On Mahler’s classification of transcendental numbers. II: Simultaneous Diophantine approximation

by

A. Baker (Cambridge)

1. Introduction. The class of irrationals with bounded partial quotients has the cardinal of the continuum and hence there exist transcendental numbers \( \theta \) such that all rational approximations \( p/q \) (\( q > 0 \)) satisfy

\[
\left| \theta - \frac{p}{q} \right| > \frac{\sigma}{q^d},
\]

where \( \sigma \) is a positive number. In [1] we investigated the nature of such transcendental numbers and proved a stronger result, namely that there exist \( U \)-numbers with the above property and also there exist either \( T \)-numbers or \( S \)-numbers of arbitrarily high type with this property\(^1\).

In 1954 Davenport [5] proved, for the first time, that there exist continuum-many distinct pairs of irrationals \( \theta, \phi \) such that all rational fractions \( p/q, r/q \) (\( q > 0 \)) satisfy

\[
\max\left( \left| \theta - \frac{p}{q} \right|, \left| \phi - \frac{r}{q} \right| \right) > \frac{\sigma}{q^d},
\]

where \( \sigma \) is a positive constant. Thus there exist pairs of transcendental numbers \( \theta, \phi \) for which (1) holds. It is the purpose of the present paper to investigate the nature of these transcendental numbers and so deduce

\(^1\) We take this opportunity to correct a few misprints and one minor mistake on the last two pages of [1]. On page 119, \( A^K \) on line 15 should be replaced by \( A + A^K, \ldots, A^K \); the formula for \( S \) on line 20 should read \( S = 2d^{K+1}(d-1) \); replace \( s, \lambda K, \mu K, \delta \) occurring on the penultimate line by \( s, \lambda K, \mu K, \delta \); and for \( N > 4 \) on the last line read \( N > 16 \). On page 120 the factor 5 on the first line should be replaced by 4 and \( s, d K \) in the last displayed set of inequalities should read \( s, d K \).
the analogues for pairs $\theta, \phi$ of the results of the previous paper established for a single irrational $\theta$. Accordingly we prove the following

**Theorem.** There exist $U$-numbers $\theta, \phi$ such that (1) holds for all integers $p, q, r, s > 0$, where $c$ is a positive constant. Further, for any $\Theta > 1$, there exist transcendental numbers $\theta, \phi$, each of which is either a $T$-number or an $S$-number of type exceeding $\Theta$, with this property.

Cassels [2] in 1955 proved Davenport's result by a different method and indeed was able to establish a generalization for sets of $n$ irrationals $\theta_1, \theta_2, \ldots, \theta_n$; he showed that there exist continuum-many sets $\theta_1, \theta_2, \ldots, \theta_n$ such that

$$\max \left( \left| \frac{\theta_1 - P_1}{q} \right|, \left| \frac{\theta_2 - P_2}{q} \right|, \ldots, \left| \frac{\theta_n - P_n}{q} \right| \right) > \frac{c}{q^{\Theta^2/\log^2 q}}$$

for all integers $P_1, P_2, \ldots, P_n, q$ ($q > 0$), where $c$ is a positive constant. More recently Davenport [6], [7] (see also Schmidt [8]) has proved these results, and further generalizations, using a much simpler technique, which is itself derived from some earlier work of Cassels (see [3]). This latter method, however, is, in a sense, non-constructive whereas the methods of the original papers of Davenport and Cassels give the required irrationals as limits of certain specified sequences. As far as I can see, of the three available techniques, it is only the principle behind the original construction of Davenport that can be adapted for our purpose, and it is to this that we shall return in the subsequent work.

It is probably that the assertions of the theorem are valid more generally for sets of $n$ irrationals $\theta_1, \theta_2, \ldots, \theta_n$. For $n \geq 3$, however, I have only been able to prove slightly weaker results namely that there exist $U$-numbers $\theta_1, \theta_2, \ldots, \theta_n$ such that

$$\max \left( \left| \frac{\theta_1 - P_1}{q} \right|, \left| \frac{\theta_2 - P_2}{q} \right|, \ldots, \left| \frac{\theta_n - P_n}{q} \right| \right) > \frac{c}{(\log q)^{\Theta^2/\log^2 q}}$$

for all integers $P_1, P_2, \ldots, P_n, q, r > 3$, where $c$ is a positive number depending only on $n$. Further, for any $\Theta > 1$, there exist transcendental numbers $\theta_1, \theta_2, \ldots, \theta_n$, each of which is either a $T$-number or an $S$-number of type exceeding $\Theta$, with this property.

The proofs of these results are long and rather complicated, and we shall not present them here. It suffices to say that the basic ideas are illustrated by the present exposition, but it is necessary to work from first principles with a general algebraic number field rather than the specific cubic fields used in Davenport [5]. Further we remark that just as Davenport's method in the cubic case gives, in some respects, the nearest approach we have to a continued fraction process for a pair of irrationals $\theta, \phi$ so the proof in the higher dimensional case establishes a similar algorithm for $n$ irrationals $\theta_1, \theta_2, \ldots, \theta_n$.

2. The **main construction**. The purpose of this section is to give a brief outline of the construction of Davenport [5], emphasizing, in particular, the explicit definitions of $\theta$ and $\phi$ as limits of certain sequences. These definitions are implied but not stated explicitly in the original paper. We have attempted to retain, as far as possible, the notation of [5] so as to facilitate the reference to established results.

We begin by putting

$$a = 2\cos(2\pi/7), \quad \beta = 2\cos(4\pi/7), \quad \gamma = 2\cos(6\pi/7),$$

$$A = -2\cos(8\pi/9), \quad B = -2\cos(10\pi/9), \quad I' = -2\cos(2\pi/9)$$

so that $\beta, \gamma$ are the conjugates of $a$, and $B, I'$ are the conjugates of $A$ in the totally real cubic fields $k$ and $K$ generated by $a$ and $A$ respectively. Let $l_1, l_2, l_3$ be defined by the matrix equation

$$\begin{pmatrix} A & B & 1 \\ B & I' & 1 \\ B & A & 1 \end{pmatrix} \begin{pmatrix} l_1 \\ l_2 \\ l_3 \end{pmatrix} = \begin{pmatrix} a & \beta & 1 \\ \beta & \gamma & 1 \\ \gamma & a & 1 \end{pmatrix}$$

and let $L_1, L_2, L_3$ be defined similarly with $a, \beta, \gamma$ and $A, B, I'$ interchanged.

We denote by $S$ a sequence of units $e_1, e_2, e_3, e_4, \ldots$ such that each $e_n$ has the form $(a - 1)^n \beta^m$ and each $E_n$ has the form $B^n(B/A)^{2m}$, where $t, s$ are positive integers. Let $e_n$, $E_n$ denote the conjugates of $e_n$ and $E_n$ in $k$ and $K$ respectively, corresponding to the conjugates $a, \beta$ of $a$ and $B, I'$ of $A$. We put

$$\rho_0 = 0, \quad \rho_0 = 1, \quad \rho_0 = 0,$$

$$\rho_0 = 0, \quad \rho_0 = 0, \quad \rho_0 = 1,$$

and then define $\rho_0, \rho_0, \rho_0, \rho_0, \rho_0, \rho_0$ ($n = 1, 2, \ldots$) inductively by the matrix equations

$$\begin{pmatrix} \rho_{n+1} \\ \rho_{n+2} \\ \rho_{n+3} \\ \rho_{n+4} \end{pmatrix} = \begin{pmatrix} l_1 & l_2 & l_3 & l_4 \\ l_2 & l_3 & l_4 & l_5 \\ l_3 & l_4 & l_5 & l_6 \\ l_4 & l_5 & l_6 & l_7 \end{pmatrix} \begin{pmatrix} \rho_n \\ \rho_n \\ \rho_n \\ \rho_n \end{pmatrix}$$

$$\begin{pmatrix} \rho_{n+1} \\ \rho_{n+2} \end{pmatrix} = \begin{pmatrix} l_1 & l_2 & l_3 & l_4 \\ l_2 & l_3 & l_4 & l_5 \\ l_3 & l_4 & l_5 & l_6 \\ l_4 & l_5 & l_6 & l_7 \end{pmatrix} \begin{pmatrix} \rho_n \\ \rho_n \end{pmatrix}$$

(\(n = 1, 2, \ldots\)).

(\(n = 1, 2, \ldots\)).

Although the basic ideas are the same, several difficulties arise in generalizing the work of [5] to higher dimensions and the methods I have used in proving the results for $n > 3$ differ from those of [5] in a number of important respects. As regards the factor $\log q$ in (3), this is caused by the accumulation of constants during the course of application of the algorithm.)
if \( n \) is odd and by the same equations with \( E, L \) in place of \( k, l \) if \( n \) is even. Further let

\[
X_n = \begin{pmatrix}
-1/2 & \gamma_0 + \gamma_1/2 \\
1/2 & \gamma_0 - \gamma_1/2
\end{pmatrix} (\gamma_0^2 + \gamma_1^2)^{-1/2}
\]

if \( n \) is odd and let \( X_n \) be defined similarly if \( n \) is even with \( E \) in place of \( l \).

Since \( \alpha, \beta, 1, A, B, E \) are bases for \( k \) and \( K \) respectively there exist rational integral matrices

\[
\Xi_n = \begin{pmatrix}
P(n) & Q(n) & R(n) \\
P'(n) & Q'(n) & R'(n)
\end{pmatrix} (n = 1, 2, \ldots)
\]

satisfying the equation

\[
(\alpha \beta 1 \gamma_01)^{-1} = (\alpha \beta 1 \gamma_01) X_n
\]

if \( n \) is odd and the same equation if \( n \) is even with \( A, B, E \) in place of \( \alpha, \beta, E \). For each positive integer \( n \) we take \( \Theta(n), \Phi(n) \) to be \( \alpha, \beta \) or \( A, B \) respectively according as \( n \) is odd or even and then define \( \Theta_0, \Phi_0 \) inductively for \( j = n-1, n-2, \ldots, 1, 0 \) by the equations

\[
\Theta(n) = P(n)/P(n), \quad \Phi(n) = P(n)/P(n)
\]

where, for brevity, we have put

\[
W(n) = \begin{pmatrix} W_1 & W_2 \\
W_3 & W_4
\end{pmatrix} = P(n)^{1/2} P(n)^{1/2} + Q(n)^{1/2} Q(n)^{1/2} + R(n)^{1/2} R(n)^{1/2}
\]

The main result of [5] may then be stated as follows.

**Lemma 1.** There are positive numbers \( \delta_1, \delta_2 \) such that if each unit in \( S \) is less than \( \delta_1 \) and, further, the ratio of the conjugates of the units satisfy

\[
|\gamma_{i+1}^{i+1}/\gamma_{i+2}^{i+2} - \zeta| < \delta_1
\]

for all even \( n \) and a similar inequality with \( e \) replaced by \( E \) for all odd \( n \), then the sequences \( \Theta(n), \Phi(n), \Theta_0, \Phi_0 \) (\( n = 1, 2, \ldots \)) converge to limits \( \theta, \phi \) respectively and these satisfy (1) for all integers \( p, q, r, q > 0 \), where \( c \) is a positive constant.

Suppose that \( S \) satisfies the hypotheses of Lemma 1 and for each non-negative integer \( j \) let \( \epsilon_j, \epsilon_0 \) denote the limits of the sequences \( \Theta(n), \Phi(n) \) (\( n = 1, 2, \ldots \)) respectively. Clearly we have \( \theta = \epsilon_0, \phi = \epsilon_0 \) and

\[
\epsilon_j = \eta_j \eta_0, \quad \epsilon_0 = \eta_0 \eta_0,
\]

where

\[
\eta_j = P(n) \eta_0 + \gamma_{i+1}^{i+1} \phi_{j+1}^{j+1} + \zeta
\]

(\( h = 1, 2, 3 \)).

The following results are implied by the work of [5] (see Sections 4 and 6).

**Lemma 2.** Suppose that \( S \) satisfies the hypotheses of Lemma 1 and that \( n \) is a positive odd integer. Then

(i) The elements of \( \Xi_n \) have absolute values at most \( 2^{n-1} \).

(ii) The minors of order \( 2 \) contained in the determinant of \( \Xi_n \) have absolute values at most \( 72^{n-1} \).

(iii) Each \( \eta_{n-1} \) has absolute value at least \( (2n)^{-1} \).

(iv) Each \( \eta_n \) is less than 10.

(v) We have

\[
|\eta_n - \epsilon| < 36n^{2/3}, \quad |\eta_n - \epsilon| < 36n^{2/3}.
\]

The same holds for even \( n \) with \( \alpha, \beta, \epsilon \) replaced by \( A, B, E \) respectively.

**3. Further Lemmas.** Suppose that \( S \) is a sequence of units satisfying the hypotheses of Lemma 1 with \( \delta_1, \delta_2 \) less than a sufficiently small absolute constant. We prove

**Lemma 3.** For each positive even integer \( n \), \( \Theta_0 \) and \( \Phi_0 \) are elements of \( k \) with field heights at most

\[
H_n = \Theta_0(\Xi_n) (E_n \epsilon_{n-1} \ldots E_n \epsilon_1)^{-1/2}
\]

Also we have

\[
\max (|\eta_0 - \Theta_0|, |\phi - \Phi_0|) < \Theta_0(\Xi_n) (E_n \epsilon_{n-1} \ldots E_n \epsilon_1)^{3/4}.
\]

The same holds for odd \( n \) with \( K \) in place of \( k \) and other obvious changes.

**Proof.** We shall prove the assertions of the lemma for \( \Theta_0 \) with \( n \) even. The proofs for \( \Phi_0 \) and for odd \( n \) follow in a similar manner.

It is easily verified by induction, using the equations (3) and (4) of Lemma 2, that \( \Theta_0(n) \) has the form \( U/V \) where

\[
U = U_0 + U_1 \beta + \ldots + U_n \beta^n, \quad V = V_0 + V_1 \beta + \ldots + V_n \beta^n
\]

and the \( U_i, V_i \) are rational integers with absolute values at most

\[
\Theta_0(\Xi_n) (E_n \epsilon_{n-1} \ldots E_n \epsilon_1)^{-1}.
\]

Hence \( \Theta_0 \) is an element of \( K \). Further it is clear that \( \Theta_0 \) satisfies an equation \( W_0 W_1 W_2 = 0 \), where

\[
W_0 = (V_0 - U_0 \Theta_0)^{-1}, \quad W_1 = (V_1 - U_1 \Theta_0)^{-1}, \quad W_2 = (V_2 - U_2 \Theta_0)^{-1}
\]

and \( W_0, W_1, W_2 \) are the factors which result in \( \alpha, \beta, \epsilon \) in \( W_0 \), by their conjugates \( \beta, \gamma, \gamma \), respectively. Here \( W_0 W_1 W_2 \) is a polynomial in \( \Theta_0(n) \) of degree at most 3, with integer coefficients. By virtue of our estimates for the \( U_i, V_i \) given above, and noting that \( |a| < 2, |\beta| < 2 \), it follows that these coefficients have absolute values at most \( H_n \), where \( H_n \) is given by (8), and this proves the first part of the lemma.
For the proof of (7) we again use induction. Our object is to show that for each integer \( j = n, n-1, \ldots, 1, 0 \) we have

\[
\max(|\theta_j - \Phi_j^n|, |\phi_j - \Phi_j^n|) < \delta_j^{(n)} \cdot \delta_j^{(n)}
\]

where \( \delta_j^{(n)} \) is defined in (7) and \( \phi_j, \theta_j \) are given by

\[
\phi_j = \phi_j^n, \quad \theta_j = \theta_j^n
\]

By our inductive hypothesis we see that \( B_1 \) and \( B_2 \) have absolute values at most \( B \), where

\[
B = \delta_j^{(n-k-1)}(\delta_j^{(n-k-1)} B_{n-1} \ldots B_{k+1} B_{k+1})^{\frac{1}{2^k}}
\]

and since \( |\phi_j| < 3, |\theta_j| < 3 \), it follows that \( |B_j| < \delta B_2 \). Now from (ii) of Lemma 2 we deduce that the first factor on the right of (9) has absolute value at most \( (24)^k B_2^{k-1} \). To calculate bounds for the remaining factors we observe first that

\[
\Psi_j^{(n)} = \Psi_j^{(n-k)} \cdot B_j - \Psi_j^{(n-k)} B_j
\]

Hence from (i) and (ii) of Lemma 2, noting that \( B < 1/16 \) provided \( \delta_j, \delta_j \) are sufficiently small, we obtain

\[
|\Psi_j^{(n-k)}| > (2\delta_j)^{k} B_2^{k-1} (4\delta_j)^{k-1} - 1.
\]

From this, (iii) of Lemma 2 and the estimates deduced above we see that the inequality for \( \theta \) implied by (9) is satisfied with \( j = k-1 \). Similarly the inequality for \( \phi \) is satisfied and then (7) follows by induction.

We shall require two further lemmas. The first is deduced by the arguments of Section 11 of [5]. For a simple proof of the second see Cassels [4] p. 286.

**Lemma 4.** All the \( \Theta_j \) and all the \( \Phi_j \) (\( n = 1, 2, \ldots \)) are distinct.

**Lemma 5.** Let \( \alpha, \beta, \gamma, \delta \) be real numbers with \( \alpha \delta - \beta \gamma \neq 0 \). Suppose that \( \alpha \beta \) is irrational. Then to every \( \varepsilon > 0 \) there is an \( \eta = (\alpha \delta - \beta \gamma) \delta \varepsilon \) with the following property. If \( \alpha, \beta \) are integers \( m, n \) such that

\[
|\alpha m + n \beta - \delta| < \varepsilon, \quad \mu < m \eta + n \eta \beta < \mu + \eta.
\]

**4. Proof of Theorem.** We suppose that the numbers \( \delta_1, \delta_2 \) indicated in Lemma 1 are sufficiently small so that Lemmas 3 and 4 will hold for any sequence \( S \) of units provided only that the hypotheses of Lemma 1 are satisfied. We distinguish two cases as in the enunciation of the theorem.

(i) First we prove the existence of a pair of badly approximable \( U \)-numbers. Let \( s < \delta \) be a unit in \( \mathbb{h} \) (*) such that (4) holds with \( n = 0 \). That such a unit exists follows from Lemma 5 on noting that

\[
|\log(\beta - 1)/(\gamma - 1)|, |\log(\gamma - 1)/|\varepsilon| > \log(\beta - 1)/|\varepsilon|
\]

and that the number on the left is a negative irrational \((*)\). We proceed to define the sequence \( S \) inductively. Let \( \lambda \) be a positive even integer and suppose that \( \epsilon_1, \epsilon_2, \epsilon_3, \ldots, \epsilon_{s-1}, \epsilon_s \) have been defined as units in \( \mathbb{h} \) or \( \mathbb{h} \), satisfying the hypotheses of Lemma 1. With \( \lambda \) defined as in Section 2 and \( H_{\lambda} \) given by (6), we take \( \epsilon_{s+1} \) to be a unit in \( \mathbb{h} \) less than \( H_{\lambda}^{-1} \) such that (4) holds with \( n = s \). A similar definition applies for odd \( \lambda \). Then clearly the sequence \( S \) satisfies all the hypotheses of Lemma 1.

The first part of the theorem now follows immediately from Lemmas 1, 3 and 4. For the numbers \( \theta, \phi \) given by Lemma 1 satisfy (1) for all integers \( p, q, r, s \) (\( q > 0 \)), where \( \sigma \) is a positive constant. Further, from (6), (7) and the definition of \( S \) we see that

\[
\max(|\theta - \Phi_j^n|, |\phi - \Phi_j^n|) < H_{\lambda}^{-n}
\]

for sufficiently large \( n \). This implies that \( \theta, \phi \) are \( U \)-numbers with degree at most 3 and hence also \( U \)-numbers \((*)\).

(i) The proof of the second part of the theorem proceeds similarly but there is less range in which to choose the successive terms of the sequence \( S \). Let \( \eta \) be the constant given by Lemma 5 corresponding to the five numbers

\[
4 \log(\beta - 1)/(\gamma - 1), \quad 4 \log(\gamma - 1)/|\varepsilon|, \quad -2 \log(\alpha - 1)/|\varepsilon|, \quad -2 \log(\beta)/|\varepsilon|, \quad \delta_{\lambda}^{(n)}.
\]

For each positive even integer \( \lambda \) we now choose \( \epsilon_{s+1} \) to be a unit in \( \mathbb{h} \) satisfying (4) with \( n = \lambda \) such that

\[
e^r < \epsilon_{s+1}/H_{\lambda}^{-n} < 1.
\]

That such a unit exists follows by applying Lemma 5 with \( \lambda = \log(\beta)/\mu = 3\log(\alpha)/\mu \) and noting also (iv) of Lemma 2. Again a similar definition applies for odd \( \lambda \).

(*) It is understood that all units \( \epsilon \) or \( H \) have the form indicated in Section 2.

(**) We require that \( \delta_{\lambda} \) has the form \( (\alpha - 1)/\beta \mu \) where \( \alpha, \beta \) are positive integers.

On applying Lemma 5 the signs of \( \alpha \) and \( \beta \) are undetermined. However \( \alpha \) can certainly be taken as positive and it then follows that \( \epsilon \) is positive provided \( \delta_{\lambda} \) is sufficiently small. We suppose that \( \delta_{\lambda} \) is so chosen in the subsequent work.

(3) See Schneider [9], Satz 21, p. 73.
It remains only to prove that each of the numbers $\delta, \phi$ given by Lemma 1 is either a $T$-number or an $S$-number of type exceeding $S$. From Lemma 3 we obtain
\[
\max(\|\delta - \Theta_0^m\|, \|\phi - \Theta_0^m\|) < \Theta^{(m+1)\beta + 1/\beta},
\]
and it follows that $\delta, \phi$ cannot be $S$-numbers of type $\leq \Theta(t)$. Finally we appeal to Theorem 1 of [1]. From Lemma 4 and the inequality
\[
H_{A+1} < H_{n+1}^{2\gamma^2}(\gamma)^{\delta + 1/\beta},
\]
it follows that all the hypotheses of Theorem 1 are satisfied with $\alpha_1 = \Theta_0^m$, or $\alpha_2 = \Theta_0^m$, provided $j$ is sufficiently large (and similarly with the superscript $2j+1$ in place of $2j$), and hence $\delta, \phi$ are neither algebraic nor $U$-numbers. This completes the proof of the theorem.

---

(6) See Schneider [9], Satz 22, p. 82. Again we are assuming $\delta, \phi$ sufficiently small so that $H_4^{(m)} > \Theta^{(m+1)}$ if $n$ is sufficiently large.

References


Oeuvre de la Réunion de t. 4, 1958

On a conjecture of Davenport and Lewis concerning exceptional polynomials

by

C. R. MacIntyre (Ann Arbor, Mich.)

1. Exceptional polynomials over arbitrary fields. Let $K$ be an arbitrary field. A polynomial $f(x)$ in $K[x]$ is said to be exceptional over $K$ if the polynomial $\Phi(x, y) = (f(x) - f(y))/(x^a - y)$ has no absolutely irreducible factors in $K[x, y]$.

In the investigation into the average error term of the number of solutions of congruence relations, Davenport and Lewis [1] were led to propose the following conjecture:

**The Davenport-Lewis Conjecture.** For $f(x)$ in $Z[x]$ and for all large primes $p$, if $f(x)$ is exceptional over $Z_p$, then the map

\[
f: Z_p \rightarrow Z_p
\]

is one-to-one and onto.

The object of this note is to show that the Davenport-Lewis Conjecture is indeed correct. In fact,

**Theorem 1.** Let $K$ be an arbitrary field and let $f(x)$ be a polynomial in the ring $K[x]$ of degree $n$. Suppose $\text{char} K = 0$ or $n < \text{char} K$. If $f(x)$ is exceptional over $K$, then $f(x)$ is a one-to-one map of $K$ into $K$.

The proof of Theorem 1 will follow some necessary observations concerning the splitting fields of polynomials in two variables and some remarks on pure equations.

For the remainder of this note let $K$ be an arbitrary field and let $A$ be the algebraic closure of $K$.

**Definition 1.** If $a(x, y)$ in $K[x, y]$ is of the form

\[
a(x, y) = ax^n + P_1(y)x^{n-1} + \ldots + P_n(y)
\]

where each $P_i(y)$ is in $K[y]$ and where $a$ is a non-zero element of $K$, then $a(x, y)$ is said to be regular in $x$. If, in addition, $a = 1$, then $a(x, y)$ is said to be monic in $x$.

* Research was sponsored by the National Science Foundation, Ann Arbor, Michigan, U. S. A.

Acta Arithmetica XII (1967)