Sur la complexité des nombres algébriques

On the complexity of algebraic numbers

Boris Adamczewski [a] Yann Bugeaud [b] Florian Luca [c]

[a] *Laboratoire de Recherche en Informatique, UMR 8623 Bât. 490 Université Paris-Sud 91405 Orsay, France*
[b] *Université Louis Pasteur, UFR de mathématiques, 7, rue René Descartes, 67084 Strasbourg, France*
[c] *Instituto de Matemáticas, UNAM, Campus Morelia, C. P. 58180, Morelia, Michoacán, México*

Abstract

Let $b \geq 2$ be an integer. We prove that real numbers whose b-ary expansion satisfies some given, simple, combinatorial condition are transcendental. This implies that the b-ary expansion of any algebraic irrational number cannot be generated by a finite automaton. *To cite this article: B. Adamczewski, Y. Bugeaud, F. Luca, C. R. Acad. Sci. Paris, Ser. I 336 (2004).*

Résumé

Pour tout entier b supérieur ou égal à 2, nous prouvons la transcendance des nombres réels dont le développement b-adique vérifie une condition combinatoire donnée. Nous en déduisons que le développement b-adique d'un nombre algébrique irrationnel ne peut être engendré par un automate fini. *Pour citer cet article : B. Adamczewski, Y. Bugeaud, F. Luca, C. R. Acad. Sci. Paris, Ser. I 336 (2004).*

Au long de cette Note, b désigne un entier supérieur ou égal à 2. S'il est bien connu que, pour tout entier $b \geq 2$, le développement b-adique d'un nombre rationnel est ultimement périodique, que peut-on dire sur la régularité du développement d'un irrationnel algébrique ? Cette question fut posée pour la première fois par É. Borel [5], qui conjecture qu'un tel développement doit satisfaire à certaines lois suivies par un nombre tiré au hasard. Plus précisément, il est attendu que tout irrationnel algébrique soit un nombre normal. Rappelons qu'un nombre réel θ est dit *normal en base* b si pour tout entier n, chacun des b^n mots de longueur l sur l'alphabet $\{0, 1, \ldots, b-1\}$ apparît dans le développement b-adique de θ la fréquence $1/b^n$. Bien que cette conjecture soit considérée comme totalement hors d'atteinte, il est cependant possible d'obtenir des informations non triviales sur la complexité du développement b-adique d'un nombre réel irrationnel algébrique, mesurée au moyen d'une *fonction de complexité* p, qui compte le

Email addresses: Boris.Adamczewski@lri.fr (Boris Adamczewski), bugeaud@math.u-strasbg.fr (Yann Bugeaud), fluca@matmor.unam.mx (Florian Luca).

nombre $p(n)$ de facteurs dinstincts de longueur n qui y apparaissent. Ainsi, S. Ferenczi et C. Mauduit [7] ont prouvé, grâce à une reformulation astucieuse d'un théorème de D. Ridout [12], la transcendance des nombres réels dont le développement en base entière est par exemple une suite sturmienne. Rappelons que les suites sturmiennes sont les suites non ultimement périodiques de complexité minimale, c'est-à-dire les suites vérifiant $p(n) = n + 1$ pour tout entier positif n (cf. [11]). Plusieurs auteurs ont ensuite utilisé la condition combinatoire de [7] afin d'exhiber de nouveaux exemples de nombres transcendants de faible comblexité (voir [3], [4] et [13]).

En 1965, J. Hartmanis and R. E. Stearns [8] ont proposé une approche différente de la notion de complexité pour les nombres réels en développant l'aspect quantitatif de la notion de calculabilité introduite par A. M. Turing [17]. Ainsi, un nombre réel α est dit calculable en temps $T(n)$ s'il existe une machine de Turing (à plusieurs rubans) capable de déterminer le n-ième terme de son développement binaire en (au plus) $T(n)$ opérations. Les nombres réels les plus simples en ce sens, c'est-à-dire pour lesquels on peut choisir $T(n) = O(n)$, sont dits calculables en temps réel. Les nombres rationnels fournissent évidemment de tels exemples. Le problème de Hartmanis-Stearns, auquel une réponse négative est attendue, est le suivant : existe-t-il des nombres algébriques irrationnels calculables en temps réel ? En 1988, J. H. Loxton et A. J. van der Poorten [9] ont annoncé l'avoir résolu pour une classe particulière de machines de Turing. Précisément, leur résultat affirme que le développement b-adique d'un nombre algébrique irrationnel ne peut être automatique (*i.e.*, engendré par un automate fini). La démonstration proposée, qui repose sur une méthode introduite par K. Mahler [10], s'est malheureusement révélée incomplète (voir [18]). En outre, la condition combinatoire donnée par S. Ferenczi et C. Mauduit est loin d'être suffisante pour prouver ce résultat.

L'objet de la présente Note est de raffiner la condition de Ferenczi–Mauduit en la remplaçant par une condition combinatoire beaucoup plus souple (la condition $(*)$) qui permet d'obtenir, même si nous n'en donnerons pas la démonstration complète ici, la transcendance des nombres irrationnels dont le développement b-adique est de complexité sous-linéaire (Téorème 2) et donc *a fortiori* des nombres réels automatiques (Corollaire 3).

Soit $\mathcal{A}$ un ensemble fini. Nous rappelons que si W est un mot fini sur $\mathcal{A}$, alors $|W|$ désigne la longueur de W, c'est-à-dire le nombre de lettres qui le composent. Si p est un entier positif, alors W^p désigne le mot $W \dots W$ (concaténation p fois répétée du mot W). Plus généralement, si x est un nombre rationnel W^x désigne le mot $W^{\lfloor p \rfloor} W'$, où W' est le préfixe de W de longueur $\lceil (p - \lfloor p \rfloor)|W| \rceil$. Ici, $\lfloor y \rfloor$ et $\lceil y \rceil$ désignent, respectivement, la partie entière et la partie entière supérieure du réel y. Soit $\mathbf{a} = (a_n)_{n \geq 1}$ une suite non ultimement périodique d'éléments de $\mathcal{A}$. La suite $\mathbf{a}$ satisfait à la condition $(*)$ s'il existe un nombre réel $w > 1$ et deux suites de mots finis $(U_n)_{n \geq 1}$, $(V_n)_{n \geq 1}$ tels que :

(i) $\forall n \geq 1$, $U_n V_n^w$ soit un préfixe de la suite $\mathbf{a}$;
(ii) La suite $\left(\frac{|U_n|}{|V_n|} \right)_{n \geq 1}$ est bornée ;
(iii) La suite $|V_n|$ est strictement croissante.

Théorème 1 *Soit $\mathbf{a} = (a_n)_{n \geq 1}$ une suite à valeurs dans $\{0, 1, \dots, b-1\}$ satisfaisant à la condition $(*)$. Alors, le nombre réel $\alpha := \sum_{k=1}^{+\infty} \frac{a_k}{b^k}$ est transcendant.*

Nous donnons ici une démonstration complète du Théorème 1. Elle repose sur le théorème des sous-espaces de W. M. Schmidt [15] (voir aussi [16]), et plus particulièrement sur sa généralisation p-adique, obtenue par H. P. Schlickewei [14].

La la condition $(*)$ est en particulier vérifiée par toute suite dont la fonction de complexité vérifie $p(n) = O(n)$. Nous établissons en fait un résultat sensiblement plus fort.

Théorème 2 *La fonction de complexité du développement b-adique d'un nombre algébrique irrationnel vérifie*

$$\liminf_{n\to\infty} \frac{p(n)}{n} = +\infty.$$

Puisque d'après [6] la fonction de complexité d'une suite automatique vérifie $p(n) = O(n)$, nous obtenons donc le résultat annoncé dans [9], par une méthode complètement différente.

Corollaire 3 *Un nombre algébrique irrationnel ne peut être automatique.*

Nous donnerons d'autres applications du Théorème 1 dans un travail ultérieur [2]. Notons d'ores et déjà que lon peut montrer que la condition $(*)$ est vérifié par de nombreuses classes de suites, en particulier par tous les points fixes binaires (non triviaux) de morphismes de monoïde libre. Nous étudierons le cas des bases non entières (en particulier, Pisot et Salem) ainsi que le cas du développement de Hensel des nombres p-adiques, en reprenant les idées de [1], qui se combinent très bien avec les celles de la présente note.

Démonstration du Théorème 1. Considérons une suite $\mathbf{a} = (a_n)_{n\geq 1}$ à valeurs dans $\{0, 1, \ldots, b-1\}$ et satisfaisant à la condition $(*)$. Nous supposons ainsi fixés les paramètres w, $(U_n)_{n\geq 1}$ et $(V_n)_{n\geq 1}$. Posons également, $r_n = |U_n|$ et $s_n = |V_n|$. Notons $\alpha = \sum_{k=1}^{+\infty} a_k/b^k$ le nombre réel dont le développement b-adique est donné par la suite $\mathbf{a}$. Pour tout entier n, considérons le nombre rationnel $\alpha_n = \sum_{k=1}^{+\infty} b_k^{(n)}/b^k$, où $b_k^n = a_k$ si $k \leq r_n + ws_n$ et $b_k^{(n)} = b_{k+s_n}^{(n)}$ si $k \geq r_n$. La suite $(b_k^{(n)})_{k\geq 1}$ est ultimement périodique de pré-période U_n et de période V_n. Il existe donc un entier p_n tel que l'on ait

$$\alpha_n = \frac{p_n}{b^{r_n}(b^{s_n}-1)} \quad \text{et} \quad |\alpha - \alpha_n| < \frac{1}{b^{r_n+ws_n}},$$

cette inégalité découlant de la condition (i) de $(*)$.

Supposons α algébrique, et considérons les six formes linéaires suivantes, en trois variables et à coefficients algébriques : $L_{1,\infty}(x,y,z) = \alpha x + \alpha y + z$, $L_{2,\infty}(x,y,z) = y$, $L_{3,\infty}(x,y,z) = z$, $L_{1,b}(x,y,z) = x$, $L_{2,b}(x,y,z) = y$ et $L_{3,b}(x,y,z) = z$. Les formes $L_{1,\infty}$, $L_{2,\infty}$ et $L_{3,\infty}$, d'une part, et $L_{1,b}$, $L_{2,b}$ et $L_{3,b}$, d'autre part, sont lineairement independantes. Notons $\mathcal{S}$ l'ensemble des diviseurs premiers de b. Pour tout entier n, il vient :

$$\left|L_{1,\infty}(b^{r_n+s_n}, -b^{r_n}, -p_n)\right| = |\alpha(b^{r_n}(b^{s_n}-1)) - p_n| < \frac{1}{b^{(w-1)s_n}}, \quad \left|L_{2,\infty}(b^{r_n+s_n}, -b^{r_n}, -p_n)\right| = b^{r_n}$$

et

$$\left|L_{3,\infty}(b^{r_n+s_n}, -b^{r_n}, -p_n)\right| = p_n.$$

De même, en notant $|x|_p$ la valeur absolue p-adique de x, on obtient

$$\prod_{p\in\mathcal{S}} \left|L_{1,b}(b^{r_n+s_n}, -b^{r_n}, -p_n)\right|_p = \frac{1}{b^{r_n+s_n}}, \quad \prod_{p\in\mathcal{S}} \left|L_{2,b}(b^{r_n+s_n}, -b^{r_n}, -p_n)\right|_p = \frac{1}{b^{r_n}}$$

et

$$\prod_{p\in\mathcal{S}} \left|L_{3,b}(b^{r_n+s_n}, -b^{r_n}, -p_n)\right|_p \leq 1.$$

Les estimations ci-dessus entraînent

$$\prod_{i=1}^{3} \left|L_{i,\infty}(b^{r_n+s_n}, -b^{r_n}, -p_n)\right| \times \prod_{i=1}^{3} \left(\prod_{p\in\mathcal{S}} \left|L_{i,b}(b^{r_n+s_n}, -b^{r_n}, -p_n)\right|_p\right) \ll \frac{1}{b^{(w-1)s_n}},$$

où $\ll$ désigne la notation classique de Vinogradov. Comme l'hypothèse (ii) de $(*)$ assure lexistence d'un $\delta > 0$ tel que $b^{(w-1)s_n} > (b^{r_n+s_n})^{\delta}$, on obtient

$$\prod_{i=1}^{3} \left| L_{i,\infty}(b^{r_n+s_n}, -b^{r_n}, -p_n) \right| \times \prod_{i=1}^{3} \left(\prod_{p \in \mathcal{S}} \left| L_{i,b}(b^{r_n+s_n}, -b^{r_n}, -p_n) \right|_p \right) \ll ||(b^{r_n+s_n}, -b^{r_n}, -p_n)||_{\infty}^{-\delta}.$$

Le théorème des sous-espaces impose alors aux vecteurs de la suite $(b^{r_n+s_n}, -b^{r_n}, -p_n)_{n \geq 1}$ d'appartenir à une union finie de sous-espaces vectoriels propres de $\mathbb{Q}^3$. En particulier, une infinité de ces vecteurs doivent appartenir a un sous-espace vectoriel de $\mathbb{Q}^3$ de dimension 2 sur $\mathbb{Q}$. Il existe donc un vecteur non nul $(x_0, y_0, z_0) \in \mathbb{Q}^3$ et une infinité d'entiers n vérifiant

$$x_0 - y_0 \frac{b^{r_n}}{b^{r_n+s_n}} - z_0 \frac{p_n}{b^{r_n+s_n}} = 0.$$

En passant à la limite suivant cette sous-suite, on obtient

$$x_0 = z_0 \alpha.$$

Par hypothèse, **a** n'est pas ultimement périodique, donc α est irrationnel. Il vient alors $z_0 = 0$, puis $x_0 = y_0 = 0$, ce qui est une contradiction. $\square$

Remerciements

Y. Bugeaud et F. Luca ont bénéficié du projet conjoint ECOS Nord – CONACyT, France-Mexico M02-M01.

Références

[1] B. Adamczewski. Transcendance "à la liouville" de certains nombres réels. *C. R. Acad. Sci. Paris*, 338 :511–514, 2004.

[2] B. Adamczewski and Y. Bugeaud. On the complexity of algebraic numbers. Soumis, 2004.

[3] B. Adamczewski and J. Cassaigne. On the transcendence of real numbers with a regular expansion. *J. Number Theory*, 103 :27–37, 2003.

[4] J.-P. Allouche and L. Q. Zamboni. Algebraic irrational binary numbers cannot be fixed points of non-trivial constant length or primitive morphisms. *J. Number Theory*, 69 :119–124, 1998.

[5] É. Borel. Sur les chiffres décimaux de $\sqrt{2}$ et divers problèmes de probabilités en chaîne. *C. R. Acad. Sci. Paris*, 230 :591–593, 1950.

[6] A. Cobham. Uniform Tag Sequences. *Math. Systems Theory*, 6 :164–192, 1972.

[7] S. Ferenczi and C. Mauduit. Transcendence of numbers with a low complexity expansion. *J. Number Theory*, 67 :146–161, 1997.

[8] J. Hartmanis and R. E. Stearns. On the computational complexity of algorithms. *Trans. Amer. Math. Soc.*, 117 :285–306, 1965.

[9] J. H. Loxton and A. J. van der Poorten. Arithmetic properties of automata: regular sequences. *J. Reine Angew. Math.*, 392 :57–69, 1988.

[10] K. Mahler. Arithmetische Eigenschaften der Lösungen einer Klasse von Funktionalgleichungen. *Math. Ann.*, 101 :342–366, 1929. Corrigendum 103 :532, 1930.

[11] M. Morse and G. A. Hedlund. Symbolic dynamics II. Sturmian trajectories. *Amer. J. Math.*, 62 :1–42, 1940.

[12] D. Ridout. Rational approximations to algebraic numbers. *Mathematika*, 4 :125–131, 1957.

[13] R. N. Risley and L. Q. Zamboni. A generalization of Sturmian sequences: combinatorial structure and transcendence. *Acta Arith.*, 95 :167–184, 2000.

[14] H. P. Schlickewei. The p-adic Thue-Siegel-Roth-Schmidt theorem. *Arch. Math. (Basel)*, 29(3) :267–270, 1977.

[15] W. M. Schmidt. Norm form equations. *Ann. of Math. (2)*, 96 :526–551, 1972.

[16] W. M. Schmidt. *Diophantine approximation*, volume 785 of *Lecture Notes in Mathematics*. Springer, Berlin, 1980.

[17] A. M. Turing. On computable numbers, with an application to the Entscheidungsproblem. *Proc. Lond. Math. Soc.*, 42 :230–265, 1936–37. Corrigendum 43 :544–546, 1937.

[18] M. Waldschmidt. Un demi-siècle de transcendance. In *Development of mathematics 1950–2000*, pages 1121–1186. Ed. J.-P. Pier, Birkhäuser, Basel, 2000.