Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 26 (1980)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: NOMBRES ALGÉBRIQUES ET THÉORIE DES AUTOMATES
Autor: France, Michel Mendes
DOI: https://doi.org/10.5169/seals-51067

NOMBRES ALGÉBRIQUES ET THÉORIE DES AUTOMATES

par Michel MENDES FRANCE

Résumé : La théorie des automates permet d'aborder le problème de la représentation décimale des nombres algébriques réels.

§ 1. DEUX PROBLÈMES

Ce compte rendu est un résumé d'un article à paraître au Bulletin de la Société Mathématique de France, écrit conjointement avec G. Christol, T. Kamae et G. Rauzy. L'objet de ce travail est de fournir une première approche à la solution des deux problèmes suivants:

PROBLÈME 1. *Soient* g_1 *et* g_2 *deux entiers* $\geqslant 2$ *tels que* $\log g_1/\log g_2 \notin \mathbf{Q}$. *Soit* $\varepsilon_1, \varepsilon_2, \varepsilon_3, \ldots$ *une suite infinie d'entiers tels que* $0 \leqslant \varepsilon_n < \min\{g_1, g_2\}$. *Montrer que les nombres*

$$\xi = \sum_{n=1}^{\infty} \frac{\varepsilon_n}{g_1^n} \qquad \eta = \sum_{n=1}^{\infty} \frac{\varepsilon_n}{g_2^n}$$

sont ou bien tous deux rationnels, ou bien l'un au moins est transcendant.

PROBLÈME 2. *Soit* ζ *un nombre algébrique irrationnel réel. Soit*

$$\zeta = \sum_{n=1}^{\infty} \frac{\varepsilon_n}{g^n} \qquad 0 \leqslant \varepsilon_n < g$$

son développement en base g. *La suite* $\varepsilon_1, \varepsilon_2, \varepsilon_3, \ldots$ *est-elle au « hasard » ?*

La notion de hasard est, bien entendu, à préciser. Il y a essentiellement deux interprétations possibles à la question. En premier lieu, « suite au hasard » pourrait signifier « suite normale »: la fréquence d'apparition de tout mot construit sur l'alphabet $\{0, 1, \ldots, g-1\}$ est égale à g^{-l} où l est la longueur du mot considéré (notion de nombre normal). En second

lieu, « suite au hasard » pourrait signifier une suite qui ne peut pas être engendrée par une méthode « mécaniste » du type machine de Turing. Cet aspect est lié aux travaux de Kolmogoroff [8] et de Martin Löf [10] (on pourra se reporter à Schnorr [16] ou Dellacherie [6]).

Nous montrons ici que la réponse au problème 1 est positive *à condition* de considérer les opérations sur **R** *sans retenues* respectivement par rapport aux bases g_1 et g_2. En relation avec le problème 2, nous montrons en quoi la conjecture suivante est hautement probable et sans doute accessible (nous espérons en donner une preuve bientôt).

CONJECTURE. *Si*

$$\zeta = \sum_{n=1}^{\infty} \frac{\varepsilon_n}{g^n}$$

est un nombre réel algébrique irrationnel, alors la suite $\varepsilon_1, \varepsilon_2, \varepsilon_3, \ldots$ *ne peut pas être engendrée par un* g*-automate.*

Nous définissons le g-automate plus loin.

§ 2. LA SUITE DE MORSE

Les différents concepts dont nous aurons besoin seront introduits via la suite de Morse dont nous donnons plusieurs définitions.

Définition 1. A l'entier $n \geqslant 0$, on associe son développement binaire

$$n = \sum_{k=0}^{\infty} e_k(n)\, 2^k = \ldots e_2(n)\, e_1(n)\, e_0(n)$$

où $e_k(n) \in \{0, 1\}$ et $e_k(n) = 0$ pour tout $k > \left[\frac{\log n}{\log z}\right]$. Le nombre d'apparitions du chiffre 1 dans le mot $\ldots e_2(n)\, e_1(n)\, e_0(n)$ est

$$m_n = \sum_{k=0}^{\infty} e_k(n)$$

La suite de Morse M est la suite infinie (m_n) (mod 2) ($n \in \mathbf{N} = \{0, 1, 2, \ldots\}$). Elle débute donc ainsi

$$M = 0\ 110\ 1\ 00\ 11\ 00\ 10\ 11\ 0\ 1\ \ldots \in \{0, 1\}^{\mathbf{N}}.$$

Définition 2 (automates). On considère l'automate à 2 états x_0 et x_1 dont la fonction de transition est définie par

$$\begin{aligned} 0\,x_0 &= x_0 & \qquad 1\,x_0 &= x_1 \\ 0\,x_1 &= x_1 & \qquad 1\,x_1 &= x_0 \end{aligned}$$

L'entier $n \in \mathbf{N}$, $n = e_l\, e_{l-1} \ldots e_1 e_0$ (écrit en base 2) opère sur $x \in \{x_0, x_1\}$ de la façon suivante:

$$n\,x = (e_l\, e_{l-1} \ldots e_1\, e_0)\, x = (e_l\, e_{l-1} \ldots e_1)\,(e_0\, x)\,.$$

En particulier, nx_0 est l'un des deux états x_0 ou x_1, disons x_{m_n}. La suite (m_n) est la suite de Morse.

L'automate décrit ci-dessus est un 2-automate. Le symbole 2 se réfère au fait que de chaque état partent 2 chemins. Un 2-automate peut avoir autant d'états qu'on voudra, en nombre fini toutefois. Plus généralement, soit $g \geqslant 2$ un entier. Un g-automate ne diffère du précédent automate que par le nombre de chemins partant de chaque état, ici égal à g. L'entier n, écrit en base g opère alors sur l'état initial x_0 du g-automate. (Pour une théorie générale, voir Eilenberg [7].)

Définition 3 (substitutions). Une substitution σ de $\{0, 1\}^{\mathbf{N}}$ dans $\{0, 1\}^{\mathbf{N}}$ est une application qui consiste à remplacer dans une suite infinie $\varepsilon_0, \varepsilon_1, \varepsilon_2, \ldots$ chaque 0 et chaque 1 respectivement par un mot formé de 0 et de 1. Par exemple, considérons la substitution σ qui consiste à remplacer 0 par 01 et 1 par 10. Appliquons-la à la suite de Morse M

$$\begin{array}{lcccccccccccc} M = & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & \ldots \\ \sigma M = & (01) & (10) & (10) & (01) & (10) & (01) & (01) & (10) & (10) & (01) & (01) & (10) & \ldots \end{array}$$

On constate que $\sigma M = M$. La suite de Morse est point fixe de la substitution.

La substitution ici considérée est une 2-substitution. Une g-substitution est une substitution où on remplace chaque symbole d'un alphabet fini $\sum$ par un mot appartenant à $\sum^g$.

Définition 4. Soit $\mathbf{F}_2$ le corps à 2 éléments. Une suite $S \in \mathbf{F}_2{}^{\mathbf{N}}$ peut être considérée comme une série de Laurent formelle

$$S = (\varepsilon_n) = \sum_{n=0}^{\infty} \varepsilon_n X^n \in \mathbf{F}_2\,((X))\,.$$

Comme $\mathbf{F}_2((X))$ est un corps, on pourra additionner et multiplier les suites. En particulier

$$(\varepsilon_n) + (\delta_n) = (\varepsilon_n + \delta_n)$$
$$(\varepsilon_n)(\delta_n) = (\varepsilon_0\delta_n + \varepsilon_1\delta_{n-1} + \ldots + \varepsilon_n\delta_0)\,.$$

On dit que $S \in \mathbf{F}_2{}^{\mathbf{N}} \subset \mathbf{F}_2((X))$ est algébrique (sur $\mathbf{F}_2(X)$) si il existe des polynômes $a_\nu, a_{\nu-1}, \ldots, a_0 \in \mathbf{F}_2[X]$, non tous nuls, tels que

$$a_\nu S^\nu + a_{\nu-1} S^{\nu-1} + \ldots + a_0 = 0$$

Considérons en particulier l'équation quadratique

$$(1+X)^3 S^2 + (1+X)^2 S + X = 0\,.$$

On vérifie sans peine qu'elle admet deux solutions $S = M$ (suite de Morse) et $S = M + (1+X)^{-1}$. Cette seconde solution s'obtient à partir de M en échangeant les 0 et les 1. Elle a donc la même structure et nous l'appellerons encore suite de Morse. D'une façon générale, nous ne nous intéresserons pas au nom des lettres constitutives. On parlera donc de la suite de Morse construite sur l'alphabet $\{a, b\}$ par exemple.

Avant de formuler notre résultat principal, nous pensons intéressant de signaler deux suites algébriques qui nous semblent remarquables.

Exemple 1 (Rudin [14], Shapiro [15]). Soit $S = (r_n)$ l'une des 2 solutions de l'équation quadratique

$$(1+X)^5 S^2 + (1+X)^4 S + X^2 = 0\,.$$

La suite S est celle qu'ont trouvée Rudin et Shapiro indépendamment l'un de l'autre et qui vérifie l'inégalité

$$\forall N \geqslant 1\,, \quad \forall \theta \in \mathbf{R}\,, \quad \Big| \sum_{n=1}^{N} (-1)^{r_n} e^{2i\pi n\theta} \Big| \leqslant 5\sqrt{N}\,.$$

Exemple 2 (Baum et Sweet [1]). La seule solution de l'équation cubique

$$S^3 + XS + 1 = 0$$

possède la remarquable propriété suivante. Son développement en fraction continue (dans $\mathbf{F}_2((X))$) est à quotients partiels bornés. (Dans le corps

des réels, on conjecture que tout nombre algébrique de degré 3 au moins est à quotients partiels non bornés.)

Dans ce qui suit, nous aurons à considérer des corps à $q = p^\mu$ éléments (p premier, $\mu \geqslant 1$ entier). On dira comme précédemment que $S \in \mathbf{F}_q{}^{\mathbf{N}}$ est algébrique si $S \in \mathbf{F}_q((X))$ est algébrique sur $\mathbf{F}_q(X)$.

§ 3. Le résultat

Soient Ξ et Ξ' deux alphabets finis et soient $T = (t_n) \in \Xi^N$, $T' = (t_n') \in \Xi'^N$. On dit que T' est une image de T si il existe une application $\alpha: \Xi \to \Xi'$ telle que pour tout n, $\alpha(t_n) = t_n'$.

Théorème 1. *Soit Ξ un alphabet fini non vide. Soit $T \in \Xi^N$ et soit p un nombre premier. Les trois conditions suivantes sont équivalentes.*

(i) *Il existe $q = p^\mu$ tel que T soit l'image d'un élément algébrique de $\mathbf{F}_q((X))$;*

(ii) *T est l'image d'une suite engendrée par un p-automate;*

(iii) *T est l'image d'un point fixe d'une p-substitution.*

L'équivalence entre (ii) et (iii) était connue de Cobham [3]. Dans un autre article, Cobham [2] établit que si une suite est engendrée à la fois par un g_1-automate et par un g_2-automate, alors elle est périodique à partir d'un certain rang pourvu que g_1 et g_2 soient multiplicativement indépendants. Ce résultat se traduit donc par le corollaire suivant.

Corollaire. *Soient $q_1 = p_1^{\nu 1}$ et $q_2 = p_2^{\nu 2}$ où $p_1 \neq p_2$ (premiers). Soit (ε_n) une suite infinie d'entiers $0 \leqslant \varepsilon_n < \min\{q_1, q_2\}$. Si*

$$S_1 = \sum_{n=0}^{\infty} \varepsilon_n X^n \in \mathbf{F}_{q_1}((X))$$

est algébrique sur $\mathbf{F}_{q_1}(X)$ et si

$$S_2 = \sum_{n=0}^{\infty} \varepsilon_n X^n \in \mathbf{F}_{q_2}((X))$$

est algébrique sur $\mathbf{F}_{q_2}(X)$, alors S_1 et S_2 sont tous deux rationnels.

Ainsi, si un élément est algébrique irrationnel dans une base, il est transcendant dans toute base indépendante (comparer avec le problème 1 du paragraphe 1). Il serait intéressant d'élargir le champ d'application du résultat précédent de façon à pouvoir l'appliquer au corps **R**. Dans cet ordre d'idée, il faut signaler le résultat suivant obtenu indépendamment par Dekking [5], K. Kubota [9] et A. van der Poorten [17] employant une méthode de K. Mahler.

THÉORÈME 2. *Le nombre de Morse*

$$\xi = \sum_{n=0}^{\infty} \frac{m_n}{2^n}$$

est transcendant.

La méthode employée pour établir ce résultat devrait pouvoir permettre de montrer que si la suite $S = (\varepsilon_0, \varepsilon_1, \varepsilon_2, ...)$ est engendrée par un g-automate, alors $\sum_{n=0}^{\infty} \varepsilon_n g^{-n}$ est transcendant. Ceci répondrait à la conjecture énoncée au premier paragraphe.

§ 4. APPENDICE: SUITE DE MORSE PONDÉRÉE ET NOMBRES DE PISOT

Soit $c = (c_n)$ une suite infinie de nombres réels. A l'entier $n \geqslant 0$, on associe le nombre

$$f_c(n) = \exp 2i\pi \sum_{k=0}^{\infty} e_k(n)\, c_k ,$$

où $e_k(n)$ est la k^{e} décimale binaire de n. On peut alors montrer que la suite f_c admet une corrélation:

$$\forall\, l \in \mathbf{Z},\ \lim_{N \to \infty} \frac{1}{N} \sum_{n=1}^{N} \overline{f_c(n)}\, f_c(n+l) = \gamma_c(l) \text{ existe.}$$

Cette corrélation γ_c est transformée de Fourier d'une mesure positive bornée Λ_c

$$\gamma_c(l) = \int_0^1 (\exp 2i\pi l x)\, \Lambda_c(dx) .$$

Soit $\theta \geqslant 1$ un nombre réel. Considérons la suite $c = (\theta^n)$ à laquelle correspondra la mesure Λ_c notée Λ_θ.

THÉORÈME 3. *Si θ est un nombre de Pisot, alors Λ_θ est une mesure atomique. Si θ n'est pas un nombre de Pisot, alors Λ_θ est une mesure continue, purement singulière.*
(Voir [4], [11], [12], [13].)

Ce type de résultat montre qu'une étude spectrale des suites précédemment étudiées est possible. T. Kamae est en train de l'entreprendre et ses résultats seront publiés ultérieurement.

BIBLIOGRAPHIE

[1] BAUM, L. and M. SWEET. Continued fractions of algebraic power series in characteristic 2. *Ann. Math. 103* (1976), 593-610.

[2] COBHAM, A. On the base-dependance of sets of numbers recognizable by finite automata. *Math. Syst. Theory 3* (1969), 186-192.

[3] —— Uniform Tag sequences. *Math. Syst. Theory 6* (1972), 164-192.

[4] COQUET, J., T. KAMAE et M. MENDES FRANCE. Sur la mesure spectrale de certaines suites arithmétiques. *Bull. Soc. Math. France 105* (1977), 369-384.

[5] DEKKING, M. Transcendence du nombre de Thue-Morse. *Comptes Rendus Ac. Sc. Paris 285 (A)* (1977), 157-160.

[6] DELLACHERIE, C. Nombres au hasard (de Borel à Martin Loff). *Gazette des Math., Soc. Math. France 11* (1978), 23-58.

[7] EILENBERG, S. *Automata, Languages and Machines, vol. A.* Academic Press, 1974.

[8] KOLMOGOROFF, A. N. On tables of random numbers. *Sankhyá 25* (1963), 369-376.

[9] KUBOTA, K. An application of Kronecker's theorem to transcendance theory. *Séminaire théorie des nombres de Bordeaux*, 1975-76, exposé 25.

[10] MARTIN-LÖF, P. The definition of random sequences. *Information and Control 9* (1969), 602-619.

[11] MENDES FRANCE, M. Deux remarques concernant l'équirépartition. *Acta Arith. 14* (1968), 163-167.

[12] —— Nombres normaux. Applications aux fonctions pseudo-aléatoires. *Jour. Anal. Math. Jerusalem 20* (1967), 1-56.

[13] QUEFFELEC, M. Mesures spectrales associées à certaines suites arithmétiques. *Bull. Soc. Math. France 107* (1977), 385-421.

[14] RUDIN, W. Some theorem on Fourier coefficients. *Proc. Amer. Math. Soc. 10* (1937), 413-417.

[15] SHAPIRO, H. S. *Extremal problems for polynomials and power series.* Thèse MIT 1951.

[16] SCHNORR, C. P. *Zufälligkeit und Wahrscheinlichkeit.* Lecture Notes in Math. 218, Springer Verlag, 1970.

[17] VAN DER POORTEN, A. Propriétés arithmétiques et algébriques de fonctions satisfaisant une classe d'équations fonctionnelles. *Séminaire Théorie des Nombres de Bordeaux*, 1974-75, exposé 7.

(Reçu le 3 janvier 1980)

Michel Mendes France

UER Mathématiques et Informatique
Université Bordeaux I
351, Cours de la Libération
F-33405 Talence