数理解析研究所講究録
第 496 巻 1983 年 24-34

AUTOMATA AND TRANSCENDENTAL NUMBER THEORY

MICHEL MENDES FRANCE

UNIVERSITE DE BORDEAUX I

1. An example.

Let E be the set of finite sums of distict powers of 4,

$$E = \{0,1,4,5,16,...\}$$

and let $2E$ be the set obtained by doubling E

$$2E = \{0,2,8,10,32,...\} \quad .$$

Define the real number

$$\alpha = \sum_{n \in E} \frac{1}{2^n} = \sum_{n=0}^{\infty} \frac{\alpha_n}{2^n} \quad .$$

The sequence (α_n) represents the characteristic function of E. The binary expansion of α is thus "known" in the sense which we make more precise in the last paragraph.

A.Blanchard noticed that the $1/\alpha$ has a simple binary expansion (1) . Indeed,

$$\frac{1}{\alpha} = \frac{1}{2} \times \sum_{n \varepsilon 2E} \frac{1}{2^n} .$$

The proof of this is very simple. Let

$$\beta = \frac{2}{\alpha} = \sum_{n \varepsilon 2E} \frac{1}{2^n} .$$

Observe

$$\alpha = \prod_{n=0}^{\infty} \left(1 + \frac{1}{2^{4^n}} \right)$$

$$\beta = \prod_{n=0}^{\infty} \left(1 + \frac{1}{2^{2 \cdot 4^n}} \right)$$

so that

$$\alpha\beta = \prod_{n=0}^{\infty} \left(1 + \frac{1}{2^{2^n}} \right) .$$

Using Euler's product formula

$$\prod_{n=0}^{\infty} (1 + x^{2^n}) = (1 - x)^{-1} ,$$

we conclude $\alpha\beta = 2$.

Q.E.D.

A careful look at the binary expansion of α shows that α is transcendental. To be more precise, one notices in the expansion of α long blocks of 0's from which one can deduce the following theorem.

THEOREM 1: *There exists a constant* $c > 0$ *such that for infinitely many rational numbers* a/q

$$\left| \alpha - \frac{a}{q} \right| < \frac{c}{q^3} .$$

Roth's theorem then shows that α is indeed transcendental. For details, see (1).

2. Formal power series.

We shall give here a new proof of the transcendence of α . Let γ be a real number

$$\gamma = \sum_{n=0}^{\infty} \frac{\gamma_n}{2^n}, \quad \gamma_0 = [\gamma], \quad \gamma_n \in \{0,1\} , \ n \geq 1 .$$

Let $q = p^{\mu}$ be a given prime power ($\mu \geq 1$). To γ we associate the formal power series

$$\gamma = \gamma(X) = \sum_{n=0}^{\infty} \gamma_n X^n \in F_q((X))$$

where the coefficients γ_n are considered as elements of the finite field $\mathbb{F}_q$ (γ_0 can be given the value γ_0 (mod q) for example). The ring $\mathbb{F}_q[X]$ of integers in $\mathbb{F}_q((X))$ is just the ring of polynomials. The field $\mathbb{F}_q(X)$ of rational elements in

$\mathbb{F}_q((X))$ is the set of A/B, $A \in \mathbb{F}_q[X]$, $B \in \mathbb{F}_q[X]$. An element $\gamma \in \mathbb{F}_q((X))$ is said to be algebraic (over $\mathbb{F}_q(X)$) if there exist polynomials $a_\nu, a_{\nu-1}, \ldots a_0$ not all zero such that

$$a_0 \gamma^\nu + a_1 \gamma^{\nu-1} + \ldots + a_{\nu-1}\gamma + a_\nu = 0 .$$

A nonalgebraic element is transcendental.

THEOREM 2: <u>If an element γ is an irrational algebraic element of some field, it is transcendental in any other field.</u>

This very vague statement needs to be explained. Let $q' > q$ be another prime power : $q' = (p')^\nu$, $p' \neq p$. Let j be an injective map

$$F_q \xhookrightarrow{\; j \;} F_{q'} .$$

(j is <u>not</u> a field homomorphism : j is a map defined on the <u>set</u> $\mathbb{F}_q$ and taking values in the <u>set</u> $\mathbb{F}_{q'}$). We identify $\mathbb{F}_q$ with a subset of $\mathbb{F}_{q'}$.

Suppose

$$\gamma = \sum_{n=0}^{\infty} \gamma_n X^n \in \mathbb{F}_q((X))$$

is irrational and algebraic over $\mathbb{F}_q(X)$. The theorem states that γ considered as element of $\mathbb{F}_{q'}((X))$ is transcendental over $\mathbb{F}_{q'}((X))$ is transcendental over $\mathbb{F}_{q'}(X)$. See (2).

This result led J.Loxton and A.van der Poorten (3) to the deeper result that the real number

$$\gamma = \sum_{n=0}^{\infty} \frac{\gamma_n}{2^n}$$

is transcendental over $\mathbb{Q}$.

Keeping this in mind, we turn back to our numbers

$$\alpha = \sum_{n \in E} \frac{1}{2^n} = \sum_{n=0}^{\infty} \frac{\alpha_n}{2^n} \quad (\alpha_n \in \{0,1\})$$

$$\beta = \sum_{n \in 2E} \frac{1}{2^n} = \sum_{n=0}^{\infty} \frac{\beta_n}{2^n} \quad (\beta_n \in \{0,1\}) .$$

We consider the two formal power series

$$\alpha = \alpha(X) = \sum_{n=0}^{\infty} \alpha_n X^n = \prod_{n=0}^{\infty} (1 + X^{4^n}) \quad \in \mathbb{F}_2((X))$$

$$\beta = \beta(X) = \sum_{n=0}^{\infty} \beta_n X^n = \prod_{n=0}^{\infty} (1 + X^{2 \cdot 4^n}) \quad \in \mathbb{F}_2((X)) .$$

Then

$$\alpha\beta = \prod_{n=0}^{\infty} (1 + X^{2^n}) = (1 - X)^{-1}.$$

Notice also that in $\mathbb{F}_2((X))$.

$$\alpha^2 = (\alpha(X))^2 = \alpha(X^2) = \beta$$

hence

$$\alpha^3 = (1 - X)^{-1}$$

which shows that α is a cubic irrationality in $\mathbb{F}_2((X))$.

Loxton and van der Poorten's result then implies the transcendency of the real number α .

Q.E.D.

The following conjectures are somehow related to the above discussion:

CONJECTURE 1: Suppose $\gamma_0, \gamma_1, \gamma_2, \ldots$ is an infinite sequence of 0's and 1's, which is not eventually periodic. Prove that one at least of the two numbers

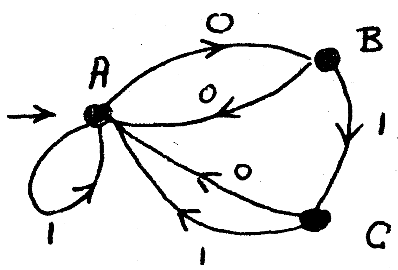
$$\sum_0^\infty \frac{\gamma_n}{2^n} , \quad \sum_0^\infty \frac{\gamma_n}{3^n}$$

is transcendental.

CONJECTURE 2: All the irrational numbers of the Cantor ternary set are transcendental.

3. AUTOMATA THEORY

An automaton is a finite set of points (states) with rules indicating how to go from one state to another. For example the automaton $\mathcal{M}$



$\mathcal{M}$

tells us that if we are given the instructions 1010 we are to leave from the initial state A, then 1 sends us back onto A, 0 onto B, 1 onto C, 0 onto A. Any finite string of 0's 1's will send us onto one of the final states A,B or C.

The definition of the automaton is not yet complete. The states themselves are renamed with the symbols 0 or 1. Say A = 1, B = 0, C = 1. Now every finite string of 0's and 1's is sent on 0 or 1.

Look at the sequence of integers as a sequence of words on the symbols 0 and 1

$$0, 1, 10, 11, 100, 101, 110, 111, 1000, \ldots$$

The integer 6 for example acts on the automaton $\mathcal{M}$ as indicated

$$110A = 11B = 1C = A \to 1$$

hence $\mathcal{M} : 6 \mapsto \mathcal{M}(6) = 1$. The infinite sequence

$$\mathcal{M}(0), \mathcal{M}(1), \mathcal{M}(2), \ldots, \mathcal{M}(n), \ldots$$

is said to be generated by the automaton $\mathcal{M}$.

Given an infinite sequence of 0's and 1's, one can ask whether there exists an automaton that generates it. The question is pertinent in that that the family of all 0,1-sequences is noncountable whereas the family of automata is countable. The following result answers our question and shows the relevance of automata theory to the theory of transcendental numbers.

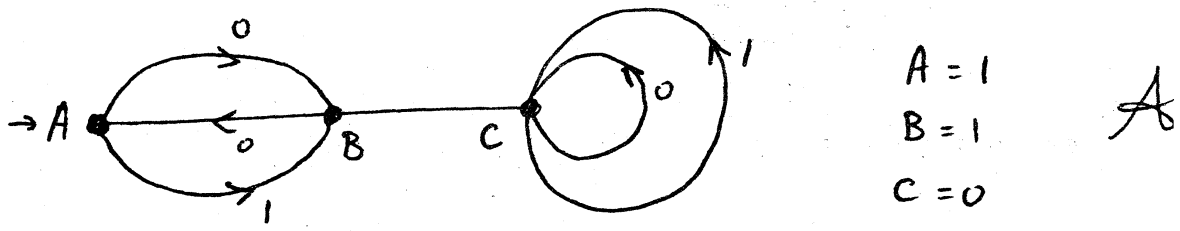
THEOREM 3: A sequence $\varepsilon = (\varepsilon_n)$ of 0's and 1's is generated by automaton if and only if the formal power series

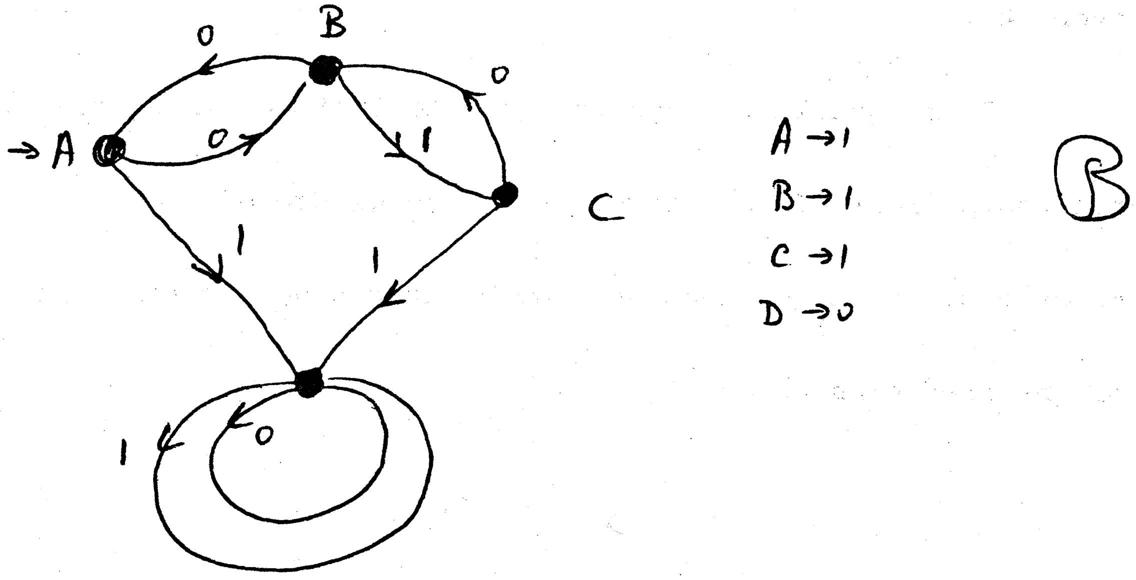
$$\sum_{n=0}^{\infty} \varepsilon_n X^n \in F_2((X))$$

is algebraic over $F_2((X))$.

(For details, see (2)).

As a consequence, the digits of α and those of β are indeed generated by automata. $\mathcal{A}$ generates α and $\mathcal{B}$ generates β





Once one knows the automaton that generates α (resp. β), then one can obtain the millionth digit, say, of α without having to compute the preceding ones. It is somehow remarkable that both α and $1/\alpha$ ($= \beta/2$) share this property.

Irrational algebraic numbers do not have this property. Indeed, as noticed by Loxton and van der Poorten, one has the following corollary of theorem 2 .

<u>COROLLARY</u>: <u>The digits of real algebraic irrational numbers are not generated by automata</u>.

Indeed if

$$\varepsilon = \sum \frac{\varepsilon_n}{2^n}$$

were automata generated, then

$$\sum \varepsilon_n X^n$$

would be algebraic over $\mathbb{F}_2(X)$ hence ε would be transcendental over $\mathbb{Q}$.

This corollary seems to indicate that the knowledge of the millionth digit of $\sqrt{2}$ imvolves the knowledge of the nine hundred ninety nine thousand nine hundred ninety ninth digit and of the preceding ones...

4. EXERCISES.

1. Let E_1 be the set of integers which do not contain 1 in their expansion in base 4 and let E_3 the set of integers which do not contain 3 in their expansion in base 4. Define

$$\gamma = \sum_{n\varepsilon E_3} \frac{1}{2^n} \qquad \delta = \frac{1}{4}\sum_{n\varepsilon E_1} \frac{1}{2^n} .$$

Prove that $\gamma\delta = 1$. Show that γ and δ are generated by automata.

2. Write the continued fraction expansion of α .

REFERENCES

(1) A.BLANCHARD,M.MENDES FRANCE: Symétrie et transcendance, Bull. Sci.Math.France,110,1982.

(2) G.CHRISTOL,T.KAMAE,M.MENDES FRANCE,G.RAUZY: Suites algébriques, automates et substitutions, Bull.Soc.Math.France ,108,1980,401-419.

(3) J.LOXTON,A.van der POORTEN: Arithmetic properties of the solutions of a class of functional equations, Jour.für reine und angew.Math.330,1982,159-172.

For broader discussion of the present and related topics, see FOLDS!: M.DEKKING,M.MENDES FRANCE,A.van der POORTEN, The Mathematical Intelligencer,14,1982,130-138.

CORRECTIONS TO AUTOMATA AND TRANSCENDENTAL NUMBER THEORY.

Page 9, ligne-3: Au lieu de imvolves, lire involves.

Page 10, ligne 11: A completer : 325-335.

Page 10, ligne-1: Corriger la reference:
Mathematical Intelligencer 4,1982,130,138.173-181,190-195.

Page 10, sous la dernière reference, ajouter la mention suivante:
I wish to thank K.Nagasaka for his help, discussions and kind hospitality.

CORRECTIONS TO PROBLEMS RELATED TO BASES.

Page 4, ligne-7: Au lieu de autonomous, lire automaton.

Page 7, ligne-4: Completer la reference:
Répartition (mod 1) des puissances successives des nombres réels, Commet.Math.Helv.,19,1946,153-160.

Page 7, reference (4); Au lieu de Copmtes, lire Comptes.

CORRECTIONS TO SPECTRAL THEORY ON UNIFORMLY DISTRIBUTED SEQUENCES.

Page 8, ligne-1: Au lieu de Les Recherehes, lire La recherche, et le title n'est pas exact.

Page 9, sous la dernière reference, ajouter la mention suivante:
This list is not complete. Some joint works with Christian Batut are missed and several reports in the Delange-Pisot-Poitou Seminar are not either found.