BULL. AUSTRAL. MATH. SOC. 10F35,
VOL. 29(1984), 127-136. 03D15, 39B30, 65C10, 68D35.

A METHOD OF MAHLER IN TRANSCENDENCE THEORY AND SOME OF ITS APPLICATIONS*

J.H. LOXTON

Remarks on transcendence theory lead to a surprising proof that the decimal expansion of an algebraic irrational is irregular and to speculations on random numbers.

Kurt Mahler has introduced many profound ideas and methods into the theory of transcendental numbers. His work in this area includes detailed study of the algebraic approximations of numbers such as e, π and $\log 2$, a new classification of real and complex numbers according to their approximation properties, and the initiation and development of p-adic transcendence theory. The particular method which I shall discuss here can be traced back to Mahler's earliest papers written in Göttingen in the 1920's. These papers were unaccountably overlooked for many years, but they have received considerable attention in recent times because of links with the theory of automata.

Transcendence theory is the study of the arithmetic properties of interesting numbers. The beginnings of the subject can therefore be traced

Received 3 October 1983.

* This is a lecture delivered at the Special Meeting of the Australian Mathematical Society "Celebration of the 80th Birthday of Kurt Mahler", Canberra, July 26, 1983.

https://doi.org/10.1017/S0004972700021341 Published online by Cambridge University Press

back to the discovery by the school of Pythagoras that $\sqrt{2}$ is irrational. Subsequent milestones were the proofs of the irrationality of e by Euler and of π by Lambert. One of the reasons for the interest in these questions comes from the classical construction problems of Greek geometry, particularly the problem of squaring the circle. This problem was finally resolved by Lindemann in 1884 when he showed that π is transcendental, that is π is not the root of any polynomial with integer coefficients. Lindemann's work rests on ideas introduced by Hermite in 1873 to prove the transcendence of e.

The first authenticated transcendental numbers were produced by Liouville in 1844. A typical example is the number $\sum_{n=1}^{\infty} 2^{-n!}$.

Liouville's argument depends on a simple but fundamental inequality which appears again and again in transcendence theory. Suppose α is a non-zero algebraic number, so that α is the root of some minimal polynomial with integer coefficients, say

$$f(x) = a_0 x^d + a_1 x^{d-1} + \dots + a_d = a_0 \prod_{j=1}^{d} (x - \alpha_j) .$$

Here $d = deg(\alpha)$ is the degree of α, $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_d$ are the conjugates of α and $h(\alpha) = max\{|\alpha_0|, |\alpha_1|, \dots, |\alpha_d|\}$ is one possible measure of the size of α.[†] Since α is non-zero, a_d is a non-zero integer and so

$$1 \le |a_d| = |a_0| \prod_{j=1}^{d} |\alpha_j| \le |\alpha| \; h(\alpha)^d .$$

This gives Liouville's inequality

$$\log|\alpha| + deg(\alpha) \log h(\alpha) \ge 0 \quad .$$

Now suppose $\alpha = \sum_{n=1}^{\infty} 2^{-n!}$ is algebraic and consider

[†] This is not the canonical height, but it will serve here. For the correct definition, see [8], pages 78-80.

https://doi.org/10.1017/S0004972700021341 Published online by Cambridge University Press

$$\alpha_N = \alpha - \sum_{n=1}^{N-1} 2^{-n!} = \sum_{n=N}^{\infty} 2^{-n!} .$$

Then α_N is a non-zero algebraic number with the same degree as α, $\log|\alpha_N| \le -cN!$ and $\log h(\alpha_N) \le c(N-1)!$ for some positive constant c. (The last assertion comes about because the conjugates of α_N are bounded independent of N and $2^{(N-1)!}\alpha_N$ satisfies a polynomial equation with integer coefficientsand with the same leading coefficient as the minimal polynomial for α.) It follows that $\log|\alpha_N| + deg(\alpha_N)\log h(\alpha_N)$ is negative for sufficiently large N, contradicting the fundamental inequality. Thus Liouville's number is transcendental. This argument can be applied to gap series $\sum_{n=0}^{\infty} a_n z^{\lambda_n}$ with $\lambda_{n+1}/\lambda_n \to \infty$ as $n \to \infty$. (See [2].)

Mahler began his studies of transcendental numbers around 1926. In his engaging account [11] of fifty years as a mathematician, he writes: "During a part of that year I was very ill and in bed. To occupy myself, I played with the function $f(z) = \sum_{n=0}^{\infty} z^{2^n}$ and tried to prove that $f(\zeta)$ is irrational for rational ζ satisfying $0 < |\zeta| < 1$." The function $f(z)$ does not have large enough gaps to accommodate Liouville's method, but it does have the functional equation $f(z^2) = f(z) - z$, and this is the key to the method. By way of illustration, I shall sketch the proof of the transcendence of $f(\frac{1}{2}) = \sum_{n=0}^{\infty} 2^{-2^n}$. (*) Suppose, on the contrary, that $f(\frac{1}{2})$ is algebraic. Choose polynomials $p_0(z), \ldots, p_N(z)$, with degrees at most N and integer coefficients and not all identically zero, so that

$$E_N(z)(say) = \sum_{j=0}^{N} p_j(z)f(z)^j = \sum_{n=N^2}^{\infty} c_n z^n .$$

* This is an interesting number and can be treated by several different methods. It has an interesting continued fraction development with bounded partial quotients. (See [5], Section 2.3.)

https://doi.org/10.1017/S0004972700021341 Published online by Cambridge University Press

This is possible because the $p_j(z)$ have in all $(N+1)^2$ coefficients and these must satisfy N^2 linear equations to give $E_N(z)$ a zero of order N^2 at the origin. Now consider the number

$$\alpha_{N,k} = E_N(2^{-2^k}) = \sum_{j=0}^{N} p_j(2^{-2^k})\left\{f(\tfrac{1}{2}) - \sum_{i=0}^{k-1} 2^{-2^i}\right\}^j = \sum_{n=N^2}^{\infty} c_n \, 2^{-2^k n} .$$

(The first representation is obtained by iterating the functional equation to get $f(z^{2^k}) = f(z) - z - z^2 - \ldots - z^{2^{k-1}}$.) Then $\alpha_{N,k}$ is an algebraic number with degree at most the degree of $f(\frac{1}{2})$, $\log h(\alpha_{N,k}) \leq c2^k N$ for some positive constant c from the first representation of $\alpha_{N,k}$ and $\log|\alpha_{N,k}| \leq -c2^k N^2$ from the second. Thus

$$\log|\alpha_{N,k}| + \deg(\alpha_{N,k}) \log h(\alpha_{N,k}) < 0 \text{ for sufficiently large } N$$

and k. The difficulty, as in most transcendence proofs, is to show that $\alpha_{N,k}$ is non-zero. In this example, $f(z)$ has a natural boundary on the unit circle $|z| = 1$, so $f(z)$ is a transcendental function and the function $E_N(z)$ does not vanish identically. Thus $E_N(2^{-2^k})$ is non-zero for all sufficiently large k. Again, this contradicts the fundamental inequality, showing $f(\frac{1}{2})$ is transcendental. Mahler generalised this argument to power series in several variables which satisfy a very general type of functional equation. (See [9] .)

The example above is based on the generating function of the powers of 2. As another example, consider the generating function for numbers missing the digit 1 in base 3, say $g(z) = \sum_{n=0}^{\infty} a_n z^n$, where $a_n = 0$ or 1 according as n has a 1 in its ternary representation or not. Then $a_{3n} = a_{3n+2} = a_n$ and $a_{3n+1} = 0$, so

$$g(z) = \sum_{n=0}^{\infty} a_{3n} z^{3n} + \sum_{n=0}^{\infty} a_{3n+2} z^{3n+2} = (1 + z^2)g(z^3) .$$

Mahler's theorem shows that $g(\frac{1}{2}) = \sum_{n=0}^{\infty} a_n 2^{-n}$ is transcendental since

https://doi.org/10.1017/S0004972700021341 Published online by Cambridge University Press

$g(z) = \prod_{n=0}^{\infty} (1+z^{2.3^n})$ is a transcendental function. Another infamous example is the paper-folding sequence. (See [5], Section 1.1). If a piece of paper is folded in half repeatedly, right half over left, a sequence of folds results which can be represented by the sequence

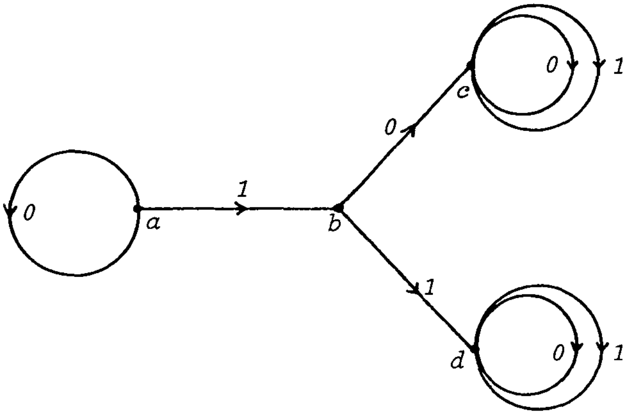
$$110110011100100111011000110010 01 \ldots ,$$

where 1 denotes a crease V and 0 denotes a crease Λ .(†) Suppose the pattern of creases after n folds is $a_1 a_2 \ldots a_{2^n-1}$. It is easy to see that the first half of this sequence gives the pattern for $n-1$ folds, so the pattern converges to an infinite sequence. The $(n+1)$-st fold produces the sequence $1a_1 0a_2 1a_3 0a_4 \ldots 1a_{2^n-1}$, so $a_{4n+1} = 1$, $a_{4n+3} = 0$ and $a_{2n} = a_n$. The generating function $h(z) = \sum_{n=0}^{\infty} a_n z^n$ satisfies the functional equation $h(z)=h(z^2) + z/(1-z^4)$. Again the decimal $h(\frac{1}{2}) = \sum_{n=0}^{\infty} a_n 2^{-n}$ is transcendental.

These examples are all regular sequences in the following sense. (See [5], Sections 1.2 and 2.4.) A finite automaton is a device with a finite number of states, an input which reads the digits $0,1, \ldots ,r-1$, say, and an output. On reading an input digit, the machine goes to a new state which depends on the old state and the input. This step can be repeated to accommodate a finite string of input digits. The output indicates whether the final state is accepted or not. A sequence $\{a_n\}$ is regular in base r if, for each n , there is a finite automaton whose output corresponding to the string of digits of n in base r is a_n . The machine shown generates the paper-folding sequence.

† Of course, this is theoretical paper-folding. A real piece of paper cannot be folded more than 7 times.

https://doi.org/10.1017/S0004972700021341 Published online by Cambridge University Press



The initial state is a and the input is the binary representation $(n)_2 = c_s \dots c_1c_0$ of n, read from right to left. The output is 1 if the final state is a, b, or c and 0 if it is d. In general, let $a_s(n)$ be the output corresponding to initial state s and input $(n)_r$. Then $a_s(nr+t) = a_{t(s)}(n)$, in the obvious notation, because the input t moves the machine from state s to state $t(s)$. If $f_s(z) = \sum_{n=1}^{\infty} a_s(n)z^n$, then

$$f_s(z) = \sum_{t=0}^{r-1} z^t f_{t(s)}(z^r) .$$

This property characterises the generating functions of regular sequences in base r : there is a vector $\underset{\sim}{f}(z)$, whose first component is the given generating function, satisfying a system of functional equations $\underset{\sim}{f}(z) = A(z)\,\underset{\sim}{f}(z^r)$, where $A(z)$ is a matrix of rational functions. Mahler's method can be used to show that, if α is an algebraic number with $0 < |\alpha| < 1$, then the algebraic relations among the numbers $\underset{\sim}{f}(\alpha)$

https://doi.org/10.1017/S0004972700021341 Published online by Cambridge University Press

arise from the algebraic relations among the functions $\underset{\sim}{f}(z)$. In particular, if $f(z) = \sum_{n=0}^{\infty} a_n z^n$ is the generating function of a regular sequence, then $f(z)$ is either rational or transcendental and, correspondingly, the decimal $f(b^{-1}) = \sum_{n=0}^{\infty} a_n b^{-n}$ is either rational or transcendental. Thus, the decimal expansion of an algebraic irrational cannot be generated by a finite automaton. (See [10] .(*))

Extraordinarily little is known about the decimal expansions of irrational numbers. It is reasonable to conjecture that "simple" irrationals such as e , π and $\sqrt{2}$ have "random" decimals. Of course, rational numbers have periodic expansions, but if the period is sufficiently long, it is possible to prove various results and the period appears to be practically random. (See [13]). This is important because it is closely related to the way in which pseudo-random numbers are generated by a computer. Nothing of the sort has been proved about e, π, or $\sqrt{2}$. The simplest requirement for randomness is normality, namely that the various patterns of digits in the expansion should appear with the correct uniform frequencies. Almost all numbers are normal, but explicit examples are rare. The interesting, but distinctly non-random number $0.123456789101112\ldots$ is normal in base 10 and is another of Mahler's transcendental numbers. No-one has found a normal algebraic number. A battery of statistical tests has been developed to try to capture the idea of a random sequence (See [7] .) These have been applied to large chunks of the decimal expansions of e, π and various simple algebraic numbers. ([1], [6] and [12]). The statistical evidence offers no surprises, except perhaps for some peculiarities found by Stoneham in the first 60,000 decimal digits of e. It has to be admitted that this ad hoc battery of statistical tests does not amount to a satisfying definition of randomness.

The result about the decimal expansion of algebraic irrationals and finite automata suggests an alternative theoretical approach to randomness.

* The annoying technical restriction in the results in this paper has recently been removed.

https://doi.org/10.1017/S0004972700021341 Published online by Cambridge University Press

We can try to assign a measure of computational complexity to a sequence by means of the following hierarchy:

(0) periodic sequences,

(1) regular sequences generated by finite automata,

(2) sequences generated by automata with one push-down store,

(3) sequences generated by non-deterministic automata with one push-down store, and

(4) sequences generated by Turing machines.

Essentially, the n-th term of a regular sequence is computed from the input n without any memory of the earlier terms. A push-down store allows an arbitrary number of terms of the sequence to be stored and recalled later, the first one in being the last one out. Two push-down stores are equivalent to the doubly infinite tape of a Turing machine, which explains why the classification stops as it does. A random sequence is now one which cannot be generated by any machine less powerful than a Turing machine. The class of regular sequences has been investigated in some depth by Cobham. ([3] and [4].) He has shown that the notion is base dependent, that is, if a sequence is regular in two multiplicatively independent bases, then it is periodic. Unfortunately, although the regular sequences are accessible, they are extremely restricted. For example, a regular sequence defined on an alphabet with s symbols can contain at most $c\,n$ n-tuples out of the total of s^n n-tuples on the given alphabet; in other words, regular sequences have zero entropy. There are some fascinating possibilities here involving transcendence theory, automata and the spectral properties of sequences. The remarks made above about Mahler's method, regular sequences and entropy can be extended in various ways and the combination of these ingredients seems likely to yield further interesting results.

https://doi.org/10.1017/S0004972700021341 Published online by Cambridge University Press

References

[1] W.A. Bayer, N. Metropolis and J.R. Neergard, "Statistical study of the digits of some square roots of integers in various bases", *Math. Comp.* 24 (1970), 455-473.

[2] P.L. Cijsouw and R. Tijdeman, "On the transcendence of certain power series of algebraic numbers", *Acta Arith.* 23 (1973), 301-305.

[3] A. Cobham, "On the base dependence of sets of numbers recognised by finite automata", *Math. Systems Theory* 3 (1969), 186-192.

[4] A. Cobham, "Uniform Tag sequences", *Math. Systems Theory* 6 (1972), 164-192.

[5] M. Dekking, M. Mendès France and A. van der Poorten, "Folds!", *Mathematical Intelligencer*4 (1982), 130-138, 173-180 and 190-195.

[6] J. Guilloud and M. Bouyer, "1,000,000 de decimales de π", *(Commissariat à l'energie Atomique,* 1974*)*.

[7] D. Knuth, *The art of computer programming: Volume 2* (Addison-Wesley, 1969).

[8] S. Lang, *Elliptic curves, diophantine analysis* (Springer, 1978).

[9] J.H. Loxton and A.J. van der Poorten, "Transcendence and algebraic independence by a method of Mahler". In *Transcendence theory: advances and applications*, A. Baker and D.W. Masser (Academic Press, 1977), 211-226.

[10] J.H. Loxton and A.J. van der Poorten, "Arithmetic properties of the solutions of a class of functional equations", *J. reine angew. Math.* 330 (1982), 159-172.

[11] K. Mahler, "Fifty years as a mathematician", *J. Number Theory*, 14 (1982), 121-155.

[12] R.G. Stoneham, "A study of 60,000 digits of the transcendental "e"." *Amer. Math. Monthly* 72 (1965), 483-500.

https://doi.org/10.1017/S0004972700021341 Published online by Cambridge University Press

[13] R.G. Stoneham, "On the uniform ε-distribution of residues within the periods of rational numbers with applications to normal numbers", *Acta Arith.* 22 (1973), 371-389.

School of Mathematics,
University of New South Wales,
Kensington, N.S.W., 2033,
AUSTRALIA.