ARITHMETICAL PROPERTIES OF POWERS OF ALGEBRAIC NUMBERS

ARTŪRAS DUBICKAS

Abstract

We consider the sequences of fractional parts \( \{\xi\alpha^n\} \), \( n = 1, 2, 3, \ldots \), and of integer parts \( [\xi\alpha^n] \), \( n = 1, 2, 3, \ldots \), where \( \xi \) is an arbitrary positive number and \( \alpha > 1 \) is an algebraic number. We obtain an inequality for the difference between the largest and the smallest limit points of the first sequence. Such an inequality was earlier known for rational \( \alpha \) only. It is also shown that for roots of some irreducible trinomials the sequence of integer parts contains infinitely many numbers divisible by either 2 or 3. This is proved, for instance, for \( [\xi((\sqrt{13} - 1)/2)] \), \( n = 1, 2, 3, \ldots \). The fact that there are infinitely many composite numbers in the sequence of integer parts of powers was proved earlier for Pisot numbers, Salem numbers and the three rational numbers 3/2, 4/3, 5/4, but no such algebraic number having several conjugates outside the unit circle was known.

1. Introduction

Let \( \xi > 0 \) be a real number, and let \( \alpha > 1 \) be an algebraic number. In this paper, we are interested in the sequence of fractional parts \( \{\xi\alpha^n\} \), \( n = 1, 2, 3, \ldots \), and in the sequence of integer parts \( [\xi\alpha^n] \), \( n = 1, 2, 3, \ldots \). Denote

\[
\Delta(\xi, \alpha) = \limsup_{n \to \infty} \{\xi\alpha^n\} - \liminf_{n \to \infty} \{\xi\alpha^n\}.
\]

There are several interesting old problems concerning the distribution of fractional parts \( \{\xi\alpha^n\} \), \( n \in \mathbb{N} \), where \( \xi > 0 \) and \( \alpha > 1 \) are real numbers. Apparently, Vijayaraghavan [22] was the first to obtain some definitive results about the set of limit points of such fractional parts, although earlier Koksma [17] proved that for almost all \( \alpha > 1 \) the sequence \( \{\xi\alpha^n\}, n = 1, 2, \ldots \), is uniformly distributed in \([0, 1]\). In contrast, for ‘almost all’ specific numbers \( \alpha > 1 \) the problem is open. It is not known, for instance, whether the set \( \{e^n\}, n \in \mathbb{N} \), has one or more than one limit point. Also, it is not known whether there are any Mahler’s Z-numbers. A positive number \( \xi \) is called Mahler’s Z-number if \( 0 \leq \{\xi(3/2)^n\} < 1/2 \) for every non-negative integer \( n \).

In connection with Mahler’s problem [18], Flatto, Lagarias and Pollington [14] showed that if \( \alpha = p/q \), where \( p > q > 1 \) are coprime positive integers, then \( \Delta(\xi, p/q) \geq 1/p \) for any \( \xi > 0 \). The inequality \( \Delta(\xi, 3/2) > 1/2 \) would imply that Mahler’s Z-numbers do not exist. Further results in this direction were recently obtained by Bugeaud [5] (based on the transformations considered by Flatto in [13]) and by the present author [11], but closing off the gap between 1/3 and 1/2 seems to be out of reach. In this paper, we will prove a lower bound for the quantity \( \Delta(\xi, \alpha) \), where \( \alpha > 1 \) is an arbitrary algebraic number.

Another direction concerns the problem initiated by Forman and Shapiro [15] (see also [16, Problem E19]). The result of Koksma quoted above implies that for
almost all \( \alpha > 1 \) the set \([\alpha^n], n \in \mathbb{N}\), contains infinitely many composite numbers. (Setting, for instance, \( \xi = 1/2 \) we have \([\alpha^n] = 2[\alpha^n/2]\) whenever \(\{\alpha^n/2\} < 1/2\) which, for almost all \( \alpha \), happens for infinitely many \(n\).) However, once again for ‘almost all’ specific numbers such results are inaccessible. The fact that there are infinitely many composite numbers of the form \([\alpha^n]\), where \(n \in \mathbb{N}\), was proved for \(\alpha = 3/2\) and \(\alpha = 4/3\) (Forman and Shapiro [15]), for \(\alpha = 5/4\) (see [12]), for \(\alpha\) being a quadratic unit (see Cass [6]) and, more generally, for all Pisot and Salem numbers (see [9, 10]). A similar result for some explicit (but specially constructed) transcendental numbers was proved in [1]. In Section 3 we will state a result claiming that there are infinitely many composite numbers among the natural powers of roots of certain trinomials which have several conjugates greater than 1 in absolute value. Such results were inaccessible using earlier methods. See also [19, 23] for some nice elementary results about prime numbers of the form \([\alpha^n], n \in \mathbb{N}\), and a paper of Baker and Harman [3] for other metrical results in this direction.

This paper is organized as follows. In the next section we will give our main result concerning the distribution of the fractional parts of powers of an algebraic number. Section 3 is devoted exclusively to integer parts. A result about non-periodicity (which is used in several proofs) and other auxiliary results will be stated and proved in Section 4. In Section 5 we will prove our main Theorems 1 and 2. The proof of Proposition 1 and other information concerning the so-called reduced length of a polynomial will be given in Section 6.

2. Fractional parts of powers of an algebraic number

Given an algebraic number \( \alpha \) over the field of rational numbers \( \mathbb{Q} \) whose minimal polynomial in \( \mathbb{Z}[x] \) is

\[
P(x) = a_d x^d + \ldots + a_1 x + a_0 = a_d (x - \alpha_1) (x - \alpha_2) \ldots (x - \alpha_d), \quad a_d > 0,
\]

where \( \alpha_1 = \alpha, \alpha_2, \ldots, \alpha_d \) is the set of conjugates of \( \alpha \), its length is defined as \( L(\alpha) = L(P) = \sum_{j=0}^{d} |a_j| \). Similarly, the length of an arbitrary polynomial \( F \in \mathbb{C}[x] \) is defined as the sum of the moduli of its coefficients. We will consider the set of polynomials

\[
\Gamma = \{b_0 + b_1 x + \ldots + b_m x^m \in \mathbb{R}[x], \text{ where } b_0 = 1 \text{ or } b_m = 1\},
\]

where \( m \) runs over every non-negative integer. For an algebraic number \( \alpha \) with minimal polynomial \( P \) we introduce the quantity

\[
\ell(\alpha) = \ell(P) = \inf_{G \in \Gamma} L(PG).
\]

Evidently, \( \ell(\alpha) \leq L(\alpha) \). We call \( \ell(\alpha) \) the reduced length of \( \alpha \) (or \( P \)). See Proposition 1 and Section 6 for other information about the reduced length of a polynomial.

Our first main result gives a lower bound for \( \Delta(\xi, \alpha) \). Recall that an algebraic integer \( \alpha > 1 \) is called a Pisot number if the moduli of all its other conjugates (if any) are strictly smaller than 1. A Salem number is an algebraic integer \( \alpha > 1 \) having all its other conjugates in the unit disc with at least two conjugates lying on the unit circle.

**Theorem 1.** Suppose that \( \alpha > 1 \) is an arbitrary algebraic number, and suppose that \( \xi \) is an arbitrary positive number that lies outside the field \( \mathbb{Q}(\alpha) \) if \( \alpha \) is a Pisot number or a Salem number. Then \( \Delta(\xi, \alpha) \geq 1/\ell(\alpha) \).
Of course, the inequality $\ell(\alpha) \leq L(\alpha)$ implies immediately that $\Delta(\xi, \alpha) \geq 1/L(\alpha)$. However, sometimes the reduced length of $\alpha$ can be much smaller than $L(\alpha)$. This raises a problem of finding either its exact value or at least a more precise upper bound for it.

The polynomials lying in $\Gamma$ have either their constant coefficient or their leading coefficient equal to $1$. Let $\Gamma_0$ be the subset of $\Gamma$ consisting of polynomials with $b_0 = 1$. Set $\ell_0(\alpha) = \ell_0(P) = \inf_{G \in \Gamma_0} L(PG)$. It is easy to see that $\ell(P) = \min\{\ell_0(P), \ell_0(P^*)\}$, where $P^*(x) = x^d P(1/x)$ is reciprocal to $P$. Hence $\ell(\alpha) = \min\{\ell_0(\alpha), \ell_0(\alpha^{-1})\}$. Recall that the Mahler measure of a polynomial is the product of the modulus of its leading coefficient and of the moduli of its roots lying outside the unit circle. The Mahler measure is multiplicative: $M(PG) = M(P)M(G)$. Also, $M(G) = M(G^*)$. Hence $M(G) \geq 1$ for any $G \in \Gamma$. By Landau’s inequality (see, for example [20, pp. 225, 261]), we deduce that $L(PG) \geq M(PG) = M(P)M(G) \geq M(P)$. Summarizing, for $\alpha \neq 0$ we have

$$M(\alpha) \leq \ell(\alpha) \leq \ell_0(\alpha^{\pm 1}) \leq L(\alpha).$$

We will compute $\ell_0(\alpha)$ in the case when $\alpha$ has at most one conjugate in the unit disc.

**Proposition 1.** If $\alpha \in \mathbb{Q}$ has no conjugates in the unit disc then $\ell_0(\alpha) = |a_0|$. If $\alpha' \neq 0$ is the unique conjugate of $\alpha$ in the unit disc then $\ell_0(\alpha) = |a_0|(1 + 1/|\alpha'|)$.

Proposition 1 combined with the inequality $\ell(\alpha) = \min\{\ell_0(\alpha), \ell_0(\alpha^{-1})\} \geq M(\alpha) \geq \max\{a_d, |a_0|\}$ implies the following corollary.

**Corollary 1.** If the moduli of $\alpha$ and its conjugates are all strictly greater (smaller) than $1$ then $\ell(\alpha) = \max\{a_d, |a_0|\}$. If $\alpha$ and $\alpha'$ are conjugate quadratic numbers such that $|\alpha| > 1$ and $|\alpha'| < 1$ then $\ell(\alpha) = a_2|\alpha| + \min\{a_2, |a_0|\}$.

Of course, Corollary 1 gives exact values for the reduced length $\ell(\alpha)$ in the case when $\alpha > 1$ is a rational or a quadratic number. For rational numbers, Theorem 1 recovers the result of Flatto, Lagarias and Pollington that $\Delta(\xi, p/q) \geq 1/p$, since $p/q > 1$ is the root of the polynomial $p - qx$, so, by Corollary 1, $\ell(p/q) = \max\{p, q\} = p$. Similarly, for $\alpha > 1$ solving $x^3 - x - 2 = 0$ we find that $\ell(\alpha) = 2$, since the moduli of $\alpha$ and its conjugates are greater than $1$, so $\Delta(\xi, \alpha) \geq 1/2$ for any $\xi > 0$.

If $\alpha$ is a Pisot number, then Proposition 1 implies that $\ell_0(\alpha^{-1}) = 1 + \alpha$, giving $\ell(\alpha) \leq 1 + \alpha$. We thus obtain the following corollary.

**Corollary 2.** If $\alpha$ is a Pisot number and $\xi \notin \mathbb{Q}(\alpha)$ then $\Delta(\xi, \alpha) \geq 1/(1 + \alpha)$.

For $\alpha = (1 + \sqrt{5})/2$, Corollary 2 implies that $\Delta(\xi, (1 + \sqrt{5})/2) \geq (3 - \sqrt{5})/2$ if $\xi \notin \mathbb{Q}(\sqrt{5})$. (In fact, by Corollary 1, $\ell(\alpha) = (3 + \sqrt{5})/2$.) Note that, for $\xi \in \mathbb{N}$, both 0 and 1 (and only these two!) are the limit points of $\{(1 + \sqrt{5}/2)^n\}$, $n = 1, 2, \ldots$, so $\Delta(1, (1 + \sqrt{5})/2) = 1$. However, say $\alpha = 3 + 2\sqrt{2}$ is a strong Pisot number in the sense of [8], so $\lim_{n \to \infty} \{(3 + 2\sqrt{2})^n\} = 1$, giving $\Delta(1, 3 + 2\sqrt{2}) = 0$. In contrast, for $\xi \notin \mathbb{Q}(\sqrt{2})$, by Corollary 2, we have $\Delta(\xi, 3 + 2\sqrt{2}) \geq (2 - \sqrt{2})/4$. 
3. Integer parts of powers of an algebraic number

THEOREM 2. Let \( d > r \geq 1 \) be two positive integers. Suppose that \( \alpha > 1 \) is a root of one of the following six polynomials: \( x^d - x^r - 1 \), \( x^d - 2x^r + 1 \), \( x^d - x^r - 3 \), \( x^d - 3x^r - 1 \), \( x^d + x^r - 3 \), or \( x^d - 3x^r + 1 \). Let \( \xi \) be an arbitrary positive number that lies outside the field \( \mathbb{Q}(\alpha) \) if \( \alpha \) is a Pisot number. Then the set \([\xi\alpha^n], n \in \mathbb{N}\), contains infinitely many numbers divisible by 2 (in the first two cases) and either by 2 or by 3 (in cases three to six).

For instance, \( \alpha = (\sqrt[3]{13} - 1)/2 \) is the unique positive root of \( x^2 + x - 3 \), with \(- (\sqrt[3]{13} + 1)/2 \) being its other root. Hence, by Theorem 2, for any \( \xi > 0 \), the set \([\xi((\sqrt[3]{13} - 1)/2)^n], n \in \mathbb{N}\), contains infinitely many numbers divisible by either 2 or 3.

Note that some polynomials in Theorem 2 are reducible, so the degree of \( \alpha \) in this theorem (only!) may be smaller than \( d \). For example, the polynomial \( x^{d-1} - x^{d-2} - \ldots - x - 1 \) is irreducible and defines a Pisot number \( \alpha \). Although the length of this polynomial is large, \( d \), this polynomial divides the polynomial \( x^d - 2x^{d-1} + 1 \).

Theorem 2 implies that if \( \xi \notin \mathbb{Q}(\alpha) \) then the set \([\xi\alpha^n], n \in \mathbb{N}\), contains infinitely many even numbers.

Selmer [21] proved that the polynomials \( x^d - x - 1 \) are irreducible for each \( d \geq 2 \). In the proof of Theorem 2 we will derive the following corollary, which is slightly stronger than Theorem 2 for \( \alpha > 1 \) solving \( x^d - x - 1 = 0 \).

COROLLARY 3. Let \( d \geq 2 \) be a positive integer. Suppose that \( \alpha > 1 \) is a root of the polynomial \( x^d - x - 1 \). Let \( \xi \) be an arbitrary positive number that lies outside the field \( \mathbb{Q}(\alpha) \) if \( d \in \{2, 3\} \). Then the set \([\xi\alpha^n], n \in \mathbb{N}\), contains infinitely many even numbers and infinitely many odd numbers.

It is easy to see that \( \xi/2 \) is Mahler’s \( Z \)-number if and only if the numbers \([\xi(3/2)^n], n = 0, 1, 2, \ldots \) are all even. More generally, we may call \( \xi \) Mahler’s \( Z_{\alpha} \)-number if \( 0 \leq \{\xi\alpha^n\} < 1/2 \) for each \( n \geq 0 \). The corollary implies that there are no Mahler’s \( Z_{\alpha} \)-numbers if \( \alpha > 1 \) solves \( x^d - x - 1 = 0 \), where \( d \geq 4 \). Curiously, these numbers also appear in Boyd’s paper [4] as the first Perron numbers which were proved to be not Mahler measures. Moreover, they are well known as standard examples of polynomials with Galois group isomorphic to the full symmetric group \( S_d \).

4. Preliminary results

Throughout, we will write \( x_n = [\xi\alpha^n] \) and \( y_n = \{\xi\alpha^n\} \). Then \( \xi\alpha^n = x_n + y_n \).

Since \( \alpha \) is a root of its minimal polynomial \( P(x) = a_dx^d + \ldots + a_1x + a_0 \), we have \( a_d(x_{n+d} + y_{n+d}) + \ldots + a_0(x_n + y_n) = 0 \) for each \( n \geq 0 \). It follows that

\[
s_n = a_d x_{n+d} + a_{d-1} x_{n+d-1} + \ldots + a_0 x_n = -(a_d y_{n+d} + a_{d-1} y_{n+d-1} + \ldots + a_0 y_n)
\]

is an integer. Denoting by \( L^+(P) \) and \( -L^-(P) \) the sums of non-negative and negative coefficients of \( P \), respectively, we see that \( -L^+(P) < s_n < L^-(P) \). Hence \( s_n \in \{-L^+(P) + 1, -L^+(P) + 2, \ldots, L^-(P) - 1\} \).
We can also choose arbitrary real numbers \( b_0 \neq 0, b_1, \ldots, b_m \) and multiply the equalities
\[
a_dx_n + a_{d-1}x_n^{d-1} + \ldots + a_0x_n = -s_{n+j}
\]
by \( b_j \), where \( j = 0, 1, \ldots, m \), and then add all the equalities thus obtained:
\[
\sum_{j=0}^{m} b_j(a_dx_{n+j} + a_{d-1}x_{n+j}^{d-1} + \ldots + a_0x_n) = -b_0s_n - b_1s_{n+1} - \ldots - b_ms_{n+m}.
\]
Setting \( v_n := b_0s_n + b_1s_{n+1} + \ldots + b_ms_{n+m} \), we see that, for each \( n \in \mathbb{N} \),
\[
c_m + d + y_{n+m+d} + \ldots + c_1y_{n+1} + c_0y_n = -b_0s_n - b_1s_{n+1} - \ldots - b_ms_{n+m} = -v_n,
\]
where \( P(x)(b_0 + b_1x + \ldots + b_mx^m) = c_0 + c_1x + \ldots + c_{m+d}x^{m+d} = F(x) \). Similarly,
\[
v_n = c_m + d + x_{n+m+d} + \ldots + c_1x_{n+1} + c_0x_n = b_0s_n + b_1s_{n+1} + \ldots + b_ms_{n+m}.
\]
Since we regard \( b_0, b_1, \ldots, b_m \) as fixed, so are \( c_0, c_1, \ldots, c_{m+d} \) too; also, \( v_n, n = 1, 2, \ldots \), all belong to a finite set. In particular, if \( F(x) \in \mathbb{Z}[x] \), then \( v_n \in \{-L^+(F) + 1, -L^+(F) + 2, \ldots, L^-(F) - 1\} \), where \( L^+(F) \) and \( L^-(F) \) are the sums of non-negative and negative coefficients of \( F \), respectively. However, in the next theorem we do not assume that \( F \in \mathbb{Z}[x] \), but only that \( F(x) = P(x)(b_0 + b_1x + \ldots + b_mx^m) \in \mathbb{R}[x], F(0) \neq 0 \).

**Theorem 3.** Suppose that \( \alpha > 1 \) is an arbitrary algebraic number, and suppose that \( \xi \) is an arbitrary positive number that lies outside the field \( \mathbb{Q}(\alpha) \) if \( \alpha \) is a Pisot number or a Salem number. Then the sequences \( s_1, s_2, s_3, \ldots \) and \( v_1, v_2, v_3, \ldots \) are not ultimately periodic.

Recall that the sequence \( s_1, s_2, s_3, \ldots \) is called **ultimately periodic** if there are positive integers \( n_0 \) and \( t \) such that \( s_{m+t} = s_m \) for all \( m \geq n_0 \).

We begin with the following three lemmas, the first one being rewritten from [7].

**Lemma 1.** If \( P(x) = a_dx^d + a_{d-1}x^{d-1} + \ldots + a_0 = a_d(x - \alpha_1) \ldots (x - \alpha_d) \in \mathbb{C}[x] \) has distinct roots and
\[
X_1\alpha_1^j + \ldots + X_d\alpha_d^j = Z_j, \quad j = 0, 1, \ldots, d - 1,
\]
then \( X_j = (1/P'(\alpha_j)) \sum_{k=0}^{d-1} \beta_{j,k} Z_k \) for \( j = 1, 2, \ldots, d \) with \( \beta_{j,k} = \sum_{l=k+1}^{d} a_l \alpha_j^{l-k-1} \).

**Proof.** The linear system has a unique solution, since its Vandermonde determinant is nonzero. Setting \( P_j(x) = (P(x) - P(\alpha_j))/(x - \alpha_j) = \sum_{k=0}^{d-1} \beta_{j,k} x^k \), we have \( P'_j(\alpha_j) = P'(\alpha_j) \) and \( P'_j(\alpha_k) = 0 \) for \( k \neq j \). Hence \( \sum_{k=0}^{d-1} \beta_{j,k} Z_k = X_1P_j(\alpha_1) + \ldots + X_d P_j(\alpha_d) = X_j P'(\alpha_j) \), giving the right value for \( X_j \).

**Lemma 2.** Assume that an infinite sequence of letters of a finite alphabet \( B = \{B_1, \ldots, B_n\} \) is not ultimately periodic. Then, for every \( N \in \mathbb{N} \), there is a pattern \( X \) of length at least \( N \) and two different letters \( B_i \) and \( B_j \) such that the sequence contains infinitely many patterns of the form \( B_i X \) and \( B_j X \). Similarly, there is a pattern \( Y \) of length at least \( N \) and two different letters \( B_u \) and \( B_v \) such that the sequence contains infinitely many patterns of the form \( Y B_u \) and \( Y B_v \).
Proof. The proof of the first part of the lemma is given in [11]. The proof of the second part is similar and symmetric. We distribute the sequence into equal blocks of length \( N \). Assume that in this sequence of blocks only the blocks \( Y_1, \ldots, Y_s \) occur infinitely often. Clearly, \( s \geq 2 \). If this sequence contains infinitely many patterns of the form \( Y_1Y_i \) and \( Y_1Y_j, \ i \neq j \), then the proof is finished immediately. Assume that we have infinitely many patterns of the form \( Y_1Y_i \) only. Here \( i \neq 1 \), since otherwise the sequence from a certain place must be \( Y_1^\infty \), a contradiction. Now, without loss of generality we may assume that \( i = 2 \) and argue with the pattern \( Y_1Y_2^2 \) (instead of \( Y_1 \)) as above. More precisely, consider the patterns of the form \( Y_2Y_i \) which occur infinitely often. As above, \( i \neq 1, 2 \), so we can set \( i = 3 \) without loss of generality. In this way, since all patterns \( Y_1, \ldots, Y_s \) occur infinitely often, we will see that, starting with a certain place, we can have only \( Y_2 \) to the right of \( Y_1 \), only \( Y_3 \) to the right of \( Y_2 \), and so on, with only \( Y_s \) to the right of \( Y_{s-1} \). In other words, from a certain place only \( Y_{j-1} \) can occur to the left of \( Y_j \) for every \( j > 1 \). Clearly, we can only have \( Y_j \) infinitely often, since all the other patterns are already occupied. Namely, if \( Y_jY_i \), where \( j < s \), occurs infinitely often, then this contradicts the fact that only \( Y_jY_{j+1} \) occurs infinitely often. Then, starting with a certain place, the sequence is \((Y_1 \ldots Y_s)^\infty \), so the initial sequence is ultimately periodic, a contradiction. \( \square \)

Remark 1. The referee noted that using some results from combinatorics on words (for example [2, Theorem 10.2.6]) one can derive the conclusion of Lemma 2 with ‘of length at least \( N \)’ replaced by ‘of length \( N \)’.

Lemma 3. Let \( B \) be a finite set of complex numbers, and let \( b_0 \neq 0, b_1, \ldots, b_m \) be complex numbers. Set \( v_n = b_0s_n + \ldots + b_ms_{n+m} \) for each \( n \in \mathbb{N} \), where \( s_1, s_2, s_3, \ldots \in B \). If the sequence \( s_1, s_2, s_3, \ldots \) is not ultimately periodic then neither is the sequence \( v_1, v_2, v_3, \ldots \).

Proof. If \( v_n, n = 1, 2, \ldots, \) were ultimately periodic with period \( t \), then \( r_n := s_{n+t} - s_n \) would satisfy the linear recurrence \( b_0r_n + \ldots + b_mr_{n+m} = 0 \), where \( n \geq n_1 \). Now, if \( r_1, r_2, \ldots \) were ultimately periodic with period \( T \), then \( w_n := r_n + r_{n+t} + \ldots + r_{n+(T-1)} = s_{n+tT} - s_n \) would have to be an ultimately periodic sequence too. Furthermore, \( w_n = w_{n+tT} = w_{n+2tT} = \ldots \). Hence

\[ kw_n = w_n + w_{n+tT} + \ldots + w_{n+(k-1)tT} = s_{n+ktT} - s_n \]

Since all \( s_n \) belong to a finite set and \( k \) can be taken arbitrarily large, this implies that \( w_n = 0 \) for each sufficiently large \( n \), and hence \( s_1, s_2, \ldots \) must be ultimately periodic, a contradiction. Hence, as \( r_1, r_2, \ldots \) is not ultimately periodic, we can apply to it Lemma 2. More precisely, this sequence must contain infinitely many patterns of the form \( rX \) and of the form \( r'X \), where \( r \neq r' \) and \( X \) is a pattern of length at least \( m \). Taking two such patterns starting at places \( \geq n_1 \) and subtracting one linear recurrence from another, we will get \( b_0(r'-r) = 0 \), a contradiction. \( \square \)

Proof of Theorem 3. Assume that the sequence \( s_1, s_2, s_3, \ldots \) is ultimately periodic with period \( t \in \mathbb{N} \). Then, for \( n \) sufficiently large, \( s_n = s_{n+t} \), so the difference \( u_n := x_{n+t} - x_n \) satisfies the linear recurrence \( a_0u_n + a_1u_{n+1} + \ldots + a_du_{n+d} = 0 \). Hence, there are complex numbers \( \xi_1, \ldots, \xi_d \) such that \( u_n = \xi_1\alpha_1^n + \ldots + \xi_d\alpha_d^n \) for each \( n \geq n_0 \). Now, for every sufficiently large \( m \), we apply Lemma 1 to the linear
system \( X_1 \alpha_1^{n-m} + \ldots + X_d \alpha_d^{n-m} = u_n, n = m, m+1, \ldots, m+d-1, \) with variables \( X_j = \xi_j \alpha_j^m, j = 1, 2, \ldots, d. \) We obtain \( P'(\alpha_j) \xi_j \alpha_j^m = G_m(\alpha_j) \) for each \( j = 1, \ldots, d, \) where \( G_m \) are integer polynomials of degree at most \( d-1. \) Hence \( \xi_j \in \mathbb{Q}(\alpha_j) \) are algebraic numbers and, moreover, \( \xi_1, \ldots, \xi_d \) are conjugate over \( \mathbb{Q}. \) Evidently, \( \xi_1 \neq 0, \) as otherwise \( u_n = 0 \) for all large \( n, \) which is impossible. Let \( q \) be a fixed integer for which \( q/(P'(\alpha) \xi_1), q/(P'(\alpha) \xi_1), \ldots, q/(P'(\alpha) \xi_1) \) are algebraic integers. Then \( q \alpha_m = q G_m(\alpha)/(P'(\alpha) \xi_1) \) is an algebraic integer for every sufficiently large \( m. \) However, from the factorization of \( q \alpha_m \) into prime ideals we see that this is impossible (since \( q \) is fixed and \( m \) is as large as we wish), unless \( \alpha \) is an algebraic integer. Hence it is.

Now, observe that \( \delta_n = (\xi(\alpha'-1) - \xi_1) \alpha_n - \xi_1 \alpha_n^2 - \xi_2 \alpha_n^3 - \ldots - \xi_d \alpha_n^d, \) where \( \delta_n : = y_n + x_n \). Clearly, \( |\delta_n| < 1. \) Once again, on applying Lemma 1 to the linear system \( X_1 \alpha_1^{n-m} + \ldots + X_d \alpha_d^{n-m} = \delta_n, n = m, m+1, \ldots, m+d-1, \) with variables \( X_1 = (\xi(\alpha'-1) - \xi_1) \alpha_n^m, X_2 = -\xi_2 \alpha_n^m, \ldots, X_d = -\xi_d \alpha_n^m, \) we deduce that the moduli of \( (\xi(\alpha'-1) - \xi_1) \alpha_n^m, -\xi_2 \alpha_n^m, \ldots, -\xi_d \alpha_n^m \) are all smaller than a positive constant \( c \) depending on \( \alpha \) only. By taking sufficiently large \( m, \) we see that this is only possible if \( \xi = \xi_1/(\alpha'-1) \) (because \( \alpha_1 = \alpha > 1 \)) and if all \( \alpha_j \) with \( j \geq 2 \) lie in the unit disc. Since \( \alpha \) is an algebraic integer it must be a Pisot or a Salem number. Furthermore, \( \xi \in \mathbb{Q}(\alpha), \) because \( \xi_1 \in \mathbb{Q}(\alpha), \) a contradiction with the condition of Theorem 3. The proof of the theorem for the sequence \( s_1, s_2, s_3, \ldots \) is complete. Combining this with Lemma 3 we see that the sequence \( v_1, v_2, v_3, \ldots \) is also not ultimately periodic. \( \square \)

5. Proofs of the main results

Proof of Theorem 1. Since \( \ell(\alpha) = \min\{\ell_0(\alpha), \ell_0(\alpha^{-1})\}, \) either \( \ell(\alpha) = \ell_0(\alpha) \) or \( \ell(\alpha) = \ell_0(\alpha^{-1}) \). Suppose first that \( \ell(\alpha) = \ell_0(\alpha) \). Then, for every \( \epsilon > 0, \) there is a polynomial \( G \in \Gamma_0 \) such that \( L(PG) \leq \ell_0(\alpha) + \epsilon. \) Suppose that \( G(x) = 1 + b_1 x + \ldots + b_m x^m, \) and set \( F = PG. \) By Theorem 3, the sequence \( s_1, s_2, s_3, \ldots \) is not ultimately periodic. By Lemma 2, since each \( s_j \) belongs to a finite set, there are two distinct values, say \( s < s', \) and a pattern \( X \) of length at least \( m \) such that the patterns \( sX \) and \( s'X \) occur in the sequence infinitely often. (Note that by either adding terms of the form \( 0 \cdot x^j \) to \( G(x) \) or by using the ‘improved’ Lemma 2 we may assume that it is the same \( m \) as is the degree of \( G(x). \) Recall that

\[-v_n = c_{m+d} y_{n+m+d} + \ldots + c_1 y_{n+1} + c_0 y_n = -s_n - b_1 s_{n+1} - \ldots - b_m s_{n+m}, \]

where \( F(x) = P(x) G(x) = c_0 + c_1 x + \ldots + c_{m+d} x^{m+d}. \)

Let \( \lambda > 0 \) be a fixed positive number. Setting \( \mu = \lim sup_{n \to \infty} y_n \) and \( \lambda = \lim inf_{n \to \infty} y_n, \) we have \( \lambda - \epsilon \leq y_n \leq \mu + \epsilon \) for each \( n \) sufficiently large, say \( n \geq M. \)

Suppose that \( X = z_1 z_2 \ldots z_m. \) Then, choosing any \( n \geq M \) such that the pattern \( sX \) starts at the \( n \)th place, we see that \( (\mu + \epsilon) L^+ - (\lambda - \epsilon) L^- \geq -s - b_1 z_1 - \ldots - b_m z_m. \)

Here, \( L^+ = L^+(F), L^- = L^-(F). \) Similarly, taking any \( n \geq M \) such that the pattern \( s'X \) starts with the \( n \)th place we obtain \( (\mu + \epsilon) L^- - (\lambda - \epsilon) L^+ \geq s' - b_1 z_1 + \ldots + b_m z_m. \)

Adding both inequalities, we deduce that \( (L^+ + L^-)(\mu - \lambda + 2\epsilon) \geq s' - s. \) Since \( s' - s \geq 1 \) and \( L^+ + L^- = L(PG), \) it follows that

\[ \Delta(\xi, \alpha) = \mu - \lambda \geq -2\epsilon + 1/L(PG) \geq -2\epsilon + 1/(\ell_0(\alpha) + \epsilon). \]

As \( \epsilon \) and \( \epsilon \) can be chosen arbitrarily small, this implies that \( \Delta(\xi, \alpha) \geq 1/\ell_0(\alpha). \)
Assume now that \( \ell(\alpha) = \ell_0(\alpha^{-1}) = \ell_0(P^*) \). Then, for every \( \epsilon > 0 \), there is a polynomial \( G \) such that \( G^* \in \Gamma_0 \) and \( L(P^*G^*) = L(PG) \leq \ell_0(\alpha^{-1}) + \epsilon \). Now, \( G(x) = b_0 + b_1x + \ldots + b_{m-1}x^{m-1} + x^m \). Set \( F = PG \). Similarly, by Lemma 2, there are two distinct integers, say \( s < s' \) again, and a pattern \( Y \) of length at least \( m \) such that the patterns \( Ys \) and \( Ys' \) occur in the sequence infinitely often. (As above, we may assume that the length of the pattern \( Y \) is equal to \( m = \deg G \) and, by an abuse of notation, write \( Y = \frac{z_1}{z_2} \ldots \frac{z_m}{z_m} \).) This time \[-v_n = c_{n+d}y_{n+d} + \ldots + c_1y_1 + c_0y_0 = -b_0s_n - \ldots - b_{m-1}s_{n+m-1} - s_{n+m},\] where \( F(x) = P(x)G(x) = c_0 + c_1x + \ldots + c_{m+d}x^{m+d} \). Hence, as above, choosing \( n \geq M \) such that \( y_n, \ldots, y_{n+m+d} \leq \mu + \varepsilon \) we get \((\mu + \varepsilon)L^+ - (\lambda - \varepsilon)L^{-} \geq -b_0z_1 - b_1z_2 - \ldots - s\). Doing the same with \( Ys' \) we get \((\mu + \varepsilon)L^+ - (\lambda - \varepsilon)L^{-} \geq b_0z_1 + b_1z_2 + \ldots + s'\). Adding both inequalities we obtain \((L^+ + L^-)(\mu - \lambda + 2\varepsilon) \geq s' - s\). Therefore \( \Delta(\xi,\alpha) = \mu - \lambda \geq -2\varepsilon + 1/L(PG) = -2\varepsilon + 1/L(P^*G^*) \geq -2\varepsilon + 1/(\ell_0(\alpha^{-1}) + \epsilon) \), where \( G^* \in \Gamma_0 \). Now \( \varepsilon \) and \( \epsilon \) can be chosen arbitrarily small, so that \( \Delta(\xi,\alpha) \geq 1/\ell_0(\alpha^{-1}) \). This completes the proof of Theorem 1.

**Proof of Theorem 2.** All polynomials \( F \) considered in Theorem 2 have integer coefficients. Hence \( v_n \in \mathbb{Z} \) for every \( n \in \mathbb{N} \) and \(-L^+(F) < v_n < L^-(F)\). Of course, if \( F \) is irreducible then \( v_n = s_n \). Note also that none of the numbers considered in Theorem 2 is a Salem number, so Theorem 3 is applicable in all cases below. If \( \alpha > 1 \) is a root of \( x^d - x^r - 1 \) then \( v_n = x_{n+d} - x_{n+r} - x_n \) can only take the values \( 0 \) or \( 1 \). By Theorem 3, both values \( 0 \) and \( 1 \) occur infinitely often, because the sequence \( v_1, v_2, v_3, \ldots \) is not ultimately periodic. If \( v_n = 0 \) then the triple \( x_n, x_{n+r}, x_{n+d} \) contains an even number, while if \( v_n = 1 \) then this triple contains an odd number. It follows that there are infinitely many even and infinitely many odd numbers among \( x_n \). This proves Corollary 3, because \( x^d - x - 1 \) defines a Pisot number precisely when \( d \in \{2,3\} \).

Suppose that \( \alpha > 1 \) is a root of \( x^d - 2x^r + 1 \). The sequence \( v_n = x_{n+d} - 2x_{n+r} + x_n \) can take the values \(-1, 0, 1 \). Since \( v_n \) is not ultimately periodic, either \( v_n = -1 \) occurs infinitely often or \( v_n = 1 \) occurs infinitely often. In both cases we see that the sequence \( x_n, n = 1, 2, \ldots \), contains infinitely many even numbers.

Next, suppose that \( \alpha > 1 \) is a root of the polynomial \( x^d - x^r - 3 \). Then \( v_n = x_{n+d} - x_{n+r} - 3x_n \in \{0,1,2,3\} \). As above, we can exclude the cases \( v_n = 0 \) and \( v_n = 2 \), because then the triple \( x_{n+d}, x_{n+r}, x_n \) would contain an even number. Assume therefore that \( v_n \in \{1,3\} \). We need to show that there are infinitely many \( x_n \) divisible by \( 3 \). Assume that this is not the case. Then \( x_{n+d} \) is either \( x_{n+r} \) or \( x_{n+r} + 1 \) modulo 3 depending on whether \( v_n = 3 \) or \( v_n = 1 \). If \( v_n = 1 \), a corresponding \( x_{n+r} \) must be equal to 1 modulo 3 and \( x_{n+d} = 2 \) modulo 3. Then \( x_{n+d+k(d-r)} \) is equal to 2 modulo 3 for each \( k \geq 0 \). Analogously, if \( v_n = 3 \) then \( x_{n+d+k(d-r)} \), \( k \geq 0 \), are all equal modulo 3. Consequently, the sequence \( x_1, x_2, x_3, \ldots \) modulo 3 is ultimately periodic. By Lemma 3, it follows that \( v_1, v_2, v_3, \ldots \) modulo 3 is ultimately periodic. Plainly, this implies that \( v_1, v_2, v_3, \ldots \) itself is ultimately periodic, contrary to Theorem 3. The argument for \( \alpha > 1 \) solving \( x^d - 3x^r - 1 = 0 \) is similar to that above.

Finally, suppose that \( \alpha > 1 \) is a root of the polynomial \( x^d + x^r - 3 \). Then \( v_n = x_{n+d} + x_{n+r} - 3x_n \in \{-1, 0, 1, 2\} \). As above, we can exclude the values 0 and
2 by a parity argument. Hence \( v_n \) is either \(-1\) or \(1\). Assume that there are only finitely many \( x_n \) divisible by \(3\). Then, for all sufficiently large \(n\), \(x_{n+d}\) and \(x_{n+r}\) must be equal modulo \(3\), namely, \(x_m\) and \(x_n\) are either both equal to \(1\) modulo \(3\) or both equal to \(2\) modulo \(3\) provided that \(m-n=d-r\). Thus for each fixed \(n \in \{0,1,\ldots,d-r-1\}\), the sequence \(x_{n+k(d-r)}\), \(k=0,1,2,\ldots\), modulo \(3\) starting with a certain place is either \(1,1,\ldots\) or \(2,2,2,\ldots\) Consequently, the sequence \(v_{n+k(d-r)-r}, k=k_0, k_1, \ldots\), must be either \(-1,-1,-1,\ldots\) or \(1,1,1,\ldots\). This implies that the sequence \(v_1, v_2, v_3, \ldots\) is ultimately periodic, contrary to Theorem 3. By the same argument we can prove the theorem for \(\alpha > 1\) solving \(x^d-3x^r+1=0\); this completes the proof of Theorem 2.

\[
6. \text{ Reduced length of an algebraic number}
\]

The quantities \(\ell(P)\) and \(\ell_0(P)\) can be defined for an arbitrary polynomial \(P\) with real coefficients. They can also be defined for polynomials with complex coefficients but then it is more natural to assume that \(G \in \Gamma\) has complex coefficients. First of all, we prove the following proposition.

**Proposition 2.** Suppose that \(\omega, \eta, \psi \in \mathbb{R}, \nu \in \mathbb{C}, |\omega| \leq 1, |\eta| > 1, |\nu| > 1, \psi \neq 0\). Then, for every \(Q \in \mathbb{R}[x],\)

(i) \(\ell_0(\psi Q) = |\psi|\ell_0(Q)\);
(ii) \(\ell_0(\omega + x) = 1 + |\omega|\);
(iii) if \(T(x) = Q(x)(1 - x/\eta),\) then \(\ell_0(T) = \ell_0(Q)\);
(iv) if \(T(x) = Q(x)(1 - x/\nu)(1 - x/\tau),\) then \(\ell_0(T) = \ell_0(Q)\).

**Proof.** The proof of part (i) is immediate. For (ii), note that the length of the polynomial \((\omega + x)(1 + b_1 x + \ldots + b_m x^m)\) is equal to

\[|\omega| + |b_1 \omega + 1| + |b_2 \omega + b_1| + \ldots + |b_m \omega + b_{m-1}| + |b_m|.
\]

From the identity

\[1 + b_1 \omega - \omega(b_1 + b_2 \omega) + \ldots + (-1)^{m-1} \omega^{m-1}(b_{m-1} + \omega b_m) + (-1)^m \omega^m b_m = 1,
\]

using \(|\omega| \leq 1\), we deduce that

\[|b_1 \omega + 1| + |b_2 \omega + b_1| + \ldots + |b_m \omega + b_{m-1}| + |b_m|\]

\[\geq |b_1 \omega + 1| + |\omega| |b_2 \omega + b_1| + \ldots + |\omega|^{m-1} |b_m \omega + b_{m-1}| + |\omega|^m |b_m| \geq 1.
\]

Hence \(L((\omega + x)G(x)) \geq |\omega| + 1\) for any \(G \in \Gamma_0\), giving \(\ell_0(\omega + x) \geq 1 + |\omega|\). Combining this inequality with the trivial inequality \(\ell_0(\omega + x) \leq L(\omega + x) = 1 + |\omega|\) we obtain \(\ell_0(\omega + x) = 1 + |\omega|\).

For the third part, set \(G_0(x) = 1 + x/\eta + (x/\eta)^2 + \ldots + (x/\eta)^m\). Then, for arbitrary \(G \in \Gamma_0, T(x)G(x)G_0(x) = Q(x)G(x)(1 - (x/\eta)^{m+1}),\) giving 
\(L(TG_0G_0) \leq L(QG)(1+|\eta|^{-m-1}).\) Since \(GG_0 \in \Gamma_0\) and \(|\eta| > 1\), this yields \(\ell_0(T) \leq \ell_0(Q)\), because we can take \(m\) arbitrarily large. On the other hand, since \((1-x/\eta)Q(\eta) \in \Gamma_0\) if \(G \in \Gamma_0\), from \(TG = (1 - x/\eta)QG\) we deduce that \(\ell_0(Q) \leq \ell_0(T)\). Hence \(\ell_0(T) = \ell_0(Q)\).

The proof of (iv) is exactly the same, because \((1-x/\nu)(1-x/\tau) \in \Gamma_0\), so setting

\[G_0(x) = (1 + x/\nu + \ldots + (x/\nu)^m)(1 + x/\tau + \ldots + (x/\tau)^m) \in \Gamma_0
\]

we can argue as above. \(\square\)
Proof of Proposition 1. Without loss of generality we may assume that $|\alpha_1|, \ldots, |\alpha_k| > 1$ and $|\alpha_k+1|, \ldots, |\alpha_d| \leq 1$. Recall that $M(\alpha) = a_d|\alpha_1 \ldots \alpha_k|$. We can write

$$P(x) = a_d(x-\alpha_1) \ldots (x-\alpha_d) = \pm M(\alpha)(1-x/\alpha_1) \ldots (1-x/\alpha_k)(x-\alpha_{k+1}) \ldots (x-\alpha_d).$$

On applying Proposition 2(i), (iii) and (iv), we get

$$\ell_0(\alpha) = M(\alpha)\ell_0((x-\alpha_{k+1}) \ldots (x-\alpha_d)).$$

If $\alpha$ has all conjugates outside the unit circle, namely $k = d$, then $M(\alpha) = a_d|\alpha_1 \ldots \alpha_d| = |a_0|$, so $\ell_0(\alpha) = |a_0|$. If $\alpha' = \alpha_d$ is the unique conjugate of $\alpha$ in the unit disc, it must be a real number. Applying Proposition 1(i) and (ii) and using $M(\alpha) = |a_0|/|\alpha'|$, we get $\ell_0(\alpha) = M(\alpha)(1+|\alpha'|) = |a_0|(1+1/|\alpha'|)$, as claimed. This completes the proof of Proposition 1.

Note that if $\alpha'$ is any conjugate of $\alpha$ satisfying $|\alpha'| > 1$ then, taking $G_0(x) = 1 + x/\alpha' + (x/\alpha')^2 + \ldots + (x/\alpha')^m$ with $m$ sufficiently large, from $\ell_0(\alpha) \leq L(PG_0)$ we obtain

$$\ell_0(\alpha) \leq |a_0| + \frac{|a_0 + a_1\alpha'|}{|\alpha'|} + \frac{|a_0 + a_1\alpha' + a_2\alpha'^2|}{|\alpha'|^2} + \ldots + \frac{|a_0 + a_1\alpha' + \ldots + a_d\alpha_d^d|}{|\alpha'|^{d-1}}.$$

Naturally, we conclude with the following problem: find $\ell_0(P) = \inf_{G \in \Gamma_0} L(PG)$ for each $P(x) \in \mathbb{R}[x]$. This will give a respective value for

$$\ell(P) = \inf_{G \in \Gamma} L(PG) = \min\{\ell_0(P), \ell_0(P^*)\},$$

and, in the case when $P$ is an integer irreducible polynomial having a root $\alpha > 1$, a lower bound for $\Delta(\xi, \alpha)$ via Theorem 1. A similar problem in $L_2$-norm was solved a long time ago. A theorem of Szeg"{o} implies that $\inf_{G \in \Gamma_0} L_2(PG) = M(P)$. (See, for instance, [20, pp. 227, 261] for a respective result of Ruzsa for polynomials in several variables.) Of course, $G^* \in \Gamma_0$ means nothing else but that $G$ is a monic polynomial with real coefficients. Since $M(P) = M(P^*)$, this implies that $\inf_{G \in \Gamma} L_2(PG) = M(P)$.

Acknowledgements. The author thanks the referee for some useful corrections and Toufik Zaïmi for drawing the author’s attention to a gap in the initial proof of Theorem 3. The research was partially supported by the Lithuanian State Science and Studies Foundation.

References


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