A characterization of Mahler’s generalized Liouville numbers by simultaneous rational approximation

Andreas Dress, Noam D. Elkies, and Florian Luca
February 2003

Abstract. Given a real number \(\alpha\), we consider the set \(\mathcal{LM}(\alpha)\) of all positive real numbers \(\tau\) for which there exist, for every \(s \in \mathbb{N}\), infinitely many \((s + 1)\)-tuples \(q, p_1, \ldots, p_s\) of integers with \(q > 0\) and \(|p_k - q\alpha^k| \leq C q^{-\frac{2}{3}}\) for some \(C > 0\), and show that a non-rational number \(\alpha\) is algebraic of degree \(m\) if and only if \(\mathcal{LM}(\alpha) = [m, \infty)\) holds, that \(\alpha\) is a Mahler \(U_m\) number if and only if \(\mathcal{LM}(\alpha) = (m, \infty)\) holds, and that \(\mathcal{LM}(\alpha)\) is empty for all other non-rational real numbers \(\alpha\).

Apart from combining elementary and straightforward, yet rather lengthy computations and estimations keeping good control of all the quantifiers involved, the proof makes use of some properties of an apparently new canonical \(\mathbb{Z}\)-basis of the \(\mathbb{Z}\)-module consisting of all homogeneous polynomials of degree \(e\) in \(m\) variables.

1 Introduction

It is well known and goes back at least to Kronecker (see, for example, Theorem VII in Diophantine Approximation by J.W.S. Cassels or 2.1 below) that, given \(s\) real numbers \(\alpha_1, \alpha_2, \ldots, \alpha_s\), there exist infinitely many \((s + 1)\)-tuples of integers \((p_1, p_2, \ldots, p_s, q)\) with \(q > 0\) such that

\[
|\alpha_k - \frac{p_k}{q}| \leq \frac{1}{q^{\frac{s}{s+1}}}
\]

holds for all \(k = 1, 2, \ldots, s\) whenever \(s\) does not exceed \(\tau\). In addition, it is also noted in Cassels’ book that, in general, this is best possible.

This can be rephrased as follows:

- For any real number \(\beta\), denote by

\[
[\beta] := \lfloor \beta + \frac{1}{2} \rfloor
\]

that integer \(n \in \mathbb{Z}\) that is closest to \(\beta\) (i.e., with \(\min(|\beta - n'| : n' \in \mathbb{Z}) = |\beta - n|\) — and, in case there are two such integers, the larger one of both.

- For any \(s\)-vector \(\xi = (\xi_1, \xi_2, \ldots, \xi_s) \in \mathbb{R}^s\), denote by

\[
\langle \xi \rangle = \langle \xi \rangle_{\infty} := \max_{i=1, \ldots, s} \|\xi_i\| = \min_{n_1, \ldots, n_s \in \mathbb{Z}} \left( \max_{i=1, \ldots, s} |n_i - \xi_i| \right)
\]
the minimum of the $L_\infty$ distances of $\xi$ to the points $(n_1, \ldots, n_s)$ in the lattice $\mathbb{Z}^s$.

- And for $\alpha_1, \alpha_2, \ldots, \alpha_s \in \mathbb{R}$ as above, let $F_{\alpha_1, \alpha_2, \ldots, \alpha_s}(q)$ denote the sequence defined by

$$F_{\alpha_1, \alpha_2, \ldots, \alpha_s}(q) := (q(\alpha_1, \alpha_2, \ldots, \alpha_s)) = ((q\alpha_1, q\alpha_2, \ldots, q\alpha_s)).$$

Then, the two assertions above are essentially equivalent to asserting that

$$\lim_{q \to \infty} q^{1/\tau} F_{\alpha_1, \alpha_2, \ldots, \alpha_s}(q) \leq 1$$

holds for all $\alpha_1, \alpha_2, \ldots, \alpha_s \in \mathbb{R}$ for $\tau := s$, but not always for any smaller $\tau$.

In other words, defining

$$X(\tau) := \{G \in \mathbb{R}^N \mid \lim_{q \to \infty} q^{1/\tau}|G(q)| < \infty\}$$

for $\tau > 0$, the above assertions are equivalent to asserting that

$$[s, \infty) = \{\tau \in \mathbb{R}_{>0} \mid F_{\alpha_1, \alpha_2, \ldots, \alpha_s} \in X(\tau) \text{ for all } \alpha_1, \alpha_2, \ldots, \alpha_s \in \mathbb{R}\}$$

holds for any $s \in \mathbb{N}$.

Here, it will be shown that in case $\alpha_1 := \alpha, \alpha_2 := \alpha^2, \ldots, \alpha_s := \alpha^s$ for some $\alpha \in \mathbb{R}$, much more precise results can be derived. To state our results in a convenient form, let us first define $X(\tau)$ also for $\tau := 0$ by

$$X(0) := \{G \in \mathbb{R}^N \mid G(q) = 0 \text{ for infinitely many } q \in \mathbb{N}\}.$$ 

Next, given any $\alpha \in \mathbb{R}$, put

$$\mathcal{LM}(\alpha) := \{\tau \in \mathbb{R}_{>0} \mid F_{\alpha,s} := F_{\alpha, \alpha^2, \ldots, \alpha^s} \in X(\tau) \text{ holds for all } s \in \mathbb{N}\}$$

and define the **Liouville–Mahler index** $LM(\alpha)$ of $\alpha$ by

$$LM(\alpha) := 1 + \inf \mathcal{LM}(\alpha).$$

Note that one has

$$\inf\{q^{1/s}F_{\alpha,s}(q) \mid q \in \mathbb{N}\} = 0$$

for all $s \in \mathbb{N}$ and all $\tau \in \mathbb{R}$ with $\tau > \inf \mathcal{LM}(\alpha)$ and, therefore, also

$$LM(\alpha) = 1 + \inf \{\tau \in \mathbb{R}_{>0} \mid \inf\{q^{1/s}F_{\alpha,s}(q) \mid q \in \mathbb{N}\} = 0 \text{ for all } s \in \mathbb{N}\}.$$ 

The perhaps most surprising consequence of the results that we will establish below is the following rather strange characterization of positive integers:

**Theorem 1.1** A positive real number $\tau$ is an integer if and only if there exists some real number $\alpha$ with $LM(\alpha) = \tau$. 

2
Remarkably, we can also describe the real numbers $\alpha$ for which $LM(\alpha) = m$ holds for some positive integer $m$ as follows: Recall that a real number $\alpha$ is, by definition, exclusively either an algebraic number or a Mahler $U$ number of degree $e$ for some $e \leq m$ if and only if there exist, for each $t \in \mathbb{R}$, some integers $a_0 = a_0(t), \ldots, a_m = a_m(t)$ with $a_m \neq 0$ that satisfy the inequality 

$$\left| \sum_{i=0}^{m} a_i \alpha^i \right| < \left( 1 + \sum_{i=0}^{m} |a_i| \right)^{-t}$$

in which case the smallest number $m$ for which this holds is also called the degree of $\alpha$ — as an algebraic number if there exists integers $a_0, \ldots, a_m$ with $a_m \neq 0$ and $\sum_{i=0}^{m} a_i \alpha^i = 0$, and as a Mahler $U$ number if $\sum_{i=0}^{m} a_i \alpha^i \neq 0$ holds for all $a_0, \ldots, a_m \in \mathbb{Z}$ with $a_m \neq 0$ (cf. [4, 6, 7]). Recall also that the Mahler $U$ numbers include the Liouville numbers which are exactly the Mahler $U$ numbers of degree 1 and that — just like the Liouville numbers — all Mahler $U$ numbers are transcendental.

Indeed, Liouville introduced his numbers as examples of transcendental numbers, and his proof readily generalizes to $U$-numbers: Assume on the contrary that a $U$ number $\alpha$ of degree $m$ is algebraic of degree $d$; then there exists a positive $N \in \mathbb{Z}$ such that $N \alpha^i$ is an algebraic integer for each $i = 0, 1, \ldots, m$ and thus so is $\nu := N \sum_{i=0}^{m} c_i \alpha^i$ for any $c_i \in \mathbb{Z}$. But then, if $\nu \neq 0$, the product of $\nu$ with its $d - 1$ conjugates is also a nonzero integer and so it has absolute value at least 1. Each of these conjugates is $\ll \sum_{i=0}^{m} |c_i|$, the implied constant depending on $\alpha$ and $m$, but not on the $c_i$. Thus,

$$\left( \sum_{i=0}^{m} |c_i| \right)^{1-d} \ll |\nu|,$$

implying that

$$\left( 1 + \sum_{i=0}^{m} |a_i| \right)^{1-d} \ll |\nu| \leq \left( 1 + \sum_{i=0}^{m} |a_i| \right)^{-t}$$

and, hence,

$$\left( 1 + \sum_{i=0}^{m} |a_i| \right)^{1+t-d} \ll 1$$

holds for every solution $a_0, a_1, \ldots, a_m$ of (2), so (2) can have only finitely many solutions once $t > d - 1$ holds. In consequence, as a Mahler $U$ number of degree $m$ cannot simultaneously show up as an algebraic number of degree $m' > m$, the degree $\deg(\alpha)$ of any real number $\alpha$ is well defined (being infinite if and only if $\alpha$ is neither algebraic nor a Mahler $U$ number).

Theorem 1.1 above is clearly a simple consequence of the following rather explicit description of the sets $\mathcal{L}M(\alpha)$:
**Theorem 1.2** The degree $m$ of a real number $\alpha$ and its Liouville–Mahler index always coincide, and one has

$$\mathcal{L}\mathcal{M}(\alpha) = [m - 1, \infty)$$

if and only if $\alpha$ is an algebraic number of degree $m$, and

$$\mathcal{L}\mathcal{M}(\alpha) = (m - 1, \infty)$$

if and only if $\alpha$ is a Mahler $U$ number of degree $m$.

To establish these results, we will introduce a third numerical invariant of $\alpha$ that is defined as follows: For each $q \in \mathbb{N}$, consider the infinite sequence $P(q, \alpha) := (p_0(q, \alpha), p_1(q, \alpha), p_2(q, \alpha), \ldots)$ defined by

$$p_i(q, \alpha) := \lfloor q \alpha^i \rfloor$$

for all $i = 0, 1, 2, \ldots$, and its various Hankel matrices

(3) \hspace{1cm} \mathcal{H}_{m,n}(q, \alpha) := \mathcal{H}_{m,n}(P(q, \alpha)) = (p_{i+j}(q, \alpha))_{i=0, \ldots, m; j=0, \ldots, n},

put

(4) \hspace{1cm} Q_{rk}(m, n) := \{q \in \mathbb{N} | \text{rk} \ \mathcal{H}_{m,n}(q, \alpha) < m + 1\}

for all $m, n \in \mathbb{N}$, and put

(5) \hspace{1cm} m(\alpha) := \min \{m \in \mathbb{N} | \lim \mathcal{F}_{\alpha, m+n} | Q_{rk}(m, n) = 0 \text{ holds for every } n \in \mathbb{N}\}

where, for any real-valued map $G$ defined on a set containing a given set $X$, we put

$$\lim (G | X) := \inf (\rho \in \mathbb{R} | \# \{x \in X | G(x) \leq \rho\} = \infty)$$

$$= \sup (\rho \in \mathbb{R} | \# \{x \in X | G(x) \leq \rho\} < \infty)$$

so that

$$\lim (G | X) = \lim_{q \in X, q \to \infty} G(q)$$

holds in case $X$ is an infinite subset of $\mathbb{N}$.

Theorem 1.2 is obviously a consequence of the following three results:

**Theorem 1.3** (i) One has

$$\mathcal{L}\mathcal{M}(\alpha) \leq \text{deg}(\alpha)$$

for every real number $\alpha$.

(ii) And one has

$$\text{deg}(\alpha) - 1 \in \mathcal{L}\mathcal{M}(\alpha)$$
for every algebraic real number $\alpha$. In other words,
\[
(\deg(\alpha) - 1, \infty) \subseteq \mathcal{LM}(\alpha)
\]
holds for all $\alpha \in \mathbb{R}$, and
\[
[\deg(\alpha) - 1, \infty) \subseteq \mathcal{LM}(\alpha)
\]
holds for every algebraic number $\alpha \in \mathbb{R}$.

**Theorem 1.4** (i) One has
\[
\deg(\alpha) \leq m(\alpha)
\]
for every non-zero real number $\alpha$. (ii) A real number $\alpha$ with $m(\alpha) - 1 \in \mathcal{LM}(\alpha)$ is an algebraic number.

**Theorem 1.5** One has
\[
m(\alpha) \leq \mathcal{LM}(\alpha)
\]
or, equivalently,
\[
\mathcal{LM}(\alpha) \subseteq [m(\alpha) - 1, \infty)
\]
for every real number $\alpha$.

Thus, we have
\[
\deg(\alpha) = m(\alpha) = \mathcal{LM}(\alpha) \in \mathbb{N}
\]
as well as
\[
(\deg(\alpha) - 1, \infty) \subseteq \mathcal{LM}(\alpha) \subseteq [\deg(\alpha) - 1, \infty)
\]
for every real $\alpha \in \mathbb{R}$, and equality holds on the right-hand side if and only if one has
\[
m(\alpha) - 1 = \deg(\alpha) - 1 \in \mathcal{LM}(\alpha)
\]
and, thus, if (Theorem 1.3, (ii)) and only if (Theorem 1.4, (ii)) $\alpha$ is an algebraic number.

We will prove Theorem 1.3 in the next section. Then we will prove Theorem 1.5. In the last section, we will prove Theorem 1.4.

## 2 Proof of Theorem 1.3

In this section, we are going to show that
\[
m - 1 \in \mathcal{LM}(\alpha)
\]
holds for every algebraic number $\alpha$ of degree $m$, and that
\[
\tau \in \mathcal{LM}(\alpha)
\]
holds for every $\tau > m - 1$ in case $\alpha$ is a Mahler $U$ number of degree $m$. We will do this by first recalling Kronecker's famous Approximation Lemma, i.e. by establishing that (1) holds indeed for any family of real numbers $\alpha_1, \alpha_2, \ldots, \alpha_s$, and by showing then that, given any real number $\alpha$ and any polynomial $f(x) = a_m x^m + a_{m-1} x^{m-1} + \ldots + a_0$ of degree $m$ with integral coefficients for which $|f(\alpha)| \leq 1$ holds, one can derive useful estimates of $\langle r a_m^{-m+1} a^n \rangle$ for any integer $s \geq m$ and any positive integer $r$ in terms of the sum $\sum_{i=1}^{m-1} \langle r a_i^i \rangle + r |f(\alpha)|$.

2.1 Kronecker's Lemma

The following fact has been established by L.Kronecker in 1870 (cf. [5]):

\textbf{Lemma} Given any family of $s$ real numbers $\alpha_1, \alpha_2, \ldots, \alpha_s$ and some real number $R > 1$, there exists some $r = r_R \in \{1, 2, \ldots, \lfloor R \rfloor\}$ with

$$\langle r \alpha_1, r \alpha_2, \ldots, r \alpha_s \rangle \leq (1/R)^{1/s}.$$  

\textbf{Proof:} For every vector $\xi = (\xi_1, \xi_2, \ldots, \xi_s) \in \mathbb{R}^s$, let $[\xi]$ denote the (closed) subset of the $s$-dimensional torus $\mathbb{R}^s/\mathbb{Z}^s$ consisting of all cosets of the form $\eta + \mathbb{Z}^s \in \mathbb{R}^s/\mathbb{Z}^s$ for some $\eta = (\eta_1, \eta_2, \ldots, \eta_s) \in \mathbb{R}^s$ with

$$\langle \xi - \xi \rangle \leq (1/R)^{1/s}/2$$

and note that the volume of $[\xi]$ (relative to the canonical Haar measure defined on $\mathbb{R}^s/\mathbb{Z}^s$) is $1/R$. Hence, there must exist two integers among the $1 + \lfloor R \rfloor > R$ integers in $r_1, r_2 \in \{0, 1, 2, \ldots, \lfloor R \rfloor\}$ with $r_1 < r_2$ and $[r_1(\alpha_1, \alpha_2, \ldots, \alpha_s)] \cap [r_2(\alpha_1, \alpha_2, \ldots, \alpha_s)] \neq \emptyset$. Thus, choosing some $\eta = (\eta_1, \eta_2, \ldots, \eta_s) \in \mathbb{R}^s$ with

$$\eta + \mathbb{Z}^s \in [r_1(\alpha_1, \alpha_2, \ldots, \alpha_s)] \cap [r_2(\alpha_1, \alpha_2, \ldots, \alpha_s)]$$

and putting $r = r_R := r_2 - r_1$ so that $r \in \{1, 2, \ldots, \lfloor R \rfloor\}$ clearly holds, we get

$$\langle r(\alpha_1, \ldots, \alpha_s) \rangle$$

$$\leq \langle r(\alpha_1, \ldots, \alpha_s) - r(\alpha_1, \ldots, \alpha_s) \rangle$$

$$\leq \langle r(\alpha_1, \ldots, \alpha_s) - \eta \rangle + \langle \eta - r(\alpha_1, \ldots, \alpha_s) \rangle$$

$$\leq (1/R)^{1/s}/2 + (1/R)^{1/s}/2 = (1/R)^{1/s},$$

as required. \qed

\textbf{Corollary 2.1} Given any family of real numbers $\alpha_1, \alpha_2, \ldots, \alpha_s$, one has

$$\lim_{q \to \infty} q^{1/s} F_{\alpha_1, \ldots, \alpha_s}(q) \leq 1.$$

\textbf{Proof:} All one needs to observe is that $r \leq R$ and $\langle r(\alpha_1, \ldots, \alpha_s) \rangle \leq (1/R)^{1/s}$ together imply $r^{1/s}\langle r(\alpha_1, \ldots, \alpha_s) \rangle \leq R^{1/s}\langle r(\alpha_1, \ldots, \alpha_s) \rangle \leq 1$, and that there
must exist infinitely many distinct positive integers \( r \) of the form \( r = r_R \) for some \( R > 1 \), unless \( \langle r(\alpha_1, \ldots, \alpha_s) \rangle = 0 \) holds for some positive integer \( r \) in which case all products \( r \alpha_i \) must be integers and one has \( \langle k^r(\alpha_1, \ldots, \alpha_s) \rangle = 0 \) for all \( k \in \mathbb{N} \), implying that the even stronger claim \( F_{\alpha_1, \ldots, \alpha_s} \in X(0) \) holds in this case.

2.2 A crucial inequality

In the next two subsections, we will have to combine Kronecker’s Lemma with the following result that will be crucial for establishing (6) and (7).

**Lemma 2.2** Consider a real number \( \alpha \) and a polynomial

\[
f(x) = a_m x^m + a_{m-1} x^{m-1} + \ldots + a_0
\]

of degree \( m \) with integral coefficients \( a := a_m > 0, a_{m-1}, \ldots, a_1, a_0 \) for which \( |f(\alpha)| \leq 1 \) holds. Then,

\[
\langle r a^k \alpha^{k+m-1} \rangle \leq A^k \left( r |f(\alpha)| + \sum_{i=1}^{m-1} \langle r \alpha^i \rangle \right)
\]

holds, with

\[
A := 1 + \sum_{i=0}^{m-1} |a_i|
\]

for all positive integers \( r, k \).

Proof: Recall that, for every \( k \in \mathbb{N}_0 \), there exist unique polynomials \( u^{(k)}(x) \) of degree \( k - 1 \) and \( v^{(k)}(x) = \sum_{i=0}^{m-1} v^{(k)}_i x^i \) of degree at most \( m - 1 \) in \( \mathbb{R}[x] \) such that

\[
a^k x^{k+m-1} = u^{(k)}(x) f(x) + v^{(k)}(x)
\]

holds.

Moreover, using the fact that

\[
a^{k+1} x^{k+m} = a x (a^k x^{k+m-1}) = a x u^{(k)}(x) f(x) + a x v^{(k)}(x) = (a x u^{(k)}(x) + v^{(k)}_{m-1}) f(x) + (a x v^{(k)}(x) - v^{(k)}_{m-1} f(x))
\]

holds for every \( k \in \mathbb{N}_0 \), we see that the recursion formulae

\[
u^{(k+1)}(x) = a x u^{(k)}(x) + v^{(k)}_{m-1}
\]

hold.
and

\[ v^{(k+1)}(x) = x v^{(k)}(x) - v^{(k)}_{m-1} f(x) \]

holds for every \( k \in \mathbb{N}_0 \).

Thus, noting that also

\[ u^{(0)}(x) := 0 \quad \text{and} \quad v^{(0)}(x) := x^{m-1} \]

holds, we get

\[ u^{(k)}(x), v^{(k)}(x) \in \mathbb{Z}[x] \]

as well as

\[ v^{(k+1)}_0 = - v^{(k)}_{m-1} a_0 \]

and

\[ v^{(k+1)}_i = a v^{(k)}_{i-1} - v^{(k)}_{m-1} a_i \]

for all \( k \in \mathbb{N}_0 \) and all \( i = 1, \ldots, m - 1 \).

It follows that

\[ |v^{(k+1)}_i| \leq A |v^{(k)}_i| \leq \cdots \leq A^{k+1} \]

holds for all \( k \in \mathbb{N}_0 \) and all \( i = 0, \ldots, m - 1 \).

Similarly, assuming that \( |u^{(k)}(\alpha)| \leq A^k \) holds (which is clearly true for \( k := 0 \)) and noting that

\[ |\alpha| \leq A \]

holds obviously for \( |\alpha| \leq 1 \), and that it holds also in case \( |\alpha| > 1 \) because our assumption \( |f(\alpha)| \leq 1 \) then implies

\[ |\alpha| = |f(\alpha)| \alpha^{-m} - \sum_{i=0}^{m-1} a_i \alpha^{-(m-i)}| \]

\[ \leq 1 + \sum_{i=0}^{m-1} |a_i| = A - a \leq A - 1, \]

we get

\[ |u^{(k+1)}(\alpha)| = |\alpha^k u^{(k)}(\alpha) + v^{(k)}_{m-1}| \leq (A - 1) A^k + A^k = A^{k+1}. \]

Thus, \( |u^{(k)}(\alpha)| \leq A^k \) must also hold for every \( k \in \mathbb{N}_0 \).

In consequence, we have

\[ \langle ra^k \alpha^{k+m-1} \rangle = \langle r(u^{(k)}(\alpha) + v^{(k)}(\alpha)) \rangle \]

\[ \leq \langle r(u^{(k)}(\alpha) f(\alpha) + v^{(k)}(\alpha)) \rangle + \sum_{i=0}^{m-1} \langle rv_i^{(k)} \alpha^i \rangle \]

\[ \leq r |f(\alpha)| A^k + \sum_{i=0}^{m-1} A^k (ra^i) \]

\[ = A^k (r |f(\alpha)| + \sum_{i=0}^{m-1} (ra^i)) \]

8
for every \( k \geq 1 \). Noting finally that \( \langle r \alpha^0 \rangle = \langle r \rangle = 0 \) holds for any integer \( r \), this establishes the assertion (9) above.

\[
\text{Remarks:}
\]

(1) Note that the above proof shows that the lemma holds for every map
\[
\mathbb{R} \to \mathbb{R}_{\geq 0} : \alpha \mapsto \langle \alpha \rangle
\]
with
\[
\langle \alpha + \beta \rangle \leq \langle \alpha \rangle + \langle \beta \rangle
\]
and
\[
\langle \alpha \rangle \leq |\alpha|
\]
for all \( \alpha, \beta \in \mathbb{R} \).

(2) Note also that the above arguments can be rephrased so as to yield considerably sharper inequalities for \( \langle r \alpha^k \alpha^{k+m-1} \rangle \) that will, however, not be needed in the proofs below.

### 2.3 The case of algebraic numbers

Now, assume that \( \alpha \) is an algebraic number of degree \( m \) and that, more precisely, 
\[
f(\alpha) = \sum_{i=0}^{m} a_i \alpha^i = 0
\]
holds for some integers \( a_0, a_1, \ldots, a_{m-1}, a_m = a \) with \( a > 0 \).

We want to show that \( m - 1 \in \mathcal{L}M(\alpha) \) holds. As this is obvious in case \( m = 1 \), we will assume from now on for the rest of this subsection that \( m > 1 \) holds. To establish our claim, it will be enough to show that, continuing with the notation that we developed above, the inequality
\[
q^{1/m-1} \langle qa, qa^2, \ldots, qa^m \rangle \leq (m - 1)A^{2(s-m+1)}
\]
holds, with \( A := \sum_{i=0}^{m} |a_i| \), in case \( m > 1 \) for every \( s \geq m \) and infinitely many integers \( q \in \mathbb{N} \). To find those integers \( q \), we use Lemma 2.1 to find, for any integer \( R > 1 \), some \( r = r_R \in \{1, \ldots, R\} \) with
\[
\langle r \alpha, r \alpha^2, \ldots, r \alpha^{m-1} \rangle \leq (1/R)^{1/m-1}.
\]

Next, we note that the set \( \{r_R | R \in \mathbb{N}\} \) of distinct integers \( r \) that we find in this way must be infinite because, otherwise, there would exist some \( r_0 \in \mathbb{N} \) with \( r_0 = r_R \) for infinitely many members \( R \in \mathbb{N} \) which in turn would imply \( \langle r_0 \alpha \rangle = 0 \) and therefore \( r_0 \alpha \in \mathbb{Z} \), in contradiction to our assumption that \( \alpha \) is an algebraic number of degree larger than 1.
We now put
\[ q = q_R := a^{s-m+1} r = a^{s-m+1} r_R \]
for any \( R \) as above and consider the term
\[ q^{1/m-1} \langle q \alpha^i \rangle. \]
If \( 1 \leq i \leq m - 1 \) holds, we have
\[
q^{1/m-1} \langle q \alpha^i \rangle = q^{1/m-1} \langle a^{s-m+1} r \alpha^i \rangle \\
\leq a^{s-m+1} (q/R)^{1/m-1} = a^{s-m+1} (a^{s-m+1} r/R)^{1/m-1} \\
\leq a^{s-m+1} (a^{s-m+1})^{1/m-1} \\
\leq a^{2(s-m+1)} \\
\leq (m - 1) A^{2(s-m+1)},
\]
as required.

In the less trivial case \( m \leq i \leq s \), we put \( k := i - m + 1 \) and observe that Lemma 2.2 yields
\[
q^{1/m-1} \langle q \alpha^i \rangle = q^{1/m-1} \langle a^{s-m+1} k \alpha^{k-m+1} \rangle \\
= q^{1/m-1} \langle a^{s-i} A^k \alpha^{k-m+1} \rangle \\
\leq q^{1/m-1} a^{s-i} A^k \sum_{i=1}^{m-1} \langle r \alpha^i \rangle \\
\leq a^{s-i} A^k (m - 1) (q/R)^{1/m-1} \\
= a^{s-i} A^k (m - 1) (a^{s-m+1} r/R)^{1/m-1} \\
\leq A^{s-i} A^{1-m+1} (m - 1) (a^{s-m+1})^{1/m-1} \\
\leq A^{s-m+1} (m - 1) (A^{s-m+1})^{1/m-1} \\
\leq (m - 1) A^{2(s-m+1)},
\]
also as required. This establishes our claim
\[ m - 1 \in \mathcal{L}(\alpha) \]
in case \( \alpha \) is an algebraic number \( \alpha \) of degree \( m \).

### 2.4 The case of Mahler \( U \) numbers

Now, assume that \( \alpha \) is a Mahler \( U \) number of degree \( m \geq 1 \), that \( \tau \) is a real number with \( \tau > m - 1 \), and that \( s \) is any integer with \( s \geq m \). Clearly, it is enough to show that
\[
q^{1/\tau} \langle q \alpha, q \alpha^2, \ldots, q \alpha^s \rangle \leq m
\]
holds for infinitely many distinct integers $q \in \mathbb{N}$. To this end, we choose some real number $t$ with

$$ t > \frac{m(s + 1)(\tau + 1)}{\tau - m + 1} \quad (> 2) $$

and integers $a = a_m = a_m(t), a_{m-1} = a_{m-1}(t), \ldots, a_1 = a_1(t), a_0 = a_0(t)$ with $a > 0$ so that

$$ |f(\alpha)| \leq (1 + \sum_{i=0}^{m} |a_i|)^{-2t} \quad (< 1) $$

holds for the value $f(\alpha)$ of the polynomial

$$ f(x) = f_t(x) := \sum_{i=0}^{m} a_i x^i. $$

Observe first that with $A := \sum_{i=0}^{m} |a_i|$ as above, one has

$$ A = \sum_{i=0}^{m} |a_i| < (1 + \sum_{i=0}^{m} |a_i|)^2 $$

and, hence,

$$ |f(\alpha)| \leq (1 + \sum_{i=0}^{m} |a_i|)^{-2t} < A^{-t} $$

which implies that

$$ \langle ra^k \alpha^{k+m-1} \rangle \leq A^k \left( \sum_{i=1}^{m-1} \langle ra^i \rangle + rA^{-t} \right) $$

must hold for every $r \in \mathbb{N}$. Next, using Kronecker’s Lemma once more, choose some positive integer $r = r_t \leq A^{t(m-1)/m}$ such that

$$ \langle ra, ra^2, \ldots, ra^{m-1} \rangle \leq A^{-t/m} $$

holds and put

$$ q = q_t := a^s r A. $$

As above, there must be infinitely many distinct integers $r$ of the form $r = r_t$ in view of the fact that a Mahler $U$ number is not even an algebraic number, so there are also infinitely many distinct integers $q$ of the form $q = q_t$. Consequently, all we have to show is that

$$ q^{1/\tau} \langle q\alpha, q\alpha^2, \ldots, q\alpha^s \rangle \leq m $$

holds for every $t$, for the integer $q = q_t$ defined above. If $1 \leq i \leq m - 1$ holds, this follows from

$$ q^{1/\tau} \langle q\alpha^i \rangle = (a^s r A)^{1/\tau} \langle a^s r A \alpha^i \rangle $$

$$ \leq r^{1/\tau} (a^s A)^{1+1/\tau} \langle rA^i \rangle $$

$$ \leq A^t (m-1)/m \cdot A^{(s+1)(1+1/\tau)} A^{-t/m} $$

$$ < 1 \leq m $$
in view of our assumption

\[ t > \frac{m(s+1)(\tau + 1)}{\tau - m + 1} \]

as multiplying both sides with \((\tau - m + 1)/m \tau = 1/m - (m - 1)/m \tau\) and adding \(t(m-1)/m \tau\), this implies

(10) \[ \frac{t}{m} > \frac{t(m-1)}{m \tau } + (s+1)(1+\tau ) \]

Similarly, putting \(k := i - m + 1\) and applying Lemma 2.2 as above in case \(m \leq i \leq s\), we get

\[ q^{1/\tau} \langle q \alpha^i \rangle = (a^\tau A)^{1/\tau} \langle a^\tau A \alpha^i \rangle \leq r^{1/\tau} (a^\tau A)^{1/\tau} A^{s-k} \langle q^{k+1} \alpha^{k+1} \rangle \]

\[ \leq A^{t(m-1)/m \tau} (a^\tau A)^{1/\tau} A^{s-k} A^k (r_1 f(\alpha)) + \sum_{i=1}^{m-1} \langle r \alpha^i \rangle \]

\[ \leq A^{t(m-1)/m \tau} A^{(s+1)(1+1/\tau)} (A^{t(m-1)/m} A^{t(m-1)/m} + (m-1)A^{-t/m}) \]

\[ = A^{t(m-1)/m \tau} A^{(s+1)(1+1/\tau)} (A^{-t/m} + (m-1)A^{-t/m}) \]

\[ = mA^{t(m-1)/m \tau} A^{(s+1)(1+1/\tau)} A^{-t/m} < m \]

as required, again in view of (10). This clearly establishes our claim in case \(\alpha\) is a Mahler \(U\) number of degree \(m\).

**Remark:** Obviously, the proof can be modified so as to yield

\[ \lim_{q \to \infty} q^{1/\tau} \sum_{k=0}^{s} \langle q \alpha^k \rangle = 0 \]

for any \(\tau > m - 1\). However, this follows anyway also from what we just proved as it is obviously an immediate consequence of the fact that

\[ \lim_{q \to \infty} q^{1/\tau'} \sum_{k=0}^{s} \langle q \alpha^k \rangle < \infty \]

holds for any \(\tau'\) with \(m - 1 < \tau' < \tau\).

3 Proof of Theorem 1.5

We will now show that \(m(\alpha) \leq LM(\alpha)\) holds for every real number \(\alpha\).

To this end, let us recall first that, given any sequence \(P = (p_0, p_1, \ldots, p_N)\) of elements from a commutative ring \(R\) and any two non-negative integers \(m, n\)
with \( m + n \leq N \), the associated \((m + 1) \times (n + 1)\) Hankel matrix \( \mathcal{H}_{m,n}(P) \) is defined by

\[
\mathcal{H}_{m,n}(P) := (p_{i+j})_{i=0,\ldots,m; j=0,\ldots,n}.
\]

Clearly, putting

\[
\Delta_m(h_0, h_1, \ldots, h_m | P) := \det(p_{i+j})_{i,j=0,1,\ldots,m}
\]

for all \((m+1)\)-sequences \(h_0, h_1, \ldots, h_m\) of integers in

\[
\mathbf{H}(m,n) := \{(h_0, h_1, \ldots, h_m) \in \mathbb{N}_0 \mid 0 \leq h_0 < h_1 < \cdots < h_m \leq n\}
\]

one has \( \text{rk} \mathcal{H}_{m,n} < m + 1 \) for some \( m, n \) as above if and only if one has

\[
\Delta_m(h_0, h_1, \ldots, h_m | P) = 0
\]

for all \((m+1)\)-sequences \((h_0, h_1, \ldots, h_m) \in \mathbf{H}(m,n)\) as above. Thus, Theorem 1.5 follows immediately from

**Lemma 3.1** Given any \( m, n \in \mathbb{N} \), the inequality

\[
\left| \Delta_m(h_0, h_1, \ldots, h_m | P(q, \alpha)) \right| \leq (m + 1)!q (1 + |\alpha|^m) \left(1 + |\alpha|\right)F_{\alpha,m+n}(q)^m \\
\leq (m + 1)!q (1 + |\alpha|)^{m+n} F_{\alpha,m+n}(q)^m
\]

holds for every \((h_0, h_1, \ldots, h_m) \in \mathbf{H}(m,n)\).

In particular, the set \( \{q \in \mathbb{N} \mid q^{1/m} F_{\alpha,m+n}(q) \leq \Gamma \} \) is a subset of \( Q_{\alpha k}(m,n) = \{q \in \mathbb{N} \mid \text{rk} \mathcal{H}_{m,n}(q,\alpha) < m + 1\} \) for every positive real number \( \Gamma \) with

\[
q^{1/m} F_{\alpha,m+n}(q) \Gamma^m (m + 1)! (1 + |\alpha|)^{m+n} < 1.
\]

Thus, \( Q_{\alpha k}(m,n) \) is infinite and we have

\[
\lim_{m, n \to \infty} \left(q^{1/m} F_{\alpha,m+n}(Q_{\alpha k}(m,n))\right) = 0
\]

for all \( m, n \in \mathbb{N} \) with \( m > \inf \mathcal{L}(\alpha) \) and, thus, for all \( n \in \mathbb{N} \) and for

\[
m := 1 + \lceil \inf \mathcal{L}(\alpha) \rceil = \lceil LM(\alpha) \rceil.
\]

**Proof:** To establish our claim, all we need to observe is that the value

\[
\Delta_m(h_0, h_1, \ldots, h_m | P(q, \alpha))
\]

of the determinant of the matrix

\[
\Pi_m(h_0, h_1, \ldots, h_m | P(q, \alpha)) := (p_{i+j})_{i,j=0,1,\ldots,m}
\]

does not change if we consecutively subtract (a) from the last row in this matrix the next to last row multiplied with \( \alpha \), then (b) from this row the row below
it also multiplied with $\alpha$, and so on up to, finally, we subtract the first row multiplied with $\alpha$ from the second row. Thus, noting that, with

$$\beta_i(q, \alpha) := q\alpha^i - p_i$$

for all $i \in \mathbb{N}$, we have

$$F_{a, m+n}(q) = F_{a, a^1, \ldots, a^{m+n}}(q) = \max(|\beta_i(q, \alpha)| : i = 0, 1, 2, \ldots, m + n)$$

as well as

$$|p_{i+h_j} - \alpha p_{i-1+h_j}| = |\alpha(q\alpha^{i-1+h_j} - p_{i-1+h_j}) - (q\alpha^{i+h_j} - p_{i+h_j})|$$

$$= |\alpha\beta_{i-1+h_j} - \beta_{i+h_j}|$$

$$\leq (1 + |\alpha|) F_{a, m+h_m}(q)$$

$$\leq (1 + |\alpha|) F_{a, m+n}(q)$$

we get that, in each of the $(m + 1)!$ terms in the Leibnitz expansion of the determinant of the thus transformed matrix, the factor from the first row is bounded from above by $q(1 + |\alpha|)^n$ and, thus, by $q(1 + |\alpha|)^n$ while all other $m$ factors in these terms are bounded from above by $(1 + |\alpha|)F_{a, m+n}(q)$. Thus, our claim follows from the standard argument in Diophantine Approximation (used already above to show that Mahler $U$ numbers are transcendental), i.e. because (a) $\Delta_m(h_0, h_1, \ldots, h_m | P)$ is necessarily an integer for any integral sequence $P$, and (b) 0 is the only integer of absolute value smaller than one.

\[\blacksquare\]

## 4 Proof of Theorem 1.4

Finally, to establish Theorem 1.4, we continue our investigation of Hankel matrices.

We begin with the following

**Lemma 4.1** Given any sequence $P = (p_0, p_1, \ldots, p_N)$ of elements from a field $R$ and any two non-negative integers $m, n$ with $m + n \leq N$, the following assertions are equivalent:

- $H_{m,n}(P)$ is of rank $m$ while all the matrices $H_{h,n}(P)$ are of maximal rank $h + 1$ for all $h < m$;
- $\text{rk}(H_{m,n}(P)) = \text{rk}(H_{m-1,n}(P)) = m$ holds;
- there exist elements $c_0, \ldots, c_m \in R$ with $c_m \neq 0$ and

$$\sum_{i=0}^{m} c_i p_{j+i} = 0$$

for all $j = 0, \ldots, n$, and one has $\text{rk}(H_{m-1,n}(P)) = m$. 

\[14\]
In particular, there exists a unique \((m+1)\)-tuple \(c_0, \ldots, c_m\) of integers with \(c_m > 0\), \(\gcd(c_0, \ldots, c_m) = 1\), and \(\sum_{i=0}^{m} c_ip_{j+i} = 0\) for all \(j = 0, \ldots, n\) in case \(\text{rk}(\mathcal{H}_{m,n}(P)) = \text{rk}(\mathcal{H}_{m-1,n}(P)) = m\) if \(R\) is the field of rational numbers and, thus, in particular if all elements in the sequence \(P\) are integers.

**Proof:** Indeed, if \(\text{rk}(\mathcal{H}_{m,n}(P)) \leq m\) holds, there must exist elements \(c_0, \ldots, c_m \in R\) that do not all vanish and for which (11) holds for all \(j = 0, \ldots, n\). Thus, if in addition \(\mathcal{H}_{m-1,n}(P)\) has maximal rank \(m\), we must have \(c_m \neq 0\) which in turn implies that the \((j+m)\)-th column \(p_{j+m}\) of the matrix \(\mathcal{H}_{m,n}(P)\) is linearly dependent of the \(m\) previous columns \(p_j, p_{j+1}, \ldots, p_{j+m-1}\) for all \(j = 0, \ldots, n-m\) and that we must therefore have \(m = \text{rk}(\mathcal{H}_{m,n}(P)) = \text{rk}(\mathcal{H}_{m,n-1}(P)) = \cdots = \text{rk}(\mathcal{H}_{m,m}(P)) = \text{rk}(\mathcal{H}_{m,m-1}(P))\) while the fact that also the last row in the matrix \(\mathcal{H}_{m,m-1}(P)\) must be linearly dependent of the first \(m\) rows in case \(c_m \neq 0\) implies \(\text{rk}(\mathcal{H}_{m,m-1}(P)) = \text{rk}(\mathcal{H}_{m-1,m-1}(P))\) and hence \(\text{rk}(\mathcal{H}_{m-1,m-1}(P)) = m\). Thus, all \(m\) rows in \(\mathcal{H}_{m-1,m-1}\) must be linearly independent implying that also \(\text{rk}(\mathcal{H}_{h,n}) = h+1\) must hold for all \(h = 0, \ldots, m-1\).

More generally, defining the \(m \times m\) matrices

\[
\Pi_{m-1}(n\mid P) = (p_{i+nj})_{i,j=0,\ldots,m-1}
\]

for every \(m\)-tuple \(n = (n_0, \ldots, n_{m-1})\) of integers \(n_0, \ldots, n_{m-1}\) with \(0 \leq n_j \leq n\) for all \(j = 0, \ldots, m-1\) and the corresponding determinants

\[
\Delta_{m-1}(n\mid P) := \det \Pi(n\mid P),
\]

one notes that if there exist elements \(c_0, \ldots, c_m \in R\) with \(c_m \neq 0\) such that (11) holds for all \(j = 0, \ldots, n\), one also has

\[
\sum_{i=0}^{m} c_i \Delta_{m-1}(n_0, \ldots, n_{j-1}, n_j + i, n_{j+1}, \ldots, n_{m-1}\mid P) = 0
\]

for every \(m\)-tuple \(n = (n_0, \ldots, n_{m-1})\) as above and every \(j \in \{0, \ldots, m-1\}\) with \(n_{j+m-1} \leq n\). We will show now that this simple fact can be used to derive the following remarkable consequence:

**Lemma 4.2** Given non-negative integers \(N, n, m\) with \(m+n \leq N\) and \(m \leq n+1\) as above, there exists a family \(a(k, n; h)\) of integers indexed by all triples \(k, n, h\) where \(h\) ranges over the set

\[
\mathcal{H}(m-1,n) = \{ h = (h_0, \ldots, h_{m-1}) \in \mathbb{N}^m_0 \mid 0 < h_0 < h_1 < \ldots < h_{m-1} \leq n \},
\]

\(k\) ranges over the set

\[
\mathbb{K}(m,n) := \{ k = (k_0, \ldots, k_m) \in \mathbb{N}_0^{m+1} \mid \sum_{i=0}^{m} k_i = n \},
\]

15
and \( n \) ranges over the set \( H(m - 1, k_m) \), such that, for any commutative ring \( R \), any sequence \( P = (p_0, p_1, \ldots, p_N) \) of elements from \( R \), and any family of coefficients \( c := (c_0, c_1, \ldots, c_m) \in R^{m+1} \) with

\[
\sum_{i=0}^{m} c_i p_{i+j} = 0
\]

for all \( j = 0, \ldots, n \), the identity

\[
(13) \quad \Delta^{m-1}(n|P) = c^n \sum_{h \in H(m-1, n)} a(k, n; h) \Delta^{m-1}(h|P)
\]

holds for all \( k = (k_0, \ldots, k_m) \in K(m, n) \) and all \( n \in H(m - 1, k_m) \), where \( c^k \) is defined as the product \( c^k := c_0^k c_1^k \ldots, c_m^k \).

Remarks:

(1) The integers \( a(k, n; h) \) will be defined recursively using the identity (12). We’ll need the condition \( n \in H(m - 1, k_m) \) (or, equivalently, \( n_m - 1 \leq k_m \)) in that recursion in order to guarantee that all those terms are well defined to which we’ll need to refer in Definition (16).

(2) One can also show that, somehow conversely, there exists also a family \( b(h; k) = b_{m,n}(h; k) \) of integers indexed by all pairs \( (h, k) \) in \( H(m - 1, n) \times K(m, n) \) with \( b_{m,n}(h; k) = 0 \) for all \( (h, k) \) in \( H(m - 1, n) \times K(m, n) \) with \( k_m < m - 1 \) such that, for any commutative ring \( R \), any sequence

\[
P = (p_0, p_1, \ldots, p_N)
\]

of elements from \( R \), and any family of coefficients

\[
c := (c_0, c_1, \ldots, c_m) \in R^{m+1}
\]

with

\[
\sum_{i=0}^{m} c_i p_{i+j} = 0
\]

for all \( j = 0, \ldots, n \), the identity

\[
(14) \quad c_m^n \Delta^{m-1}(h|P) = \Delta^{m-1}(0,1, \ldots, m - 1|P) \sum_{k \in K(m, n)} b_{m,n}(h; k) c^k
\]

holds for all \( h \in H(m - 1, n) \). A straightforward inductive proof of this fact — actually much simpler than the proof of Lemma 4.2 given below — is presented in [2] where, in addition, some abstract general nonsense arguments based on multilinear algebra that can alternatively be used to prove the above Lemma (as well as its ‘partial inverse’ and some further facts that appear to be of some interest in this context) are also presented.
(3) The above lemma appears to have interesting relations to the theory of Schur functions, finite-dimensional representations of $GL_{f+1}$, and/or algebraic geometry (cf. [3]). For instance, it was observed by Joe Harris that, just as the set of geometric progressions $(p_0, \ldots, p_n)$ arising in the case $m = 1$ can be viewed as a rational normal curve in projective space of dimension $n$ satisfying the identities $c^k_0 c^k_{i_1} p_{n_0} = c^k_{i_1} p_{n_0+k}$ for all integers $k_0, k_1, n_0$ with $0 \leq n_0 \leq k = n - k_0$, the set of progressions satisfying a recursion of degree $m > 1$ can be viewed as the $m$-th secant variety of a rational normal curve allowing to interpret the relations between the monomials $c^k$ and the determinants $\Delta_{m-1}(n|P)$ in terms of the associated Plücker and Veronese maps and other fancy stuff.

Proof: We will establish Lemma 4.2 by induction.
First, we put
$$d^i := (\delta_{i0}, \delta_{i1}, \ldots, \delta_{im})$$
for all $i = 0, \ldots, m$, and we define a linear order “$<$” on the set
$$A := \{(k, n) \in K(m, n) \times H(m, n) | n_{m-1} \leq k_m\}$$
by defining $(k, n) < (k', n')$ for any two pairs $(k, n), (k', n') \in A$ if and only if one has $n \preceq n'$ and $n \preceq k'$ defined by
$$n \preceq n' := (n_0, k_0, n_1, k_1, \ldots, n_{m-1}, k_{m-1})$$
and
$$n \preceq k' := (n'_0, k'_0, n'_1, k'_1, \ldots, n'_{m-1}, k'_{m-1})$$
where “$<$” denotes the standard lexicographical order according to which a sequence $(x_0, \ldots, x_b)$ of real numbers is smaller than another such sequence $(x'_0, \ldots, x'_b)$ if and only if there exists some $i \in \{0, \ldots, b\}$ with $x_i < x'_i$ and $x_j = x'_j$ for all $j \in \{0, \ldots, b\}$ with $j < i$. Note that the pair
$$(k, n) = ((0, 0, \ldots, 0, n), (n - m + 1, n - m + 2, \ldots, n))$$
is the only pair $(k, n) = ((k_0, \ldots, k_m), (n_0, \ldots, n_{m-1}))$ with $n - m + 1 \leq n_0$ among all pairs $(k, n) \in A$ because
$$n - m + 1 \leq n_0 \leq n_1 - 1 \leq \cdots \leq n_{m-1} - (m - 1) \leq k_m - (m - 1) \leq n - m + 1$$
implies $n_i = n - m + 1 + i$ for all $i = 0, \ldots, m - 1$ as well as $k_m = n$ and, hence, $k_0 = k_1 = \cdots = k_{m-1} = 0$. So, this pair is also the maximal pair relative to the linear order “$<$” defined on $A$.

Next, we put
$$a((0, 0, \ldots, 0, n), n; h) := \delta_{n, h}$$
for all $n, h \in H(m - 1, n)$ ensuring that the identity
$$c^{(0, 0, \ldots, 0, n)} \Delta_{m-1}(n|P) = c^m \sum_h a((0, 0, \ldots, 0, n), n; h) \Delta_{m-1}(h|P)$$
holds indeed for all such \( n \).

To define \( a(k, n; h) \) also in case \( k \neq (0, 0, \ldots, 0, n) \), that is, in case there is some index \( j \) smaller than \( m \) with \( k_j > 0 \), we define \( \text{sign}(n) \) for any sequence \( n = (n_0, \ldots, n_{m-1}) \) of real numbers by

\[
\text{sign}(n) := 0
\]

if \( \#\{n_0, \ldots, n_{m-1}\} < m \) holds in which case we also put \( n^* := n \), and by

\[
\text{sign}(n) := \text{sign}(\sigma)
\]

for the unique permutation \( \sigma = \sigma_n \) of \( \{0, \ldots, m - 1\} \) with

\[
n_{\sigma(0)} < n_{\sigma(1)} < \ldots < n_{\sigma(m-1)}
\]

in case one has \( \#\{n_0, \ldots, n_{m-1}\} = m \) in which case we put

\[
n^* := (n_{\sigma(0)}, n_{\sigma(1)}, \ldots, n_{\sigma(m-1)}).
\]

Further, we define \( n_{ij} \) by

\[
n_{ij} := (n_0, n_1, \ldots, n_j-1, n_j - j + i, n_{j+1}, \ldots, n_{m-1})
\]

and

\[
\text{sign}(n; ij) := \text{sign}(n_{ij})
\]

for all \( i = 0, \ldots, m \) and \( j = 0, \ldots, m - 1 \).

And we note that (12) — with \( n_j \) replaced by \( n_j - j \) — implies

\[
\sum_{i=0}^{m} c_i \Delta_{m-1}(n_0, \ldots, n_j-1, n_j - j + i, n_{j+1}, \ldots, n_{m-1}|P) = 0
\]

and, hence,

\[
c_j \Delta_{m-1}(n|P) = \sum_{i=0, \ldots, m; i \neq j} -c_i \text{sign}(n; i, j) \Delta_{m-1}(n^*_{ij}|P)
\]
or — multiplying with \( c^k - d^i \) —

\[
(15) \quad c^k \Delta_{m-1}(n|P) = \sum_{i=0, \ldots, m; i \neq j} -c^{k-d^i+d^i} \text{sign}(n; i, j) \Delta_{m-1}(n^*_{ij}|P)
\]

for all \( k \in K(m, n), n \in H(m-1, n), \) and \( j = 0, \ldots, m - 1 \) with \( k_j > 0 \).

This suggests how to define \( a(k, n; h) \) inductively in case \( k \neq (0, 0, \ldots, 0, n) \). In this case, let \( j \) denote the smallest index \( j \) with \( k_j > 0 \) and note that

\[
(k, n) \ll (k - d^j + d^i, n^*_{ij})
\]

18
holds for all $i = 0, \ldots, m-1$ with $i \neq j$ and $\text{sign}(n_{ij}) \neq 0$ because, choosing the integers $k'_0, k'_1, \ldots, k'_{m-1}, k'_m, n'_0, n'_1, \ldots, n'_{m-1}$ so that

$$(k - d^j + d^i, n^*_i) = ((k'_0, k'_1, \ldots, k'_{m-1}, k'_m), (n'_0, n'_1, \ldots, n'_{m-1}))$$

holds and assuming $i < j$, the inequality $n_i - i \leq n_j - j$ implies that either $n_i = n_j - j + i$ and, hence, $\text{sign}(n_{ij}) = 0$ or $n_i < n_j - j + i$ and, hence,

$$n'_0 = n_0, \ k_0 = k'_0, \ n'_1 = n_1, \ k_1 = k'_1, \ldots, n'_{i-1} = n'_{i-1}, \ k_{i-1} = k'_{i-1}$$

as well as

$$n'_i = n_i, \ k'_i = k_i + 1$$

hold while, assuming that $i > j$ and $\text{sign}(n_{ij}) \neq 0$ holds, implies

$$n'_0 = n_0, \ k_0 = k'_0, \ n'_1 = n_1, \ k_1 = k'_1, \ldots, n'_{j-1} = n'_{j-1}, \ k_{j-1} = k'_{j-1}$$

as well as

$$n'_j = \min(n_{j+1}, n_j - j + i) > n_j$$

in case $j < m - 1$, and

$$n'_0 = n_0, \ k_0 = k'_0, \ n'_1 = n_1, \ k_1 = k'_1, \ldots, k_{m-2} = k'_{m-2}$$

as well as

$$n'_{m-1} = n_{m-1} + 1 > n_{m-1}$$

in case $j = m - 1$ (and, hence, $i = m$).

Furthermore, we have

$$n'_{m-1} \leq k'_m$$

(also as required) because we have $n'_m = n_{m-1}$ and $k'_m \geq k_m$ unless we have $n_j - j + i > n_{m-1}$ in which case $i = m$ as well as $n'_m = n_{m-1} + 1 \leq k_m + 1 = k'_m$ must hold in view of $m - 1 \leq n_{m-1} - n_j + j < i$.

Thus, assuming that $a(k', n'; h)$ has been defined already for all $h$ and all pairs $(k', n') \in \mathcal{A}$ with $(k, n) \ll (k', n')$ so that the identity (13) holds for all those pairs $(k', n')$ and putting

$$I_j := \{i \in \{0, \ldots, m\} \mid i \neq j, \text{sign}(n_i; ij) \neq 0\},$$

we can now define $a(k, n; h)$ by

$$(16) \quad a(k, n; h) := \sum_{i \in I_j} -\text{sign}(n_i; ij) \ a(k - d^j + d^i, n^*_i; h)$$

and just use (15) to show that (13) also holds for the pair $(k, n)$.

Thus, our claim now follows indeed by induction.

In what follows, we will only use the following simple consequence of this lemma:
**Corollary 4.3** Given two integers \( m, n \) with \( 0 < m \leq n + 1 \), a sequence \( P = (p_0, p_1, \ldots, p_{m+n}) \) of integers with \( \Delta_{m-1}(0,1,\ldots,m-1|P) \neq 0 \), and a family \( c_0, c_1, \ldots, c_m \) of integers with \( c_m > 0 \), \( \text{gcd}(c_0, c_1, \ldots, c_m) = 1 \), and

\[
\sum_{i=0}^{m} c_i p_{i+j} = 0
\]

for all \( j = 0, \ldots, n \), the \( n-m+1 \)th power \( c_i^{n-m+1} \) of \( c_i \) divides

\[
A(i) = A_{m,n}^{p}(i) := \sum_{h \in H_{m-1,n}} a((n-m+1)d^i + (m-1)d^m, (0,1,\ldots,m-1); h) \Delta_{m-1}(h|P)
\]

for all \( i = 0, \ldots, m \), and we have \( A(i) \neq 0 \) for all \( i = 0, \ldots, m \) with \( c_i \neq 0 \).

In particular, one has

\[
\max \{|c_i| : i = 0, \ldots, m\}^{n-m+1} \leq \binom{n+1}{m} a(m,n) \max \{|\Delta_{m-1}(h|P)| : h \in H(m-1,n)\}
\]

for

\[
a(m,n) := \max \{|a(k,(0,1,\ldots,m-1); h)| : k \in K(m,n), h \in H(m-1,n)\}.
\]

**Proof:** Indeed, the identity

\[
c^k \Delta_{m-1}(n|P) = c^n_m \sum_{h \in H_{m-1,n}} a(k,n; h) \Delta_{m-1}(h|P)
\]

implies that \( c^n_m \) must be a divisor of

\[
c^k \Delta_{m-1}(n|P) = c_0^k \cdots c_{m-1}^k \Delta_{m-1}(n|P)
\]

for all \( k = (k_0, \ldots, k_m) \) with \( \sum_{i=0,\ldots,m} k_i = n \) and all \( n = (n_0, \ldots, n_{m-1}) \) with \( 0 \leq n_0 < n_1 < \ldots < n_{m-1} \leq k_m \). Thus, \( c^{n-k}_m \) must be a divisor of \( \Delta_{m-1}(n|P) \) for all \( n \) as above in view of our assumption \( \text{gcd}(c_0, c_1, \ldots, c_m) = 1 \). In turn, this implies that the product \( c_0^k \cdots c_{m-1}^k \) must be a divisor of \( \sum_{h \in H_{m-1,n}} a(k,n; h) \Delta_{m-1}(h|P) \) for all \( k, n \) as above with \( \Delta_{m-1}(n|P) \neq 0 \) which implies our claim for all \( i = 0, \ldots, m-1 \) by choosing

\[
k := (n-m+1)d^i + (m-1)d^m \text{ and } n := (0,1,\ldots,m-1)
\]

while

\[
c_m^{n-m+1} \mid \sum_{h \in H_{m-1,n}} a((0,\ldots,0,n),(0,1,\ldots,m-1); h) \Delta_{m-1}(h|P)
\]

holds in view of the fact that this sum coincides with \( \Delta_{m-1}(0,1,\ldots,m-1|P) \).

Further, combining Corollary 4.3 in case \( P := P(q,\alpha) \) with Lemma 3.1 yields
Lemma 4.4 If
\[ q \in Q_{ck}(m, n) - Q_{ck}(m - 1, n) \]
holds for some \( q, m, n \in \mathbb{N} \), there exists a unique \((m + 1)\)-tuple
\[ a_0(m, n \mid q), \ldots, c_m(m, n \mid q) \]
of integers with

(i) \( c_m(m, n \mid q) > 0 \),
(ii) \( \gcd(a_0(m, n \mid q), c_1(m, n \mid q), \ldots, c_m(m, n \mid q)) = 1 \),

and

(iii) \( \sum_{i=0}^{m} c_i(m, n \mid q)p_{i+j}(q, \alpha) = 0 \) for all \( j = 0, \ldots, n \)

for which

\[
\max_{i=0, \ldots, m} \left( |c_i(m, n \mid q)| \right) \leq C_{\alpha}(m, n) q F_{\alpha, m+n-1}(q)^{m-1}
\]
and

\[
\left| \sum_{i=0}^{m} c_i(m, n \mid q) \alpha^i \right| (1 + \sum_{i=0}^{m} |c_i(m, n \mid q)|)^{n-m} \\
\leq (m + 2)^{n-m+1} C_{\alpha}(m, n) F_{\alpha, m+n-1}(q)^{m}
\]

holds for
\[ C_{\alpha}(m, n) := \binom{n + 1}{m} a(m, n) m!(1 + |\alpha|)^{m+n-1}. \]

Proof: The existence of a unique \((m + 1)\)-tuple \( a_0(m, n \mid q), \ldots, c_m(m, n \mid q) \) of integers for which (i) to (iii) holds, follows immediately from Section 3. To derive (17) and (18), we put
\[ C_{\alpha}(m, n \mid q) := \max_{i=0, \ldots, m} (|c_i(m, n \mid q)|) \]
for all \( q, m, n \) as above and note first that
\[
C_{\alpha}(m, n \mid q)^{n-m+1} \\
\leq \binom{n + 1}{m} a(m, n) \Delta(m - 1, n; q) \\
\leq \binom{n + 1}{m} a(m, n) m!(1 + |\alpha|)^{m+n-1} q F_{\alpha, m+n-1}(q)^{m-1} \\
= C_{\alpha}(m, n) q F_{\alpha, m+n-1}(q)^{m-1}
\]
holds in view Corollary 4.3 and Lemma 3.1.
In addition, we have

\[
\left| \sum_{i=0}^{m} c_i(m, n \mid q) \alpha^i \right| \leq q^{-1} (m + 1) C_\alpha(m, n \mid q) F_{\alpha, m}(q)
\]

in view of

\[
\sum_{i=0}^{m} c_i(m, n \mid q) q\alpha^i = \sum_{i=0}^{m} c_i(m, n \mid q) (q\alpha^i - p_i(q, \alpha)) = \sum_{i=0}^{m} c_i(m, n \mid q) \beta_i(q, \alpha).
\]

Together, this yields

\[
\left| \sum_{i=0}^{m} c_i(m, n \mid q) \alpha^i \right| \left( 1 + \sum_{i=0}^{m} |c_i(m, n \mid q)| \right)^{n-m} \leq q^{-1} (m + 1) C_\alpha(m, n \mid q) \left( (m + 2) C_\alpha(m, n \mid q) \right)^{n-m} \leq q^{-1} (m + 2)^{n-m+1} C_\alpha(m, n \mid q)^{n-m+1} F_{\alpha, m}(q) \leq (m + 2)^{n-m+1} C_\alpha(m, n) F_{\alpha, m+n-1}(q)^{m-1} F_{\alpha, m}(q) \leq (m + 2)^{n-m+1} C_\alpha(m, n) F_{\alpha, m+n-1}(q)^{m} \]

as claimed.

Our definition of \( m(\alpha) \) (cf. (5)) implies, of course, that

\[
0 < \lim_{n \to \infty} (F_{\alpha, m(\alpha) - 1 + n_0} \mid Q_{\alpha k}(m(\alpha) - 1, n_0))
\]

must hold for some \( n_0 \in \mathbb{N} \). Thus, we must also have

\[
0 < \lim_{n \to \infty} (F_{\alpha, m(\alpha) + n} \mid Q_{\alpha k}(m(\alpha) - 1, n))
\]

for all \( n \in \mathbb{N} \) with \( n \geq n_0 \) in view of the fact that

\[
F_{\alpha, m(\alpha) - 1 + n_0}(q) \leq F_{\alpha, m(\alpha) + n}(q)
\]

as well as

\[
Q_{\alpha k}(m(\alpha), m(\alpha) - 1 + n) \subseteq Q_{\alpha k}(m(\alpha), m(\alpha) - 1 + n_0)
\]

hold for all \( n \geq n_0 \) and \( q \in \mathbb{N} \) which in turn implies that

\[
\lim_{n \to \infty} (F_{\alpha, m(\alpha) + n} \mid Q_{\alpha k}(m(\alpha), n) - Q_{\alpha k}(m(\alpha) - 1, n)) = 0
\]

must hold for all \( n \geq n_0 \).
Further, given any \( q \in Q_{r_k}(m(\alpha), n) - Q_{r_k}(m(\alpha) - 1, n) \), Lemma 4.4 implies that there exists a unique \( m(\alpha) + 1 \)-tuple of integers
\[
c_0 := c_0(m(\alpha), n \, | \, q), \ldots, c_{m(\alpha)} := c_{m(\alpha)}(m(\alpha), n \, | \, q)
\]
with \( c_{m(\alpha)} > 0 \), \( \gcd(c_0, \ldots, c_{m(\alpha)}) = 1 \), and \( \sum_{i=0}^{m(\alpha)} c_i p_i(q, \alpha) = 0 \) for which (18) holds for \( m := m(\alpha) \).

Thus, given any integer \( t \in \mathbb{N} \) for which \( n := t + m(\alpha) \) is sufficiently large, the fact that \( \lim (F_{\alpha, m(\alpha) + n} \mid Q_{r_k}(m(\alpha) - 1, n)) = 0 \) holds (by definition of \( m(\alpha) \)) implies that we can find some sufficiently large \( q \in Q_{r_k}(m(\alpha), n) - Q_{r_k}(m(\alpha) - 1, n) \) with
\[
(m + 2)^{n-m+1} C_{\alpha}(m, n) F_{\alpha, m(\alpha) + n}(q)^{m(\alpha)} \leq 1
\]
implying that
\[
\left| \sum_{i=0}^{m(\alpha)} a_i \alpha^i \right| (1 + \sum_{i=0}^{m(\alpha)} |a_i|)^t \leq 1
\]
as well as \( a_{m(\alpha)} \neq 0 \) hold for the integers \( a_i := c_i(m(\alpha), n \mid q) \), \( i = 0, \ldots, m(\alpha) \).

It follows that \( \alpha \) must be a real number of degree \( \deg(\alpha) \leq m(\alpha) \), and it remains to show that \( \alpha \) is an algebraic number in case \( m(\alpha) - 1 \in \mathcal{L} \mathcal{M}(\alpha) \).

However, this assumption implies that
\[
\lim (q^{1/m(\alpha) - 1} F_{\alpha, m(\alpha) + n - 1}(q) \mid \mathbb{N}) < \infty
\]
and, hence, that also
\[
\lim (q^{1/m(\alpha) - 1} F_{\alpha, m(\alpha) + n - 1}(q) \mid Q_{r_k}(m(\alpha), n)) < \infty
\]
holds for every \( n \in \mathbb{N} \) because every sufficiently large \( q \in \mathbb{N} \) from the infinite set of all \( q \in \mathbb{N} \) with, say,
\[
q^{1/m(\alpha) - 1} F_{\alpha, m(\alpha) + n - 1}(q) \leq \lim (q^{1/m(\alpha) - 1} F_{\alpha, m(\alpha) + n - 1}(q) \mid \mathbb{N}) + 1
\]
must be contained in \( Q_{r_k}(m(\alpha), n) \) in view of Lemma 3.1 as this implies
\[
q^{1/m(\alpha) - 1} F_{\alpha, m(\alpha) + n}(q) = q^{1/m(\alpha)(m(\alpha) - 1)} q^{1/m(\alpha) - 1} F_{\alpha, m(\alpha) + n}(q).
\]

Further, we have
\[
\lim (q^{1/m(\alpha) - 1} F_{\alpha, m(\alpha) + n - 1}(q) \mid Q_{r_k}(m(\alpha) - 1, n)) = \infty
\]
in view of
\[
\lim (q^{1/m(\alpha) - 1} F_{\alpha, m(\alpha) + n - 1}(q) \mid Q_{r_k}(m(\alpha) - 1, n)) =
\]
23
\[
\lim_{q^{1/m(\alpha)}} (q^{1/m(\alpha)} F_{\alpha,m(\alpha)+n-1}(q) | Q_{rk}(m(\alpha) - 1, n)) \quad \text{and} \quad \lim_{q^{1/m(\alpha)}} (q^{1/m(\alpha)} F_{\alpha,m(\alpha)+n-1}(q) | Q_{rk}(m(\alpha) - 1, n)) > 0,
\]

Thus, we must also have
\[
\lim_{q^{1/m(\alpha)}} (q^{1/m(\alpha)-1} F_{\alpha,m(\alpha)+n-1}(q) | Q_{rk}(m(\alpha), n) - Q_{rk}(m(\alpha) - 1, n)) = \lim_{q^{1/m(\alpha)}} (q^{1/m(\alpha)-1} F_{\alpha,m(\alpha)+n-1}(q) | Q_{rk}(m(\alpha), n)) < \infty.
\]

However, this implies
\[
\lim_{q^{1/m(\alpha)}} (Q_{rk}(m(\alpha), n) < \infty
\]

which in turn implies that there must exist some \((m(\alpha) + 1)\)-tuple of integers
\[
a_0, \ldots, a_{m(\alpha)}
\]

with \(a_{m(\alpha)} > 0\) such that
\[
a_0 = c_0(m(\alpha), n, q), a_1 = c_1(m(\alpha), n, q), \ldots, a_{m(\alpha)} = c_{m(\alpha)}(m(\alpha), n, q)
\]

holds for infinitely many \(q \in Q_{rk}(m(\alpha), n) - Q_{rk}(m(\alpha) - 1, n)\). Thus, noting that
\[
\lim_{q \to \infty} \frac{p_i(q | \alpha)}{q} = \lim_{q \to \infty} \frac{|q a_i^i|}{q} = a_i^i
\]

holds for all \(i \in \mathbb{N}_0\), the fact that
\[
\sum_{i=0}^{m(\alpha)} a_i p_i(q | \alpha) = 0
\]

holds for all of those infinitely many \(q\) in \(Q_{rk}(m(\alpha), n) - Q_{rk}(m(\alpha) - 1, n)\) with \(a_i = c_i(m(\alpha), n, q)\) for all \(i = 0, \ldots, m(\alpha)\) readily implies that also
\[
\sum_{i=0}^{m} c_i \alpha_i^i = 0
\]

must hold.

\[\blacksquare\]

**Remarks:**

1. The fact that the degree \(\deg(\alpha)\) of a real number \(\alpha\) coincides with the smallest integer \(m(\alpha) \in \mathbb{N}\) for which \(\lim_{n \to \infty} (F_{\alpha,m(\alpha)+n} | Q_{rk}(m(\alpha), n)) = 0\) holds for all \(n \in \mathbb{N}\) raises the obvious question about what can be said regarding the value of \(\lim_{n \to \infty} (F_{\alpha,\deg(\alpha)-1+n} | Q_{rk}(\deg(\alpha) - 1, n))\). Clearly, the fact that \(0 \leq
\( F_{\alpha,s}(q) \leq 1/2 \) holds for all \( \alpha \in \mathbb{R} \) and \( s, q \in \mathbb{N} \) implies that \( 0 \leq \lim (F_{\alpha,s}|X) \leq 1/2 \) holds for a subset \( X \) of \( \mathbb{N} \) if and only if \( X \) is infinite, and one could speculate that \( Q_{rk}(m,n) \) is finite for all \( m < \deg(\alpha) \) and all sufficiently large \( n \). One may also wonder for which \( \alpha \) and \( m > m(\alpha) \) one has \( \lim (F_{\alpha,m+n}Q_{rk}(m,n) - Q_{rk}(m-1,n)) = 0 \).

(2) There should be \( p \)-adic versions of Theorem 1.2 that might be worthwhile to investigate.

Acknowledgements. Andreas Dress is grateful to the Deutsche Forschungsgemeinschaft for its support. Noam D. Elkies gratefully acknowledges the support of the Packard Foundation. Florian Luca worked on this paper while visiting Bielefeld; he thanks the Forschungsschwerpunkt Mathematisierung and the Graduate College Strukturbildungsprozesse there for their hospitality, and the Alexander von Humboldt Foundation for support.

References


[2] Dress, A.: All Ideals of the Form \((x_0,x_1,\ldots,x_n)\) in the Polynomial Ring \( \mathbb{Z}[x_0,x_1,\ldots,x_n] \) are \( e \)-th Exterior Powers. Manuscript, Bielefeld (2002).


[5] Kronecker, L.: ...


Mathematics Department, Bielefeld University, Postfach 10 01 31, 33 501 Bielefeld, Germany email: dress@mathematik.uni-bielefeld.de

Department of Mathematics, Harvard University, Cambridge, MA 02138, U.S.A. email: elkies@math.harvard.edu

Instituto de Matemáticas de la UNAM, Campus Morelia, Ap. Postal 61-3 (Xangari), CP 58 089 Morelia, Michoacán, México email: fluca@matmor.unam.mx