7, we have

$$M^{(2)}(\alpha) \in \{\pm\alpha_1^2\alpha_2\alpha_3, \pm\alpha_1^3\alpha_2\alpha_3\alpha_4, \pm\alpha_1^2\alpha_2^2\alpha_3^2, \pm\alpha_1^2\alpha_2\alpha_4, \pm\alpha_1\alpha_2^2\alpha_3\}$$

$$= \left\{\pm\frac{\alpha_1}{\alpha_4}, \pm\alpha_1^2, \pm\frac{1}{\alpha_4^2}, \pm\frac{\alpha_1}{\alpha_3}, \pm\frac{\alpha_2}{\alpha_4}\right\} \tag{9}$$

In two of these cases the orbit of α can be determined immediately:

- If $M^{(2)}(\alpha) = \pm\alpha_1^2$, then (since we have $\#\mathcal{O}_M(\alpha) > 2$) it is $\alpha_1^n \neq \alpha_2^n$ for all $n \in \mathbb{N}$. Hence $M^{(3)}(\alpha) = M(\alpha)^2$ which implies $\#\mathcal{O}_M(\alpha) = \infty$.
- Similarly, if $M^{(2)}(\alpha) = \pm1/\alpha_4^2$, then (since $\#\mathcal{O}_M(\alpha) > 2$) it is $\alpha_3^n \neq \alpha_4^n$ for all $n \in \mathbb{N}$. Hence $M^{(3)}(\alpha) = M(\alpha_4^2) = M(\alpha)^2$ and again $\#\mathcal{O}_M(\alpha) = \infty$.

We now study the other three cases.

3.1 The case $M^{(2)}(\alpha) = \pm\alpha_1/\alpha_4$

This case occurs if $\alpha_1\alpha_3 \in G_\alpha \cdot (\alpha_1\alpha_2)$, and

- $|\alpha_1\alpha_4| > 1$ but $\alpha_1\alpha_4 \notin G_\alpha \cdot (\alpha_1\alpha_2)$, or
- $|\alpha_2\alpha_3| > 1$ but $\alpha_2\alpha_3 \notin G_\alpha \cdot (\alpha_1\alpha_2)$.

In both cases the only possibilities for G_α are the following copies of the cyclic group C_4 and the dihedral group D_8:

(I) $C_4 = \{\mathrm{id}, (1342), (14)(23), (1243)\}$, or
(II) $D_8 = \{\mathrm{id}, (1243), (14)(23), (1342), (12)(34), (13)(24), (14), (23)\}$.

In both cases $\{\alpha_1/\alpha_4, \alpha_3/\alpha_2, \alpha_4/\alpha_1, \alpha_2/\alpha_3\}$ is a full set of conjugates of α_1/α_4. It follows that

$$M^{(3)}(\alpha) = M\left(\frac{\alpha_1}{\alpha_4}\right) = \pm\frac{\alpha_1}{\alpha_4} \cdot \frac{\alpha_2}{\alpha_3} = (\alpha_1\alpha_2)^2 = M(\alpha)^2$$

Hence, by Lemma 8 we have $\#\mathcal{O}_M(\alpha) = \infty$.

3.2 The case $M^{(2)}(\alpha) = \pm\frac{\alpha_1}{\alpha_3}$

This case occurs if $\alpha_1\alpha_3 \notin G_\alpha \cdot (\alpha_1\alpha_2)$, and $|\alpha_1\alpha_4| > 1$, and $\alpha_1\alpha_4 \in G_\alpha \cdot (\alpha_1\alpha_2)$.

Hence, the only possibilities for G_α are the following copies of the cyclic group C_4 and the dihedral group D_8:

(I) $C_4 = \{\mathrm{id}, (1234), (13)(24), (1432)\}$, or
(II) $D_8 = \{\mathrm{id}, (1234), (13)(24), (1432), (12)(34), (14)(23), (13), (24)\}$.

In both cases $\{\alpha_1/\alpha_3, \alpha_2/\alpha_4, \alpha_3/\alpha_1, \alpha_4/\alpha_2\}$ is a full set of Galois conjugates of α_1/α_3. It follows that

$$M^{(3)}(\alpha) = M\left(\frac{\alpha_1}{\alpha_3}\right) = \pm\frac{\alpha_1}{\alpha_3} \cdot \frac{\alpha_2}{\alpha_4} = (\alpha_1\alpha_2)^2 = M(\alpha)^2$$

Hence, again we have $\#\mathcal{O}_M(\alpha) = \infty$ by Lemma 8.

3.3 The case $M^{(2)}(\alpha) = \pm\frac{\alpha_2}{\alpha_4}$

This case occurs if $\alpha_1\alpha_3 \notin G_\alpha \cdot (\alpha_1\alpha_2)$, and $|\alpha_2\alpha_3| > 1$, and $\alpha_2\alpha_3 \in G_\alpha \cdot (\alpha_1\alpha_2)$.

Hence, the only possibilities for G_α are the following copies of the cyclic group C_4 and the dihedral group D_8:

(I) $C_4 = \{\text{id}, (1234), (13)(24), (1432)\}$, or
(II) $D_8 = \{\text{id}, (1234), (13)(24), (1432), (12)(34), (14)(23), (13), (24)\}$.

In both cases $\{\alpha_2/\alpha_4, \alpha_3/\alpha_1, \alpha_4/\alpha_2, \alpha_1/\alpha_3\}$ is a full set of conjugates of α_2/α_4. It follows that

$$M^{(3)}(\alpha) = M\left(\frac{\alpha_2}{\alpha_4}\right) = \pm\frac{\alpha_2}{\alpha_4} \cdot \frac{\alpha_1}{\alpha_3} = \pm(\alpha_1\alpha_2)^2 = M(\alpha)^2$$

Hence, also in this case we have $\#\mathcal{O}_M(\alpha) = \infty$.

This concludes the proof of Theorem 2. We now prove Corollary 1:

Proof of Corollary 1 Let α be an algebraic unit of degree 4. We set

$$a_n = \log(M^{(n)}(\alpha))$$

for all $n \in \mathbb{N}$. If $\#\mathcal{O}_M(\alpha) \leq 2$, then $a_{n+1} = a_n$ for all $n \in \mathbb{N}$. If $\#\mathcal{O}_M(\alpha) = \infty$, then Theorem 2 tells us $a_3 = 2a_1$. Moreover, $M^{(4)}(\alpha) = M(M^{(3)}(\alpha)) = M(M(\alpha)^2) = M(M(\alpha))^2 = M^{(2)}(\alpha)^2$. Hence, $a_4 = 2a_2$, and by induction we find $a_{n+1} = 2a_{n-1}$, proving the claim. $\qquad\square$

4 Symmetric and alternating Galois groups

In this section we will prove Theorem 3. We know that $\#\mathcal{O}_M(\alpha) \in \{1, 2, \infty\}$ whenever α is an algebraic unit of degree ≤ 4. (We note in passing that the orbit size for units of degree less than 4 is trivially 1 or 2.) So we assume from now on that α is an algebraic unit with $[\mathbb{Q}(\alpha) : \mathbb{Q}] = d \geq 5$. Denote by G_α the Galois group of the Galois closure of $\mathbb{Q}(\alpha)$. We assume that G_α contains a subgroup isomorphic to A_d, so G_α is either the full symmetric group or the alternating group. Every self-reciprocal polynomial admits natural restrictions on which permutations of the zeros are given by field automorphisms. Hence, α cannot be conjugated to $\pm$ a Salem number (see [5] for more precise statements on the structure of the Galois group G_α, when α is a Salem number). If one of $\pm\alpha^{\pm 1}$ is conjugated to a Pisot number, then surely $\#\mathcal{O}_M(\alpha) \in \{1, 2\}$. Hence, we assume from now on that none of $\pm\alpha^{\pm 1}$ is conjugated to a Pisot number.

Hence, if we denote by $\alpha_1, \ldots, \alpha_d$ the Galois conjugates of α, we assume

$$|\alpha_1| \geq |\alpha_2| \geq \cdots \geq |\alpha_r| > 1 \geq |\alpha_{r+1}| \geq \cdots \geq |\alpha_d|,$$
$$\text{where } r \in \{2, \ldots, d-2\} \text{ and } 1 > |\alpha_{d-1}|. \tag{10}$$

We identify G_α with a subgroup of S_d, by the action on the indices of $\alpha_1, \ldots, \alpha_d$. In particular, for any $\sigma \in A_d$ and any $f_1, \ldots, f_d \in \mathbb{Z}$ the element

$$\sigma \cdot (\alpha_1^{f_1} \cdot \ldots \cdot \alpha_d^{f_d}) := \alpha_{\sigma(1)}^{f_1} \cdot \ldots \cdot \alpha_{\sigma(d)}^{f_d}$$

is a Galois conjugate of $\alpha_1^{f_1} \cdot \ldots \cdot \alpha_d^{f_d}$.

Lemma 9 *Let $i, j, k, l \in \{1, \ldots, d\}$ be pairwise distinct, and let $f_1, \ldots, f_d \in \mathbb{Z}$. Then*

(a) $(i, j, k) \cdot (\alpha_1^{f_1} \cdots \alpha_d^{f_d}) = \alpha_1^{f_1} \cdots \alpha_d^{f_d} \iff f_i = f_j = f_k$.

(b) $(i, j)(k, l) \cdot (\alpha_1^{f_1} \cdots \alpha_d^{f_d}) = \alpha_1^{f_1} \cdots \alpha_d^{f_d} \iff f_i = f_j$ and $f_k = f_l$.

Proof In both statements, the implication $\Longleftarrow$ is trivial. Let's start with the other implication in (a). We have

$$(i, j, k) \cdot (\alpha_1^{f_1} \cdots \alpha_d^{f_d}) = \alpha_1^{f_1} \cdots \alpha_d^{f_d} \implies \alpha_j^{f_i - f_j} \cdot \alpha_k^{f_j - f_k} \cdot \alpha_i^{f_k - f_i} = 1.$$

Since $d \geq 5$, we may choose two conjugates of α not among α_i, α_j, α_k—say α_p and α_q. Since G_α contains A_d, the elements $(i, j)(p, q)$, $(i, k)(p, q)$, $(j, k)(p, q)$, (i, j, k), and (i, k, j) are all contained in G_α. Applying these automorphisms to $\alpha_j^{f_i - f_j} \cdot \alpha_k^{f_j - f_k} \cdot \alpha_i^{f_k - f_i} = 1$, yields

$$\alpha_j^{f_i - f_j} \cdot \alpha_k^{f_j - f_k} \cdot \alpha_i^{f_k - f_i} = 1 = \alpha_j^{f_i - f_j} \cdot \alpha_i^{f_j - f_k} \cdot \alpha_k^{f_k - f_i}$$

$$\alpha_i^{f_i - f_j} \cdot \alpha_j^{f_j - f_k} \cdot \alpha_k^{f_k - f_i} = 1 = \alpha_k^{f_i - f_j} \cdot \alpha_j^{f_j - f_k} \cdot \alpha_i^{f_k - f_i}$$

$$\alpha_k^{f_i - f_j} \cdot \alpha_i^{f_j - f_k} \cdot \alpha_j^{f_k - f_i} = 1 = \alpha_i^{f_i - f_j} \cdot \alpha_k^{f_j - f_k} \cdot \alpha_j^{f_k - f_i}.$$

Hence

$$\left(\frac{\alpha_i}{\alpha_k}\right)^{2f_k - f_i - f_j} = 1, \quad \left(\frac{\alpha_i}{\alpha_k}\right)^{2f_i - f_j - f_k} = 1, \quad \text{and} \quad \left(\frac{\alpha_i}{\alpha_k}\right)^{2f_j - f_k - f_i} = 1.$$

But α_i / α_k is not a root of unity, since it is a Galois conjugate of α_1 / α_d, which lies outside the unit circle. It follows that

$$2f_k - f_i - f_j = 2f_i - f_j - f_k = 2f_j - f_k - f_i = 0,$$

and hence $f_i = f_j = f_k$. This proves part (a).

Part (b) follows similarly: $(i, j)(k, l) \cdot (\alpha_1^{f_1} \cdots \alpha_d^{f_d}) = \alpha_1^{f_1} \cdots \alpha_d^{f_d}$ implies

$$\alpha_i^{f_j} \cdot \alpha_j^{f_i} \cdot \alpha_k^{f_l} \cdot \alpha_l^{f_k} = \alpha_i^{f_i} \cdot \alpha_j^{f_j} \cdot \alpha_k^{f_k} \cdot \alpha_l^{f_l}.$$

Without loss of generality, we assume $f_j \geq f_i$ and $f_k \geq f_l$. Using that $(i,l)(j,k)$ is an element of G_α, we get

$$\left(\frac{\alpha_j}{\alpha_i}\right)^{f_j - f_i} = \left(\frac{\alpha_k}{\alpha_l}\right)^{f_k - f_l} \quad \text{and} \quad \left(\frac{\alpha_k}{\alpha_l}\right)^{f_j - f_i} = \left(\frac{\alpha_j}{\alpha_i}\right)^{f_k - f_l}.$$

Multiplying both equations yields

$$\left(\frac{\alpha_j}{\alpha_i}\right)^{(f_j - f_i) + (f_k - f_l)} = \left(\frac{\alpha_k}{\alpha_l}\right)^{(f_j - f_i) + (f_k - f_l)},$$

and hence

$$\left(\frac{\alpha_j \cdot \alpha_l}{\alpha_i \cdot \alpha_k}\right)^{(f_j - f_i) + (f_k - f_l)} = 1.$$

Again, $(\alpha_j \cdot \alpha_l)/(\alpha_i \cdot \alpha_k)$ is a Galois conjugate of $(\alpha_1 \cdot \alpha_2)/(\alpha_{d-1} \cdot \alpha_d)$, which lies outside the unit circle, and hence is not a root of unity. Therefore $(f_j - f_i) + (f_k - f_l) = 0$. Since $f_j \geq f_i$ und $f_k \geq f_l$, it follows that $f_j = f_i$ and $f_k = f_l$, proving the lemma. $\square$

Lemma 10 *Let* $f_1, \ldots, f_d$ *be pairwise distinct integers. Then* $[\mathbb{Q}(\alpha_1^{f_1} \cdots \alpha_d^{f_d}) : \mathbb{Q}] = \#G_\alpha$.

Proof The proof is essentially the same as the proof of part (1) in Theorem 1.1 from [2]. Assume there is a $\sigma^{-1} \in G_\alpha \subseteq S_d$ such that $\alpha_1^{f_1} \cdots \alpha_d^{f_d} = \sigma^{-1} \cdot (\alpha_1^{f_1} \cdots \alpha_d^{f_d})$. Then

$$1 = \alpha_1^{f_1 - f_{\sigma(1)}} \cdots \alpha_d^{f_d - f_{\sigma(d)}}. \tag{11}$$

If σ is an odd permutation, then $G_\alpha = S_d$, then it was already proven by Smyth (see Lemma 1 of [20]) that $f_i = f_{\sigma(i)}$ for all i, hence that $\sigma = \mathrm{id}$. If σ is an even permutation, then by repeated application of Lemma 9 to equation (11) above, this is only possible if $f_i - f_{\sigma(i)}$ is the same integer for all $i \in \{1, \ldots, d\}$, say $f_i - f_{\sigma(i)} = k$.

Since $\sigma^{d!} = \mathrm{id}$, it follows that

$$f_1 = k + f_{\sigma(1)} = 2k + f_{\sigma^2(1)} = \ldots = d! \cdot k + f_{\sigma^{d!}(1)} = d! \cdot k + f_1,$$

and hence $k = 0$. Therefore we have $f_i = f_{\sigma(i)}$ for all $i \in \{1, \ldots, d\}$. But by assumption the integers $f_1, \ldots, f_d$ are pairwise distinct, hence, we must again have $\sigma = \mathrm{id}$. Since in either case, $\sigma = \mathrm{id}$, this means that the images of $\alpha_1^{f_1} \cdots \alpha_d^{f_d}$ are distinct under each non-identity element of G_α, so $[\mathbb{Q}(\alpha_1^{f_1} \cdots \alpha_d^{f_d}) : \mathbb{Q}] = \#G_\alpha$. $\square$

Proposition 2 *Let* $M^{(n)}(\alpha) = \alpha_1^{e_1} \cdot \ldots \cdot e_d^{e_d}$ *such that the exponents* $e_1, \ldots, e_d$ *are pairwise distinct. Then* $M^{(n+1)}(\alpha) > M^{(n)}(\alpha)$.

Proof We denote by Z_3 the set of 3-cycles in $G_\alpha \subseteq S_d$. For any $k \in \{1, \ldots, d\}$, the number of 3-cycles which fix k is equal to $(d-1)(d-2)(d-3)/3$. For any pair $k \neq k' \in \{1, \ldots, d\}$, the number of 3-cycles sending k to k' is $(d-2)$. Therefore,

$$\left| \prod_{\tau \in Z_3} \tau \cdot M^{(n)}(\alpha) \right|$$

$$= \left| \alpha_1^{\frac{(d-1)(d-2)(d-3)}{3} e_1 + (d-2) \sum_{k \neq 1} e_k} \cdot \ldots \cdot \alpha_d^{\frac{(d-1)(d-2)(d-3)}{3} e_d + (d-2) \sum_{k \neq d} e_k} \right|. \quad (12)$$

Since α is an algebraic unit, we have

$$\prod_{j=1}^{d} \alpha_j^{\sum_{k=1}^{d} e_k} = \pm 1.$$

Hence, the value in (12) is equal to

$$\left| \prod_{j=1}^{d} \alpha_j^{\left(\frac{(d-1)(d-2)(d-3)}{3} - (d-2) \right) e_j} \right| = M^{(n)}(\alpha)^{\frac{(d-1)(d-2)(d-3)}{3} - (d-2)} > M^{(n)}(\alpha).$$

The last inequality follows from our general hypothesis that $d \geq 5$. Since $e_1, \ldots, e_d$ are assumed to be pairwise distinct, it follows from Lemma 10 that the factors $\tau \cdot M^{(n)}(\alpha)$ in (12) are also pairwise distinct conjugates of $M^{(n)}(\alpha)$. In particular

$$M^{(n+1)}(\alpha) = M(M^n(\alpha)) \geq \left| \prod_{\tau \in Z_3} \tau \cdot M^{(n)}(\alpha) \right| > M^{(n)}(\alpha)$$

which is what we needed to prove. $\square$

Lemma 11 *Let $n \in \mathbb{N}$ and let $M^{(n)}(\alpha) = \alpha_1^{e_1} \cdots \alpha_d^{e_d}$. Then we have:*

(a) $e_i \geq e_{i+1}$ *for all but at most one* $i \in \{1, \ldots, d-1\}$.
(b) *If* $e_i < e_{i+1}$ *for some* $i \in \{2, \ldots, d-1\}$, *then* $e_{i-1} > e_{i+1}$.
(c) *If* $e_i < e_{i+1}$ *for some* $i \in \{1, \ldots, d-2\}$, *then* $e_i > e_{i+2}$.
(d) *If* $e_i < e_{i+1}$ *for some* $i \in \{1, \ldots, d-1\}$, *then*

$$e_1 > e_2 > \cdots > e_{i-1} > e_{i+1} > e_i > e_{i+2} > e_{i+3} > \cdots > e_d.$$

Proof It is known that $M^{(n)}(\alpha)$ is a Perron number, which means that $M^{(n)}(\alpha)$ does not have a Galois conjugate of the same or larger modulus (cf. [10] for this and other properties of values of the Mahler measure). This fact will be used several times in the following proof.

To prove (a), we have two cases: there are three distinct elements $1 \leq i < j < k \leq d$ such that $e_i < e_j < e_k$, or else there exist $1 \leq i < j < k < l \leq d$ such that $e_i < e_j$ and $e_k < e_l$. Assume first that there are three distinct elements $1 \leq i < j < k \leq d$ such that $e_i < e_j < e_k$. Recall that by definition we have $|\alpha_i| \geq |\alpha_j| \geq |\alpha_k|$. Therefore $|\alpha_k|^{e_k - e_i} \leq |\alpha_j|^{e_k - e_i}$, which implies

$$\underbrace{|\alpha_i|^{e_i - e_j}}_{\leq |\alpha_j|^{e_i - e_j}} \cdot |\alpha_j|^{e_j - e_k} \cdot |\alpha_k|^{e_k - e_i} \leq |\alpha_j|^{e_i - e_k} \cdot |\alpha_k|^{e_k - e_i} \leq 1$$

$$\implies |\alpha_i^{e_i} \cdot \alpha_j^{e_j} \cdot \alpha_k^{e_k}| \leq |\alpha_i^{e_j} \cdot \alpha_j^{e_k} \cdot \alpha_k^{e_i}|$$

$$\implies |M^{(n)}(\alpha)| \leq |(i, k, j) \cdot M^{(n)}(\alpha)|.$$

By Lemma 9, $(i, j, k) \cdot M^{(n)}(\alpha) \neq M^{(n)}(\alpha)$ is a Galois conjugate of $M^{(n)}(\alpha)$. This contradicts the fact that $M^{(n)}(\alpha)$ is a Perron number. In particular, it is not possible that $e_i > e_{i+1} > e_{i+2}$ for any $i \in \{1, \ldots, d - 2\}$.

Now assume that we have $1 \leq i < j < k < l \leq d$ such that $e_i < e_j$ and $e_k < e_l$. Then $|\alpha_i| \geq |\alpha_j|$ and $|\alpha_k| \geq |\alpha_l|$ imply

$$|\alpha_i|^{e_j - e_i} \cdot |\alpha_k|^{e_l - e_k} \geq |\alpha_j|^{e_j - e_i} \cdot |\alpha_l|^{e_l - e_k},$$

and hence

$$|\alpha_i^{e_i} \cdot \alpha_j^{e_j} \cdot \alpha_k^{e_k} \cdot \alpha_l^{e_l}| \leq |\alpha_i^{e_j} \cdot \alpha_j^{e_i} \cdot \alpha_k^{e_l} \cdot \alpha_l^{e_k}|.$$

This, however, is equivalent to $|M^{(n)}(\alpha)| \leq |(i, j)(k, l) \cdot M^{(n)}(\alpha)|$, which is not possible by Lemma 9, since $M^{(n)}(\alpha)$ is a Perron number. This proves part (a) of the lemma.

In order to prove part (b), we assume for the sake of contradiction that $e_i < e_{i+1}$ but $e_{i-1} \leq e_{i+1}$ for some $i \in \{2, \ldots, d - 1\}$. By part (a), since we already have $e_i < e_{i+1}$, we know that $e_{i-1} \geq e_i$. We have

$$(i - 1, i, i + 1) \cdot |\alpha_{i-1}|^{e_{i-1}} |\alpha_i|^{e_i} |\alpha_{i+1}|^{e_{i+1}}$$
$$= |\alpha_i|^{e_{i-1}} |\alpha_{i+1}|^{e_i} |\alpha_{i-1}|^{e_{i+1}}.$$

Now,

$$|\alpha_{i-1}|^{e_{i-1} - e_{i+1}} |\alpha_i|^{e_i - e_{i-1}} |\alpha_{i+1}|^{e_{i+1} - e_i}$$
$$= |\alpha_{i-1}|^{e_{i-1} - e_{i+1}} |\alpha_i|^{e_i - e_{i-1}} |\alpha_{i+1}|^{e_{i+1} - e_{i-1}} |\alpha_{i+1}|^{e_{i-1} - e_i}$$
$$\leq |\alpha_{i-1}|^{e_{i-1} - e_{i+1}} |\alpha_i|^{e_i - e_{i-1}} |\alpha_{i-1}|^{e_{i+1} - e_{i-1}} |\alpha_i|^{e_{i-1} - e_i}$$
$$= 1.$$

Therefore,

$$|M^{(n)}(\alpha)| \leq |(i - 1, i, i + 1) \cdot M^{(n)}(\alpha)|,$$

giving a contradiction to $M^{(n)}(\alpha)$ being a Perron number.

Similarly, if $e_i < e_{i+1}$ and $e_i \leq e_{i+2}$, then we know by (a) that $e_{i+1} \geq e_{i+2}$. This implies that $|M^{(n)}(\alpha)| \leq |(i, i+2, i+1) \cdot M^{(n)}(\alpha)|$. This proves part (c).

So far we have proven that if $e_i < e_{i+1}$ for some $i \in \{1, \ldots, d-1\}$, then we have

$$e_1 \geq e_2 \geq \cdots \geq e_{i-1} > e_{i+1} > e_i > e_{i+2} \geq e_{i+3} \geq \cdots \geq e_d.$$

We need to show that all of the above inequalities are strict. Assume that this is not the case, and that $e_k = e_{k+1}$. Then $k, k+1, i, i+1$ must be pairwise distinct. It follows, that

$$|(i, i+1)(k, k+1) \cdot M^{(n)}(\alpha)| = |(i, i+1) \cdot M^{(n)}(\alpha)| > |M^{(n)}(\alpha)|,$$

which is a contradiction. The last inequality just follows from the fact that $|\alpha_i|^{e_{i+1}} \cdot |\alpha_{i+1}|^{e_i} > |\alpha_i|^{e_i} \cdot |\alpha_{i+1}|^{e_{i+1}}$. $\qquad \square$

Lemma 12 *Let $f_1 \geq f_2 \geq \cdots \geq f_k \geq 0$ be integers, with $f_1 \geq 1$, and let $a_1 \geq a_2 \geq \ldots \geq a_d > 0$ be real numbers such that $\prod_{i=1}^{k} a_i > 1$. Then $\prod_{i=1}^{k} a_i^{f_i} > 1$.*

Proof We prove the statement by induction on k, where the base case $k = 1$ is trivial. Now assume that the statement is true for k and that there are real numbers $a_1 \geq \ldots \geq a_{k+1} > 0$, with $\prod_{i=1}^{k+1} a_i > 1$, and integers $f_1 \geq \cdots \geq f_{k+1} \geq 0$, with $f_1 \geq 1$. If $f_1 = f_{k+1}$, then the claim follows immediately. Hence, we assume $f_1 > f_{k+1}$. Set $f_i' = f_i - f_{k+1}$ for all $i \in \{1, \ldots, k+1\}$. Then

$$f_1' \geq f_2' \geq \cdots f_k' \geq f_{k+1}' = 0 \text{ and } f_1' \geq 1.$$

Moreover, $\prod_{i=1}^{k} a_i$ is either greater than or equal to $\prod_{i=1}^{k+1} a_i > 1$ (if $a_{k+1} \leq 1$), or it is a product of real numbers > 1. Hence, our induction hypothesis states $\prod_{i=1}^{k} a_i^{f_i'} > 1$. This implies

$$\prod_{i=1}^{k+1} a_i^{f_i} = \underbrace{\left(\prod_{i=1}^{k+1} a_i \right)^{f_{k+1}}}_{\geq 1} \cdot \left(\prod_{i=1}^{k} a_i^{f_i'} \right) > 1,$$

proving the lemma. $\qquad \square$

Proposition 3 *Let $M^{(n)}(\alpha) = \alpha_1^{e_1} \cdots \alpha_d^{e_d}$. If $e_{i+1} \leq e_i$ for all $i \in \{1, \ldots, d-1\}$, then $M^{(n+1)}(\alpha) > M^{(n)}(\alpha)$.*

Proof We show that $M^{(n)}(\alpha)$ has a non-trivial Galois conjugate outside the unit circle. This immediately implies the claim.

Since α is an algebraic unit, we may assume that $e_d = 0$. Note however, that this uses our assumption $e_{i+1} \leq e_i$ for all i. We set

$$s := \max\{i \in \{1, \ldots, d\} | e_i \neq 0\}.$$

By Proposition 2 we may assume that we have $e_i = e_{i+1}$ for some $i \in \{1, \ldots, d-1\}$. This i is not equal to s, since $e_s \neq 0 = e_{s+1}$ by definition. If $i \notin \{s-1, s+1\}$, then

$$(i, i+1)(s, s+1) \cdot M^{(n)}(\alpha) = \alpha_1^{e_1} \cdots \alpha_{s-1}^{e_{s-1}} \alpha_s^{e_{s+1}} \alpha_{s+1}^{e_s}.$$

If $i = s - 1$, then

$$\begin{aligned}
(s-1, s+1, s) \cdot M^{(n)}(\alpha) &= \alpha_1^{e_1} \cdots \alpha_{s-2}^{e_{s-2}} \alpha_{s-1}^{e_s} \alpha_s^{e_{s+1}} \alpha_{s+1}^{e_{s-1}} \\
&= \alpha_1^{e_1} \cdots \alpha_{s-1}^{e_{s-1}} \alpha_s^{e_{s+1}} \alpha_{s+1}^{e_s}.
\end{aligned}$$

If finally $i = s + 1$, then

$$\begin{aligned}
(s, s+1, s+2) \cdot M^{(n)}(\alpha) &= \alpha_1^{e_1} \cdots \alpha_{s-1}^{e_{s-1}} \alpha_s^{e_{s+2}} \alpha_{s+1}^{e_s} \alpha_{s+2}^{e_{s+1}} \\
&= \alpha_1^{e_1} \cdots \alpha_{s-1}^{e_{s-1}} \alpha_s^{e_{s+1}} \alpha_{s+1}^{e_s}.
\end{aligned}$$

Since $e_{s+1} = 0$, we see that in any case

$$\alpha_1^{e_1} \cdots \alpha_{s-1}^{e_{s-1}} \alpha_{s+1}^{e_s} \text{ is a non-trivial Galois conjugate of } M^{(n)}(\alpha). \tag{13}$$

We will prove that this Galois conjugate lies outside the unit circle. Again we distinguish several cases.

If $s \leq r - 1$, then all of the elements $\alpha_1, \ldots, \alpha_{s+1}$ lie outside the unit circle. Hence $|\alpha_1 \cdots \alpha_{s-1} \alpha_{s+1}| > 1$.

If $s \geq r + 1$, then $|\alpha_1 \cdots \alpha_{s-1} \alpha_{s+1}| = |\alpha_s \alpha_{s+2} \cdots \alpha_d|^{-1} > 1$, since all of $\alpha_s, \ldots, \alpha_d$ lie inside the closed unit disc and $|\alpha_d| < 1$.

Lastly, we consider the case $2 \leq s = r \leq d - 2$. Then surely $|\alpha_1 \cdots \alpha_{r-1}| \geq |\alpha_r|$ and $|\alpha_{r+1}| \geq |\alpha_{r+2} \cdots \alpha_d|$, where the first inequality is strict whenever $r \neq 2$, and the second inequality is strict whenever $r \neq d - 2$. By our general assumption it is $d \geq 5$ and hence $|\alpha_1 \cdots \alpha_{r-1} \alpha_{r+1}| > |\alpha_r \alpha_{r+2} \cdots \alpha_d|$. Since the product of all α_i is ± 1, it follows that $|\alpha_1 \cdots \alpha_{s-1} \alpha_{s+1}| > 1$.

Hence, in any case we have $|\alpha_1| \cdots |\alpha_{s-1}| \cdot |\alpha_{s+1}| > 1$. From our assumption $e_1 \geq \cdots \geq e_d$ it follows by Lemma 12 that $|\alpha_1^{e_1} \cdots \alpha_{s-1}^{e_{s-1}} \alpha_{s+1}^{e_s}| > 1$. Therefore, $M^{(n)}(\alpha)$ has a non-trivial Galois conjugate outside the unit circle [see (13)]. Hence $M^{(n+1)}(\alpha) = M(M^{(n)}(\alpha)) > M^{(n)}(\alpha)$. □

We are now ready to prove Theorem 3.

Proof of Theorem 3 As stated at the beginning of this section, we may assume that $d \geq 5$, and that the elements $\pm\alpha^{\pm 1}$ are neither conjugates of a Pisot, nor a Salem number. Hence, we may assume that the hypothesis (10) is met. Let $n \in \mathbb{N}$ be arbitrary. Then for some $e_1, \ldots, e_d \in \mathbb{N}_0$, we have $M^{(n)}(\alpha) = \alpha_1^{e_1} \cdots \alpha_d^{e_d}$. We have seen in Lemma 11, that one of the following statements applies:

(i) $e_1 \geq e_2 \geq \cdots \geq e_d$, or
(ii) the integers $e_1, \ldots, e_d$ are pairwise distinct.

In case (i), we have $M^{(n+1)}(\alpha) > M^{(n)}(\alpha)$ by Proposition 3. In case (ii), we have $M^{(n+1)}(\alpha) > M^{(n)}(\alpha)$ by Proposition 2. Hence $\#\mathcal{O}_M(\alpha) = \infty$. □

5 Arbitrarily large finite orbit size for certain units

Let $d = 4k$, with an integer $k \geq 3$. Now, we will show that there exist algebraic units of degree d with arbitrarily large orbit size, proving Theorem 4.

Proof of Theorem 4 Let α_1, β_1 be positive real algebraic units satisfying:

1. $[\mathbb{Q}(\beta_1) : \mathbb{Q}] = 2, \beta_1 > 1$,
2. α_1 is a Salem number of degree $2k$.
3. The fields $\mathbb{Q}(\alpha_1)$ and $\mathbb{Q}(\beta_1)$ are linearly disjoint.

For any $k \geq 3$ we can indeed find such α_1 and β_1. Since there are Salem numbers of any even degree ≥ 4 we find an appropriate α_1. Now, we take any prime p which is unrammified in $\mathbb{Q}(\alpha_1)$, and let $\beta_1 > 1$ be an algebraic unit in $\mathbb{Q}(\sqrt{p})$. Note that if the above conditions are met by α_1 and β_1, then they are met by α_1^ℓ and $\beta_1^{\ell'}$, for any $\ell, \ell' \in \mathbb{N}$.

We denote the conjugates of α_1 by $\alpha_2, \cdots, \alpha_{2k}$, with $\alpha_{2k} = \alpha_1^{-1}$, and the conjugate of β_1 is $\beta_2 = \beta_1^{-1}$. Note that $\alpha_2, \cdots, \alpha_{2k-1}$ all lie on the unit circle. By assumption (3) the element $\alpha_1\beta_1$ has degree $4k$ and a full set of Galois conjugates of $\alpha_1\beta_1$ is given by

$$\{\alpha_i \beta_j : (i, j) \in \{1, \ldots, 2k\} \times \{1, 2\}\}.$$

There are two cases. First, if $\beta_1 > \alpha_1$, then $|\alpha_i \beta_1| > 1$ for all $i \in \{1, \cdots, 2k\}$ and $|\alpha_i \beta_2| < |\alpha_i \alpha_6| \leq 1$ for all $i \in \{1, \cdots, 2k\}$, hence,

$$M(\alpha_1\beta_1) = \left| \prod_{n=1}^{2k} \alpha_i \beta_1 \right| = \beta_1^{2k}. \tag{14}$$

For the second case, if $\beta_1 < \alpha_1$, then

$$|\alpha_i \beta_1| > 1 \iff i \in \{1, \cdots, 2k-1\}, \text{ and } |\alpha_i \beta_2| > 1 \iff i = 1.$$

Therefore

$$M(\alpha_1\beta_1) = |\alpha_1\beta_1| \cdot \left| \prod_{n=2}^{2k-1} \alpha_i \beta_1 \right| \cdot |\alpha_1\beta_2| = \alpha_1^2 \beta_1^{2k-2}. \tag{15}$$

We now construct an algebraic unit of degree $4k$ of finite orbit size $> S$. Let $\ell \in \mathbb{N}$ be such that $(\alpha_1^\ell)^{2^S} > \beta_1^{(2k-2)^S}$. Then by (15), we have

- $M(\alpha_1^\ell \beta_1) = (\alpha_1^\ell)^2 \beta_1^{2k-2}$,
- $M^{(2)}(\alpha_1^\ell \beta_1) = M((\alpha_1^\ell)^2)(\beta_1^{2k-2})) = (\alpha_1^\ell)^{2^2} \beta_1^{(2k-2)^2}$, and
- $M^{(n)}(\alpha_1^\ell \beta_1) = (\alpha_1^\ell)^{2^n} \beta_1^{(2k-2)^n}$, for all $n \in \{1, \ldots, S\}$.

Hence, the orbit size of $\alpha_1^\ell \beta_1$ is greater than S. However, there exists $S' > S$ such that $(\alpha_1^\ell)^{2^{S'}} < \beta_1^{(2k-2)^{S'}}$. Assume that S' is minimal with this property. Then we have

$$M^{(S'+1)}(\alpha_1^\ell \beta_1) = (\alpha_1^\ell)^{2^{S'}} \beta_1^{(2k-2)^{S'}} \overset{(14)}{=} (\beta_1^{4^{S'}})^{2k},$$

which is of degree 2. Therefore, the orbit size of $\alpha_1^\ell \beta_1$ is $S' + 2 > S$. □

References

1. Adler, R.L., Marcus, B.: Topological entropy and equivalence of dynamical systems. Mem. Am. Math. Soc. **20**(219), iv+84 (1979). https://doi.org/10.1090/memo/0219
2. Amoroso, F.: Mahler measure on Galois extensions. Int. J. Number Theory **14**(6), 1605–1617 (2018). https://doi.org/10.1142/S1793042118500963
3. Borwein, P., Dobrowolski, E., Mossinghoff, M.J.: Lehmer's problem for polynomials with odd coefficients. Ann. Math. (2) **166**(2), 347–366 (2007). https://doi.org/10.4007/annals.2007.166.347
4. Boyd, D.W.: Perron units which are not Mahler measures. Ergod. Theory Dyn. Syst. **6**(4), 485–488 (1986). https://doi.org/10.1017/S0143385700003643
5. Christopoulos, C., McKee, J.: Galois theory of Salem polynomials. Math. Proc. Camb. Philos. Soc. **148**(1), 47–54 (2010). https://doi.org/10.1017/S0305004109990284
6. Dill, G.: Unlikely Intersections with Isogeny Orbits. PhD-theses, Universität Basel (2020)
7. Dixon, J.D., Dubickas, A.: The values of Mahler measures. Mathematika **51**(1–2), 131–148 (2004). https://doi.org/10.1112/S0025579300015564
8. Dobrowolski, E.: On a question of Lehmer and the number of irreducible factors of a polynomial. Acta Arith. **34**(4), 391–401 (1979)
9. Dubickas, A.: Mahler measures close to an integer. Can. Math. Bull. **45**(2), 196–203 (2002). https://doi.org/10.4153/CMB-2002-022-8
10. Dubickas, A.: On numbers which are Mahler measures. Monatsh. Math. **141**(2), 119–126 (2004). https://doi.org/10.1007/s00605-003-0010-0
11. Dubickas, A.: Salem numbers as Mahler measures of nonreciprocal units. Acta Arith. **176**(1), 81–88 (2016)
12. Lehmer, D.H.: Factorization of certain cyclotomic functions. Ann. Math. (2) **34**(3), 461–479 (1933). https://doi.org/10.2307/1968172
13. Lind, D.A.: Entropies and factorizations of topological Markov shifts. Bull. Am. Math. Soc. (N.S.) **9**(2), 219–222 (1983). https://doi.org/10.1090/S0273-0979-1983-15162-5
14. Lind, D.A.: The entropies of topological Markov shifts and a related class of algebraic integers. Ergod. Theory Dyn. Syst. **4**(2), 283–300 (1984). https://doi.org/10.1017/S0143385700002443
15. Mossinghoff, M.J.: Lehmer's problem. http://www.cecm.sfu.ca/~mjm/Lehmer/
16. Mossinghoff, M.J.: Polynomials with small Mahler measure. Math. Comput. **67**(224), 1697–1705 (1998). https://doi.org/10.1090/S0025-5718-98-01006-0
17. Mossinghoff, M.J., Rhin, G., Wu, Q.: Minimal Mahler measures. Exp. Math. **17**(4), 451–458 (2008)

18. Schinzel, A.: On values of the Mahler measure in a quadratic field (solution of a problem of Dixon and Dubickas). Acta Arith. **113**(4), 401–408 (2004). https://doi.org/10.4064/aa113-4-7. **(Dedicated to Robert Tijdeman on the occasion of his 60th birthday)**
19. Smyth, C.J.: On the product of the conjugates outside the unit circle of an algebraic integer. Bull. Lond. Math. Soc. **3**, 169–175 (1971)
20. Smyth, C.J.: Additive and multiplicative relations connecting conjugate algebraic numbers. J. Number Theory **23**(2), 243–254 (1986). https://doi.org/10.1016/0022-314X(86)90094-6
21. Zhang, M.: Mahler measure and how it acts as a dynamical system. Master's thesis, Oklahoma State University (2015)