

DISTANCE TO THE NEAREST INTEGER AND ALGEBRAIC INDEPENDENCE OF CERTAIN REAL NUMBERS¹

AVIEZRI S. FRAENKEL

1. Introduction and results. The problem is examined of how close $\alpha p/q$ lies to an integer for an infinity of rational numbers p/q from a certain class, and, in particular, of how this proximity depends on the real constant α . It turns out, roughly speaking, that $\alpha p/q$ is not too close to an integer for most α . There exists, however, an uncountable set of α for which $\alpha p/q$ is very close to an integer for an infinity of p/q . Certain subsets of this set can be constructed effectively. Some of these subsets consist of algebraically independent numbers which have the power of the continuum.

More specifically, let $\|x\|$ denote the distance of x to the nearest integer. Let $\{P_1, \dots, P_s\}$, $\{Q_1, \dots, Q_t\}$ be finite sets of primes and let $c \geq 1$, $0 \leq \mu \leq 1$. Let

$$(1) \quad p = p^* p', \quad p' = P_1^{\rho_1} \cdots P_s^{\rho_s}, \quad q = Q_1^{\sigma_1} \cdots Q_t^{\sigma_t},$$

where $\rho_1, \dots, \rho_s, \sigma_1, \dots, \sigma_t$ are non-negative integers, and p^* is any integer satisfying

$$(2) \quad 0 < p^* \leq c p^\mu. {}^2$$

THEOREM I. *Let $\delta > 0$, $0 \leq \mu \leq 1$, $a > 0$, α real algebraic. Then the inequality $0 < \|\alpha p/q\| < q^{-(\mu+\delta)}$ holds only for a finite number of p, q of the above form with $p \geq aq$, provided that $q=1$ if $\mu=1$. In addition, for almost all real r -tuples $(\alpha_1, \dots, \alpha_r)$, $r \geq 1$, the set of inequalities*

$$(3) \quad 0 < \|\alpha_i p/q\| < p^{-(\mu/r+\delta)}, \quad i = 1, \dots, r,$$

has only a finite number of solutions in p, q of the above form with $p \geq aq$, provided that $q=1$ if $\mu=1$.

Presented to the Society, January 25, 1962, under the title *Distance to nearest integer of powers of rational numbers*; received by the editors November 13, 1961 and, in revised form, August 2, 1963.

¹ Part of this work was done while the author was at the University of Oregon.

² Since $p = p^* p'$, this inequality is equivalent to $0 < p^* \leq c^{1/(1-\mu)} (p')^{\mu/(1-\mu)}$ for $0 \leq \mu < 1$. For $\mu=1$ it becomes vacuous, i.e., p^* is unrestricted.

THEOREM II. *Let $\alpha_1, \dots, \alpha_r$ be any real numbers, $0 \leq \mu \leq 1$, $K > 0$ arbitrary if $0 \leq \mu < 1$ and $K = 1$ if $\mu = 1$. Let p', q be any integers of the form (1), with the condition that $p' = 1$ if $\mu = 1$. There exists a constant $c > 1$ depending only on r, K, μ , the α_i and the primes $P_1, \dots, P_s, Q_1, \dots, Q_t$, and an integer $p = p^* p'$ such that*

$$(4) \quad \|\alpha_i p/q\| < K p^{-\mu/r}, \quad i = 1, \dots, r,$$

where $0 < p^* \leq c p^\mu$. Thus (4) has an infinity of solutions in p, q of the form (1) subject to (2), where p', q are arbitrarily prescribed integers of the form (1) subject to the condition $p' = 1$ if $\mu = 1$.

Let $\eta > 0, a > 0$. For almost all real r -tuples $(\alpha_1, \dots, \alpha_r)$, all but a finite number of the $p \geq aq$, for which (4) holds, satisfy $p^* > p^{\mu-\eta}$.

The case $\mu = 0$ of the first part of Theorem I is equivalent to a Theorem of Mahler [6, Theorem 1, p. 151], [5]. The conditions $p \geq aq$ in Theorems I and II are necessary. Thus, for $s = t = 1, P = 2, Q = 5, p^* = 1$, and for every $0 < \delta < \log_2 5 - 2, 0 \leq \mu \leq 1, 0 < \alpha < 1$, we can write $0 < \|\alpha p/q\| = \|\alpha(2/5)^n\| < 2^{-n(\mu+\delta)} < 2^{-n\mu}$ for all $n \geq 1$. The first part of Theorem II shows that Theorem I is best possible. The second part shows that the leeway for p^* indicated by (2) is not usually realized, i.e., the p^* satisfying (4), for which $p \geq aq$, are usually close to their upper bound.

Let P be a prime, $c_0 > 1$. For any μ in $[0, 1)$, let $\{p_1^*, p_2^*, \dots\}$ be a sequence of integers such that for some index $N = N(\mu), p_N^* = r_N, p_i^* = r_i r_{i-1} \dots r_N, i > N$, where the r_i are positive integers not divisible by $P, p_i^* \leq p_i \leq c_0 p_i^*, p_i = p_i^* p_i', i \geq N$, and $p_i^* = 1$ for $1 \leq i < N$. We are interested in these sequences for $p_i' = P^{i!}$ and $p_i' = P^{2^i}$, and denote the sequences by S_μ and T_μ for these two cases, respectively. Further, let $U = \{p_1^*, p_2^*, \dots\}$ be a sequence of integers such that $p_1^* = r_1, p_i^* = r_i r_{i-1} \dots r_1, i \geq 1$, where the r_i are positive integers not divisible by $P, P^{2^i} < p_i^* < P^{2^{i+1}}$. It is easily seen that such sequences exist. In fact, we can take $S_0 = T_0 = \{1, 1, \dots\}$; if $\mu > 0$, it suffices if N is sufficiently large to satisfy $(p_N^*)^{\mu/(1-\mu)}(1 - c_0^{-1/(1-\mu)}) > 2$ for both S_μ and T_μ . For $\mu > 0$ it can even be arranged that all $r_i (i > N)$ in S_μ and T_μ be distinct primes $\neq P$. In this case N must, in addition, be so large that the interval

$$\left((p_i')^{\mu/(1-\mu)} (p_{i-1}^*)^{-1} c_0^{-1/(1-\mu)} (p_i')^{\mu/(1-\mu)} (p_{i-1}^*)^{-1} \right)$$

contains a prime $> P$ for all $i \geq N$, and that these intervals be disjoint for all $i \geq N$. Using these sequences, a real number can be constructed for which (3) has an infinity of solutions in integers p, q of the form (1) subject to (2). But first we show that there are not too many such numbers.

THEOREM III. Let $\delta > 0, a > 0$. For fixed $0 \leq \mu \leq 1$, let $R(\mu)$ be the set of all real r -tuples $(\alpha_1, \dots, \alpha_r)$ for which (3) has an infinity of solutions in p, q of the form (1) subject to (2) with $p \geq aq$. Let $R = \bigcup_{0 \leq \mu \leq 1} R(\mu)$. Then R has measure 0.

THEOREM IV. Let $0 < \delta < 1 - \mu, c > 1$. For each $0 \leq \mu < 1$ there exists an everywhere dense subset of Liouville numbers α for which $\|\alpha p/q\| < p^{-(\mu+\delta)}$ has an infinity of solutions in p, q of the form (1) subject to

$$(5) \quad p^\mu \leq p^* \leq cp^\mu,$$

with $q \rightarrow \infty$. For $q = 1$ there are Liouville numbers $\alpha_k = \sum_{i=1}^{\infty} (p_{ik}^* P^{(ik)!})^{-1}$, $p_{ik}^* \in S_\mu, k = 1, \dots, r, 0 \leq \mu < 1$ and non-Liouville transcendental numbers $\alpha_k = \sum_{i=1}^{\infty} (p_{ik}^* P^{2^{ik}})^{-1}$, $p_{ik}^* \in T_\mu, k = 1, \dots, r, 0 \leq \mu < 1$, which satisfy $\|\alpha_k p\| < p^{-(\mu/r+\delta)}, k = 1, \dots, r$ for an infinity of p of the form (1) subject to (5).

THEOREM V. Let $0 \leq \mu < 1, \delta > 0$. Each of the following four sets is algebraically independent over the rationals and, for any number ξ of these sets, $\|\xi p\| < p^{-(\mu+\delta)}$ for an infinity of p of the form (1) subject to (5):

1. The Liouville numbers $\alpha_k, k = 1, 2, \dots$, defined in Theorem IV.

$$2. \quad \beta_k = \sum_{i=1}^{\infty} (p_{ik}^* P^{k(i!)})^{-1}, \quad p_{ik}^* \in S_{1/2}, \quad k = 1, 2, \dots$$

$$3. \quad \alpha(x) = \sum_{i=1}^{\infty} p(x, i)^{-1} = \sum_{i=1}^{\infty} (p^*(x, i) P^{[i^{i+x}]})^{-1}, \quad p^*(x, i) \in U, \\ p(x, i)^x \leq p^*(x, i) \leq P^4 p(x, i)^x, \quad 0 < x < 1.$$

$$4. \quad \beta(x, y) = \sum_{i=1}^{\infty} p(x, y, i)^{-1} = \sum_{i=1}^{\infty} (p^*(x, y, i) P^{[i^{(i+x)^{i+y}}]})^{-1}, \\ p^*(x, y, i) \in U, \quad p(x, y, i)^x \leq p^*(x, y, i) \leq P^4 p(x, y, i)^x, \\ 0 < x < 1, \quad 0 < y < 1.$$

From Theorem IV there follows, in particular, that for each α for which (3) (with $r = 1$) has only a finite number of solutions, there exists a sequence $\{\beta\}$ of real numbers converging to α , such that (3) has an infinity of solutions p, q of the specified form for every $\delta > 0$ if α is replaced by β .

The sequence $\{\alpha_k\}$ considered in Theorem V constitutes an independent set for each (fixed) μ in $[0, 1)$. The case $\mu = 0$ is the case usually considered [3], [4], [7], [9]. On the other hand, μ is not fixed in the sequence $\{\beta_k\}$. The number β_k is associated with the value $\mu = (1+k)^{-1}$. Indeed, $p_{ik}^* \in S_{1/2}$ implies $P^{(ik)!} \leq p_{ik}^* \leq c_0^2 P^{(ik)!}$. Choosing c_0 to satisfy $1 < c_0^2 \leq c$ and letting $\mu = (1+k)^{-1}$, we have $P^{k(i!)^{1/(1-\mu)}}$

$\leq p_{ik}^* \leq c^{1/(1-\mu)} P^{k(i\delta)1\mu/(1-\mu)}$, which is equivalent to (5). The numbers $\alpha(x)$ and $\beta(x, y)$ each form a set with the power of the continuum. For fixed y , the numbers $\beta(x, y)$, form a subset with the power of the continuum, each number of which corresponds to some value $\mu=x$ in $(0, 1)$. For fixed x they also form a subset with the power of the continuum.

2. Proofs. We require a Theorem of Ridout [8]: *Let α be algebraic $\neq 0$. Let $\{P_1, \dots, P_s\}, \{Q_1, \dots, Q_t\}$ be finite sets of primes, μ, ν, δ, c real numbers satisfying $0 \leq \mu \leq 1, 0 \leq \nu \leq 1, \delta > 0, c \geq 1$. Let p, q be restricted to integers of the form*

$$\begin{aligned} p &= p^* p', & q &= q^* q', \\ p' &= P_1^{\rho_1} \dots P_s^{\rho_s}, & q' &= Q_1^{\sigma_1} \dots Q_t^{\sigma_t}, \end{aligned}$$

where $\rho_1, \dots, \rho_s, \sigma_1, \dots, \sigma_t$ are non-negative integers, and p^*, q^* are any integers satisfying $|p^*| \leq c|p|^\mu, 0 < q^* \leq cq^\nu$. Then the inequality

$$0 < |\alpha - p/q| < q^{-(\mu+\nu+\delta)}$$

has only a finite number of solutions in p, q of the above form.

PROOF OF THEOREM I. Suppose that for some $0 \leq \mu \leq 1, \delta > 0$, there exists an r -tuple $(\alpha_1, \dots, \alpha_r)$ for which (3) has an infinity of solutions of the specified form with $p \geq aq$. Without loss of generality we may assume that α_i is positive, $i=1, \dots, r$. With each solution associate a value $\theta = \theta(p)$ defined by $p^* = p^\theta \leq cp^\mu$. The infinite sequence $\{\theta(p)\}$ lies in $[0, \mu]$. Let $\zeta = \limsup (\theta(p))$ (as $p \rightarrow \infty$). Then for every $\epsilon > 0$ there exists an infinity of p, q of the form (1) subject to

$$(6) \quad p^{\zeta-\epsilon} < p^* \leq p^\zeta,$$

satisfying (3). For each of these solutions define $\lambda = \lambda(p)$ by $(p')^{1-\lambda} = q^{1-\zeta}$, where we let $\lambda = 1$ if $p' = 1$. Thus $\lambda \leq 1$. Let $\nu = \limsup (\lambda(p))$ (as $p \rightarrow \infty$). Then $\nu = 1$ if $\zeta = 1$. If $\zeta < 1$,

$$(p')^{(1-\lambda)/(1-\zeta)} = q \leq a^{-1}p \leq a^{-1}(p')^{1/(1-\zeta)}$$

by the right-hand side of (6). Hence $(p')^\lambda \geq a^{1-\zeta}$, and for any $\eta > 0, \lambda > -\eta$ for all sufficiently large p' . Hence $0 \leq \nu \leq 1$, and there exists an infinity of p, q of the form (1) subject to (6) and

$$(7) \quad (p')^{1-\nu} \leq q^{1-\zeta} < (p')^{1-\nu+\epsilon},$$

satisfying $0 < |\alpha_i p/q - u_i| < p^{-(\zeta/r+\delta)}, i=1, \dots, r$, where u_i is the nearest integer to $\alpha_i p/q$.

Let $l_i = u_i q$. If $\nu < 1$ (and hence $\zeta < 1$), then $u_i < \alpha_i p q^{-1} + 1 \leq \alpha_i (p')^{1/(1-\zeta)} q^{-1} + 1 \leq \alpha_i q^{\nu/(1-\zeta)} + 1 \leq c_1 q^{\nu/(1-\zeta)}$, by the right-hand side of

(6) and the left-hand side of (7), where $c_1 = 1 + \max_i \alpha_i > 1$. Hence $u_i < c_2 l_i^\nu, c_2 > 1$. But this clearly holds also if $\nu = 1$. Now,

$$0 < |\alpha_i - l_i/p| < \frac{1}{p^{\zeta/r + \nu + \delta}} \cdot \frac{q}{p^{1-\nu}}, \quad i = 1, \dots, r,$$

infinitely often. But if $\zeta < 1$, then

$$q < (p')^{(1-\nu+\epsilon)/(1-\zeta)} < p^{(1-\zeta+\epsilon)(1-\nu+\epsilon)/(1-\zeta)} = p^{1-\nu+\eta}$$

by the right-hand side of (7) and the left-hand side of (6), where $\eta > 0$ is arbitrarily small with ϵ . If $\zeta = 1$, then $\mu = \nu = 1$ and $q = 1 = p^{1-\nu}$. In either case, the inequality

$$0 < |\alpha_i - l_i/p| < p^{-(\zeta/r + \nu + \delta - \eta)}$$

has an infinity of solutions in l_i, p of the specified type. Hence by Ridout's Theorem, with μ replaced by ν, ν replaced by ζ, δ by $\delta - \eta > 0, c$ by c_2, p by l and q by p, α must be transcendental if $r = 1$. Since for $r \geq 1$ Ridout's Theorem is true for almost all real r -tuples [1, Theorem II, p. 85], $(\alpha_1, \dots, \alpha_r)$ must in fact belong to a set of measure 0.³

PROOF OF THEOREM II. Assume first $0 \leq \mu < 1$. Let $k \geq 1, p', q$ any integers of the form (1), $A = [2k(p')^{\mu/r(1-\mu)}]$. As in [1, Lemma 4, pp. 92-93], divide the r -dimensional unit cube into A^r boxes, and apply Dirichlet's box principle to conclude existence of x_1, x_2 with $0 \leq x_1 < x_2 \leq A^r$ satisfying

$$|(x_2 - x_1)\alpha_i p'/q - ([x_2 \alpha_i p'/q] - [x_1 \alpha_i p'/q])| < 1/k(p')^{\mu/r(1-\mu)},$$

$i = 1, \dots, r.$

Let $p^* = x_2 - x_1$. Then for $c = (2k)^{r(1-\mu)}$, we have $0 < p^* \leq c^{1/(1-\mu)}(p')^{\mu/(1-\mu)}$. Letting $u_i = [x_2 \alpha_i p'/q] - [x_1 \alpha_i p'/q]$, we obtain

$$\begin{aligned} \|\alpha_i p'/q\| &\leq |\alpha_i p'/q - u_i| < 1/k(p')^{\mu/r(1-\mu)} \leq c^{\mu/r(1-\mu)}/k p^{\mu/r} \\ &= 2^\mu/k^{1-\mu} p^{\mu/r} < K p^{-\mu/r}, \quad i = 1, \dots, r, \end{aligned}$$

for all sufficiently large k .

If $\mu = 1$, apply the box principle with A replaced by $k \geq 1$. Then

$$|(x_2 - x_1)\alpha_i/q - ([x_2 \alpha_i/q] - [x_1 \alpha_i/q])| < k^{-1}, \quad i = 1, \dots, r.$$

³ Added in proof. If (6) does not hold, then $p^\zeta < p^* \leq p^{\zeta-\epsilon}$ must hold. In this case we define λ by $(p')^{1-\lambda} = q^{1-\zeta-\epsilon}$, and the exponent of q in (7) becomes $1-\zeta-\epsilon$. Similarly, the ϵ in (7) may have to be put on the left side, in which case the remainder of the proof is again modified slightly.

Letting $p^* = p = x_2 - x_1 \leq k^r$, $u_i = [x_2 \alpha_i / q] - [x_1 \alpha_i / q]$, we have

$$\|\alpha_i p / q\| \leq |\alpha_i p / q - u_i| < k^{-1} \leq p^{-1/r}.$$

Suppose that the second part of the theorem is false. This means that there exist $\eta > 0$, $a > 0$ and a set of r -tuples $(\alpha_1, \dots, \alpha_r)$ of positive measure, for which (4) has an infinity of solutions in p, q of the form (1) subject to $p^* \leq p^{\mu-\eta}$, $p \geq aq$. Replacing $\mu - \eta$ by μ , we have $p^* \leq p^\mu$ and $\|\alpha_i p / q\| < K p^{-(\mu/r+\epsilon)}$, $i = 1, \dots, r$, infinitely often for any $0 < \epsilon \leq \eta/r$, and for a set of r -tuples of positive measure, contradicting Theorem I.

PROOF OF THEOREMS III, IV AND V. The proof of Theorem III is based on the second part of Theorem I. Its proof is very similar to the proof of [2, Theorem IV], and is therefore omitted. The proof of the first part of Theorem IV follows directly from [2, Theorem I]. For proving the second part, concerning the non-Liouville numbers, let

$$\frac{l_{m,k}}{p_{m,k}} = \sum_{i=1}^{mr/k} (p_{ik}^* P^{2^{ik}})^{-1}, \quad k = 1, \dots, r,$$

where m is any positive integer. Then $p_{m,k} = p_{mr/k}^* P^{2^{mr/k}}$ for $k = 1, \dots, r$, and

$$\alpha_k - \frac{l_{m,k}}{p_{m,k}} = \sum_{i > mr/k} (p_{ik}^* P^{2^{ik}})^{-1} < 2 \left(p_{mr/k}^* P^{2^{mr/k}} \right)^{-1}.$$

But $2P^{-2^{mr/k}} < (P^{-2^{mr/k}})^{1+\mu+\delta}$, $p_{mr/k}^* \leq p_{mr/k}^{*-(1+\mu+\delta)}$, if m is sufficiently large and $0 < \delta < 1 - \mu$. Hence $\|\alpha_k p\| < p^{-(\mu+\delta)} \leq p^{-(\mu/r+\delta)}$, $k = 1, \dots, r$ for an infinity of $p_{m,k} = p$, and α_k is transcendental by Ridout's Theorem. (Since the first terms of the series defining α_k can be chosen at will, the numbers α_k are also everywhere dense.) The same proof holds for the Liouville numbers.

For proving Theorem V, we use Schmidt's independence criterion for Liouville numbers [9]: Let $(\alpha_1, \dots, \alpha_n)$ be an n -tuple of reals such that for every $d > 0$ there exists an integer p with

$$0 < \|\alpha_k p\| < (\|\alpha_1 p\| \cdots \|\alpha_{k-1} p\|)^d p^{1-na}, \quad k = 1, \dots, n.$$

Then $\alpha_1, \dots, \alpha_n$ are algebraically independent over the rationals. To show that the $\beta(x, y)$ are independent, it suffices to apply Schmidt's criterion to the n^2 -tuple $(\beta(x_0, y_0), \beta(x_1, y_0), \dots, \beta(x_{n-1}, y_0), \beta(x_0, y_1), \dots, \beta(x_{n-1}, y_{n-1}))$, where n is fixed and $0 < x_0 < \dots < x_{n-1} < 1$, $0 < y_0 < \dots < y_{n-1} < 1$. Let

$$p_h = p^*(h) P^{h^h}, \quad p^*(h) \in U, \quad P^{h^h} \leq p^*(h) \leq P^{4+h^h}.$$

If h is sufficiently large,

$$\|\beta(x, y)p_h\| = p_h \sum_{i=0}^{\infty} \left(p^*(x, y, h+i) P^{[(h+i)(h+i+x)^{h+i+y}]} \right)^{-1}.$$

Hence, letting $f_{x,y} = p^*(h)/p^*(x, y, h)$,

$$f_{x,y} P^{h^h - [h^{(h+x)^{h+y}}]} < \|\beta(x, y)\| < 2f_{x,y} P^{h^h - [h^{(h+x)^{h+y}}]}.$$

If $k-1 = vn+r$, $0 \leq r < n$, then

$$\prod \|\beta(x_i, y_j)\|^d p_h^{1-nd} > p^*(h) p^*(x_r, y_v, h)^{-nd} P^{h^h - [h^{(h+x_r)^{h+y_v}}]},$$

where the product is taken over all i, j satisfying $0 \leq i+jn \leq k-1$, $0 \leq i < n$. It is easily verified that

$$P^{h^h - nd [h^{(h+x_r)^{h+y_v}}]} > \begin{cases} P^{h^h - [h^{(h+x_{r+1})^{h+y_v}}]}, & \text{if } 0 \leq r < n-1, \\ P^{h^h - [h^{(h+x_0)^{h+y_{v+1}}}]}, & \text{if } r = n-1, \end{cases}$$

and

$$p(h)^* p^*(x_r, y_v, h)^{-nd} > \begin{cases} f_{x_{r+1}, y_v}, & \text{if } 0 \leq r < n-1, \\ f_{x_0, y_{v+1}}, & \text{if } r = n-1, \end{cases}$$

if $h = h(d)$ is sufficiently large. Hence Schmidt's criterion is satisfied. For the numbers α_k the criterion is applied with $p_h = p_h^* P^{h^h}$, $p_h^* \in S_\mu$, $n! | h$, for the β_k with $p_h = p_h^* P^{n h^h}$, $p_h^* \in S_{1/2}$, $n! | h$, and for the $\alpha(x)$ it is applied with $p_h = p^*(h) P^{h^h}$, $p^*(h) \in U$, $P^{h^h} < p^*(h) < P^{h+h^h}$.

REFERENCES

1. A. S. Fraenkel, *On a Theorem of D. Ridout in the theory of Diophantine approximations*, Trans. Amer. Math. Soc. 105 (1962), 84-101.
2. ———, *Transcendental numbers and a conjecture of Erdős and Mahler*, J. London Math Soc. 39 (1964), 405-416.
3. H. Kneser, *Eine kontinuiersmächtige, algebraisch unabhängige Menge reeller Zahlen*, Bull. Soc. Math. Belg. 12 (1960), 23-27.
4. F. Kuiper and J. Popken, *On the so-called von Neumann numbers*, Nederl. Akad. Wetensch. Proc. Ser. A 65 (1962), 385-390.
5. K. Mahler, *On the fractional parts of the powers of a rational number. II*, Mathematika 4 (1957), 122-124.
6. ———, *Lectures on Diophantine approximations*, Part 1, University of Notre Dame, Notre Dame, Ind., 1961.
7. J. von Neumann, *Ein System algebraisch unabhängiger Zahlen*, Math. Ann. 99 (1928), 134-141.
8. D. Ridout, *Rational approximations to algebraic numbers*, Mathematika 4 (1957), 125-131.
9. W. M. Schmidt, *Simultaneous approximation and algebraic independence of numbers*, Bull. Amer. Math. Soc. 68 (1962), 475-478.

THE WEIZMANN INSTITUTE OF SCIENCE, REHOVOT, ISRAEL