Dirichlet's diophantine
approximation theorem

T.W. Cusick

One form of Dirichlet's theorem on simultaneous diophantine approximation asserts that if α_1, α_2, ..., α_n are any real numbers and $m \geq 2$ is an integer, then there exist integers q, p_1, p_2, ..., p_n such that $1 \leq q < m$ and $|q\alpha_i - p_i| \leq m^{-1/n}$ holds for $1 \leq i \leq n$. The paper considers the problem of the extent to which this theorem can be improved by replacing $m^{-1/n}$ by a smaller number. A general solution to this problem is given. It is also shown that a recent result of Kurt Mahler [*Bull. Austral. Math. Soc.* 14 (1976), 463-465] amounts to a solution of the case $n = 1$ of the above problem. A related conjecture of Mahler is proved.

For any real number x, let $\|x\|$ denote the distance from x to the nearest integer; thus $\frac{1}{2} \geq \|x\| \geq 0$ for all x. The well-known theorem of Dirichlet concerning simultaneous diophantine approximation can be stated as follows: if α_1, α_2, ..., α_n are any real numbers and $m \geq 2$ is an integer, then there exists an integer q such that

(1) $1 \leq q < m$ and $\|q\alpha_i\| \leq m^{-1/n}$ $(1 \leq i \leq n)$.

It is natural to ask whether the result given in (1) can be improved, and if so to what extent. In this paper we consider this question from the following point of view: define the function $f(m, n)$ for integers $m \geq 2$

and $n \geq 1$ by

$$f(m, n) = \sup_{} \min_{1 \leq q < m} \max_{1 \leq i \leq n} \|q\alpha_i\| \ ,$$

where the supremum is taken over all n-tuples of real numbers
$\alpha_1, \ldots, \alpha_n$. Thus (1) can be restated as

(2) $f(m, n) \leq m^{-1/n}$,

and (1) is improved for any pair m, n for which we can prove that strict
inequality holds in (2). We prove below that for fixed n the upper bound
$m^{-1/n}$ in (2) cannot be decreased by more than $2(n-1)m^{-2/n}$ for any m ,
and that for infinitely many m equality holds in (2). Thus (1) can never
be improved by very much, and infinitely often (1) actually gives the best
possible result of its type.

    There is another way of looking at the question of improving (1). For
any n-tuple of real numbers $\alpha_1, \ldots, \alpha_n$, define

$$c(\alpha_1, \ldots, \alpha_n) = \limsup_{m \to \infty} \min_{1 \leq q < m} \max_{1 \leq i \leq n} m^{1/n} \|q\alpha_i\| \ .$$

Thus (1) says that $c(\alpha_1, \ldots, \alpha_n) \leq 1$ for all real numbers $\alpha_1, \ldots, \alpha_n$,
and (1) is improved for any n-tuple $\alpha_1, \ldots, \alpha_n$ for which we can prove
that $c(\alpha_1, \ldots, \alpha_n) < 1$. Davenport and Schmidt [2] proved that for almost
all (in the sense of Lebesgue measure) n-tuples $\alpha_1, \ldots, \alpha_n$, we have
$c(\alpha_1, \ldots, \alpha_n) = 1$. Thus, from this point of view, no improvement of (1)
is possible except on a set of zero measure. Some results on the nature of
the n-tuples that are in this set of zero measure were proved in an
earlier paper of Davenport and Schmidt [1].

    THEOREM 1. *For any given integers $m \geq 2$ and $n \geq 1$, let k be
an arbitrary integer such that $k^n + k^{n-1} - k \leq m$ holds. Then*

(3) $k^{n-1}m^{-1} \leq f(m, n) \leq m^{-1/n}$

holds.

    Proof. We already have the right-hand inequality in (3). To prove
the left-hand inequality, we suppose $m \geq 2$ and $n \geq 1$ are given, and we

define

(4) $\alpha_j = k^{j-1}m^{-1} \quad (1 \le j \le n)$.

Now we have

(5) $k^{n-1}m^{-1} \le im^{-1} \le 1 - k^{n-1}m^{-1}$ for $k^{n-1} \le i \le m - k^{n-1}$.

If $m \ge k^n + k^{n-1} - k$ (true by the hypothesis of the theorem), then

(6) $k^{n-1}m^{-1} \le ikm^{-1} \le 1 - k^{n-1}m^{-1}$ for $k^{n-2} \le i \le k^{n-1} - 1$.

Similarly, for $2 \le r \le n-1$, if $m \ge k^n + k^{n-1} - k^r$ (true by the hypothesis of the theorem), then

(7) $k^{n-1}m^{-1} \le ik^r_m{}^{-1} \le 1 - k^{n-1}m^{-1}$ for $k^{n-r-1} \le i \le k^{n-r} - 1$.

Since for any integer a satisfying $1 \le a \le m-1$ we have $\|(m-a)\alpha_j\| = \|a\alpha_j\|$ for each α_j defined in (4), putting together (5), (6), and (7) with $r = 2, 3, \ldots, n-1$ gives

$$\min_{1 \le q < m} \max_{1 \le i \le n} \|q\alpha_i\| \ge k^{n-1}m^{-1} .$$

This proves $f(m, n) \ge k^{n-1}m^{-1}$.

COROLLARY 1. *For each* $m \ge 2$, *we have* $f(m, 1) = m^{-1}$.

This corollary is the theorem given by Mahler in [3]. Mahler stated the result in the more general form

$$\sup_\alpha \inf_s \|s\alpha\| = m^{-1} ,$$

where the supremum is taken over all real α and the infimum is taken over all s in any set S (finite or infinite) of positive integers which contains $1, 2, \ldots, m-1$ but not im for $i = 1, 2, \ldots$. However, as Mahler points out, it is easily seen that the more general result follows from the special case in which $S = \{1, 2, \ldots, m-1\}$.

COROLLARY 2. *For each* $m \ge 2$, *we have* $f(m, 2) > m^{-\frac{1}{2}} - m^{-1}$ *and* $f(m, n) > m^{-1/n} - 2(n-1)m^{-2/n}$ $(n \ge 3)$.

Proof. Theorem 1 gives $f(m, 2) \geq km^{-1}$ with k satisfying

$k^2 \leq m < (k+1)^2$; that is, $m^{\frac{1}{2}} - 1 < k \leq m^{\frac{1}{2}}$. This gives the first part

of the corollary. Similarly, for $n \geq 3$, the theorem gives

$f(m, n) \geq k^{n-1}m^{-1}$ with k satisfying

$$k^n + k^{n-1} - k \leq m < (k+1)^n + (k+1)^{n-1} - k - 1 .$$

This last inequality implies $m < (k+2)^n$; thus $k > m^{1/n} - 2$, which

implies $k^{n-1}m^{-1} > m^{-1/n} - 2(n-1)m^{-2/n}$. This gives the second part of the

corollary.

Our next theorem shows that the lower bound in (3) can sometimes be improved.

THEOREM 2. *For any given integers* $m \geq 2$ *and* $n \geq 1$, *if* t *is an*

integer satisfying $m \leq t^n$, *then*

(8) $t^{-1} \leq f(m, n)$.

In particular, for each $t \geq 2$ *we have*

(9) $t^{-1} = f(t^n, n)$.

Proof. Suppose $m \geq 2$, $n \geq 1$, and t satisfying $m \leq t^n$ are

given, and define

$$\alpha_j = t^{-j} (1 \leq j \leq n) .$$

Now $\|q\alpha_1\| \geq t^{-1}$ if $q \not\equiv 0 \bmod t$, and for $j = 2, 3, \ldots, n$,

$\|q\alpha_j\| \geq t^{-1}$ if $q \equiv 0 \bmod t^{j-1}$ but $q \not\equiv 0 \bmod t^j$. Hence for $m \leq t^n$ we

have $\min_{1 \leq q < m} \max_{1 \leq i \leq n} \|q\alpha_i\| \geq t^{-1}$, which proves (8). For $m = t^n$, (9)

follows from (8) and (2). Thus (9) shows that for each n , (2) holds with

equality for infinitely many values of m .

Our last theorem proves a conjecture of Mahler [3], which is an

extension of the case $n = 1$ of Theorem 1.

THEOREM 3. *For any given positive integers* m, n *such that* $2m \leq n$,

we have

$$(10) \qquad\qquad \sup_{\alpha} \ \min_{m \le q \le n-m} \ \|q\alpha\| = mn^{-1} \ ,$$

where the supremum is taken over all real α .

  Proof. The proof is a variation of the "box principle" argument which can be used to prove Dirichlet's theorem. The left-hand side of (10) is clearly greater than or equal to mn^{-1} $\left(\text{take} \ \alpha = n^{-1}\right)$, so we need only prove that the left-hand side of (10) is less than or equal to mn^{-1} . We divide the interval $[0, 1)$ into the n boxes $\left[in^{-1}, (i+1)n^{-1}\right)$ $(0 \le i \le n\text{-}1)$, and we say that the $2m$ boxes containing those x such that $\|x\| \le mn^{-1}$ are "special" boxes. Now take any real α and consider the $n - 2m + 1$ points $j\alpha$ $(m \le j \le n\text{-}m)$ mod 1 . If one of these points is in one of the special boxes, we are finished. If not, then one of the $n - 2m$ nonspecial boxes contains at least two of these points, say $j\alpha$ and $k\alpha$, $j < k$. We then have $\|(k\text{-}j)\alpha\| \le n^{-1}$ with $1 \le k - j \le n - 2m$. If in fact $m \le k\text{-}j$, we are finished. If not, we choose an integer a satisfying $m \le a(k\text{-}j) \le n\text{-}m$ and $1 < a \le m$. This is possible since $(n\text{-}m)(k\text{-}j)^{-1} - m(k\text{-}j)^{-1} \ge 1$. Now $\|(k\text{-}j)\alpha\| \le n^{-1}$ implies $\|a(k\text{-}j)\alpha\| \le an^{-1} \le mn^{-1}$, which proves (10).

  Mahler [3] stated his conjecture in the more general form

$$\sup_{\alpha} \inf_{s} \ \|s\alpha\| = mn^{-1} \ ,$$

where the supremum is taken over all real α and the infimum is taken over all s in any set S (finite or infinite) of positive integers which contains $m, m+1, \ldots, n\text{-}m$ and has the property that every element s of S satisfies $\|sn^{-1}\| \ge mn^{-1}$. But this more general result follows from the proof of Theorem 3.

References

[1]   H. Davenport and Wolfgang M. Schmidt, "Dirichlet's theorem on
        diophantine approximation", *Symposia Mathematica*, Volume IV:
        Teoria dei numeri, 113-132 (INDAM, Roma, 1968/1969.   Academic
        Press, London and New York, 1970).

[2]   H. Davenport and W.M. Schmidt, "Dirichlet's theorem on diophantine
        approximation.   II", *Acta Arith.* 16 (1969/70), 413-424.

[3]   Kurt Mahler, "A theorem on diophantine approximations", *Bull. Austral.*
        Math. Soc. 14 (1976), 463-465.

Department of Mathematics,
State University of New York at Buffalo,
Amherst,
New York,
USA.