Numération : mathématiques et informatique

Rencontre organisée par :
Boris Adamczewski, Anne Siegel and Wolfgang Steiner

23-27 mars 2009

Tanguy Rivoal

On the binary expansion of irrational algebraic numbers

Vol. 1, n° 1 (2009), p. 55-60.

<http://acirm.cedram.org/item?id=ACIRM_2009__1_1_55_0>

Centre international de rencontres mathématiques
U.M.S. 822 C.N.R.S./S.M.F.
Luminy (Marseille) France

Actes des rencontres du C.I.R.M.
Vol. **1** n° 1 (2009) 55-60

On the binary expansion of irrational algebraic numbers

Tanguy Rivoal

These notes correspond to my talk given during the conference "Numeration: Mathematics and Computer Science" at the CIRM (23 to 27 March 2009). I warmly thank the organisers Boris Adamczewski, Anne Siegel and Wolfgang Steiner for their invitation.

1. Introduction

My talk was centered on some recent results concerning the number of occurences of the digit 1 in the binary expansion of a real number x up to the n-th digits. I first need to introduce some notation. For any non-negative integer m, let $B(m)$ be the number of 1 in the (finite) binary expansion of m. For any non-negative real number x written in base 2 as $x = (x_{-p}x_{-p+1}\cdots x_0, x_1x_2x_3\ldots)_2$, let $B_n(x) = \#\{j \leq n : x_j = 1\}$. Of course, the counting function $B_n(x)$ is not well defined when $x = n/2^k$ (n, k non-negative integers), which has two possible binary expansions, a "finite" one (ending with infinitely many 0s) and an "infinite" one with (ending with infinitely many 1s). We choose the finite expansion, in which case we have

$$B_n(x) = B_0(x) = B(x)$$

for any non-negative integer x.

A classical problem is to estimate the asymptotic behavior of $B_n(x)$ as $n \to +\infty$, given x. Obviously, $B_n(x) \to +\infty$ for any irrational number. But at what speed? Since digits of a real number can be viewed as the realisation of independent Bernoulli random variables with respect to Lebesgue measure, the law of large numbers shows that

$$B_n(x) = \frac{n}{2} + o(n) \tag{1.1}$$

for almost all real numbers. This point of view was first developed by Borel in his celebrated paper [4], where he coined the expression "simple normal number in base 2" for those real numbers x which satisfy (1.1). (Normal numbers in base 2 are those for which any block of digits of length $q \geq 1$ appears asymptotically with the frequency 2^{-q} and absolutely normal are those for which any block of digits of length $q \geq 1$ in base b appears asymptotically with the frequency b^{-q} for any base $b \geq 2$.)

Proving the simple normality of a given number in a given base, let alone its absolute normality, is a notoriously difficult problem, except for uninteresting numbers like $2/3 = (0.1010101010\ldots)_2$. Champernowne was the first to construct an explicit irrational number, namely $C := 0.123456789101112\ldots$, normal in base 10 –the integers written in base 10 are concatenated. For any given $b \geq 2$, an obvious change in the definition of C provides a normal number in base b. Sierpiński provided an algorithm to construct an absolutely normal number, even though a simpler number is yet to be found. It is unfortunate that, so far, even the simple normality in base 2 of classical numbers like $e, \log(2), \pi, \zeta(3)$ or algebraic irrational numbers is still unknown.

However, very recently, some progresses have been made on these questions in the case of algebraic irrational numbers and I now describe them.

Text presented during the meeting "Numeration: mathematics and computer science" organized by Boris Adamczewski, Anne Siegel and Wolfgang Steiner. 23-27 mars 2009, C.I.R.M. (Luminy).
2000 *Mathematics Subject Classification.* 11K16, 11J68, 68R01.
Key words. Binary expansions, algebraic numbers, diophantine approximation.

2. Results using diophantine tools

Let us start with some easy remarks. An irrational number x is said to have a finite irrationality exponent μ if the equation

$$\left|x-\frac{p}{q}\right| \geq \frac{1}{q^{\mu}} \tag{2.1}$$

holds for all $p,q\in\mathbb{Z}$, $q\gg 1$. The irrationality exponent of x, noted $\mu(x)$, is the infimum of such μ if there exist some, and is set to $+\infty$ otherwise. Using the pigeon principle, Dirichlet proved that for any irrational numbers, we have $\mu(x)\geq 2$, but this is also a consequence of the theory of continued fractions. Furthermore, for almost all real numbers x, we have $\mu(x)=2$.

Proposition 1. *For any $\varepsilon>0$ and any irrational number $x>0$, we have*

$$B_n(x) \geq \frac{\log(n)}{\log(\mu(x)+\varepsilon)}+\mathcal{O}(1). \tag{2.2}$$

This Proposition holds even if $\mu(x)=+\infty$, in which case one must understand that $B_n(x)\gg 1$ which is plain. The proof is simple and instructive.

Proof. We assume that $x\in(0,1)$ and that $\mu(x)<+\infty$. We have

$$x=\sum_{k=1}^{\infty}\frac{1}{2^{m_k}}=\frac{p_n}{q_n}+\sum_{k=n+1}^{\infty}\frac{1}{2^{m_k}},$$

where $q_n=2^{m_n}$ and $(m_k)_{k\geq 1}$ is a strictly increasing sequence of positive integers.

On the one hand,

$$\left|x-\frac{p_n}{q_n}\right| \leq \frac{1}{2^{m_{n+1}-1}} \tag{2.3}$$

because $m_{k+1}>m_k$.

On the other hand, by hypothesis, for any $\varepsilon>0$, we get

$$\left|x-\frac{p_n}{q_n}\right| \geq \frac{1}{q_n^{\mu(x)+\varepsilon}}=\frac{1}{2^{m_n(\mu(x)+\varepsilon)}} \tag{2.4}$$

for $n\gg_{\varepsilon,x} 1$.

Comparing (2.3) and (2.4), we immediately get $m_{n+1}\leq(\mu(x)+\varepsilon)m_n+1$ for $n\gg_{\varepsilon,x}1$, hence

$$m_n\leq c(\varepsilon,x)(\mu(x)+\varepsilon)^n$$

for some constant $c(\varepsilon,x)>0$.

To conclude, it remains to see that

$$\begin{aligned} B_n(x) &= \#\{k : m_k\leq n\} \\ &\geq \#\{k : c(\varepsilon,x)(\mu(x)+\varepsilon)^k\leq n\} \\ &\geq \frac{\log(n)}{\log(\mu(x)+\varepsilon)}+\mathcal{O}(1). \end{aligned}$$

□

It is known that the numbers $e,\pi,\log(2),\zeta(3)$ all have finite irrationality exponent and thus Proposition 1 can be applied to them: it is sad to observe that this is the best known result concerning the asymptotic behavior of their binary digits, up to the value of the constant dividing $\log(n)$.

The reader can see that (2.4) does not really use the specific form of $q_n=2^{m_n}$, which is not "detected" when we use the irrationality exponent. Hence a first improvement over (2.2) would occur if it was possible to decrease $\mu(x)$. (Of course, the resulting irrationality measure would hold only for some denominators q with specific arithmetic properties.) This turns out to be possible for algebraic irrational numbers, by means of a deep theorem due to Ridout [8].

Theorem 1 (Ridout)**.** *Let ξ be a real number and S_1, S_2 two finite set of prime numbers (possibly empty). Let us assume that there exists $\varepsilon > 0$ such that the inequality*

$$\prod_{w_1 \in S_1} |p|_{w_1} \cdot \prod_{w_2 \in S_2} |q|_{w_2} \cdot \left| \xi - \frac{p}{q} \right| < \frac{1}{q^{2+\varepsilon}}$$

has infinitely many solutions p/q, with $(p,q) = 1$. Then ξ is transcendental over $\mathbb{Q}$.

Here, $|n|_w = w^{-v_w(n)}$. When $S_1 = S_2 = \emptyset$, the statement reduces to the famous Roth's Theorem [11] that $\mu(\alpha) = 2$ for all algebraic irrational numbers α.

As an application, we immediately see that for any algebraic irrational number α and for any $\varepsilon > 0$, the inequality

$$\left| \alpha - \frac{p}{2^m} \right| \geq \frac{1}{2^{m(1+\varepsilon)}} \tag{2.5}$$

holds for all $p, m \in \mathbb{Z}$, $m \gg_\varepsilon 1$. Using (2.5) instead of (2.4) during the proof of Proposition 1, we get the following

Proposition 2. *For any algebraic irrational number $\alpha > 0$ and any $\varepsilon > 0$, we have*

$$B_n(\alpha) \geq \frac{\log(n)}{\log(1+\varepsilon)} + \mathcal{O}(1). \tag{2.6}$$

Eq. (2.6) is not such a big improvement over Eq. (2.2) because only the constant is affected and not $\log(n)$. We see that if it was possible to replace q^ε by any function of slower growth, like a power of $\log(q)$, then the same argument would now improve the term $\log(n)$. Unfortunately, an improvement of Ridout's Theorem is not yet available for even at least one algebraic number. Proving a Ridout-type theorem for transcendental number is even more elusive, even though results in this direction were recently obtained by the author [10] for the numbers $\log(r)$ with $r \in \mathbb{Q}$ close to 1.

However, we will see in the next section that an argument of a different nature provides a dramatic improvement of Proposition 2. Before this, let us conclude the present section with the following remark. Roth and Ridout's Theorems have been generalised by Schmidt and then Schlickewei, culminating with the *Subspace Theorem*. We won't state it here but will quote one very important consequence of it.

Theorem 2 (Adamczewski-Bugeaud [1])**.** *Given a real number $x = (0.a_1a_2a_3\ldots)_b$ written in base $b \geq 2$, let us define the complexity function $p(x,b,n) := \#\{(a_j, a_{j+1}, \ldots, a_{j+n-1}), j \geq 1\}$. Then for any algebraic irrational number α, we have*

$$\lim_{n \to +\infty} \frac{p(\alpha, b, n)}{n} = +\infty.$$

Since the complexity of a sequence of digits generated by a finite automaton does not grow faster than linearly, this result implies that the digits of an algebraic irrational number cannot be generated by a finite automaton. This is the first qualitative result beyond the non-periodicity of digits, which is not specific to algebraicity but to irrationality. Finally, note that if x is normal in base b, then $p(x,b,n) = b^n$, but the converse is not necessarily true.

3. A combinatorial approach

In 2004, Bailey, Borwein, Crandall and Pomerance [3] proved the following theorem, which is a major improvement over Proposition 2.

Theorem 3 (BBCP)**.** *For any irrational algebraic number $\alpha > 0$, we have*

$$B_n(\alpha) \geq (2a_d)^{-1/d} n^{1/d} (1 + o(1)) \tag{3.1}$$

as $n \to +\infty$, where d is the degree of the minimal polynomial P of α and $a_d \geq 1$ is the dominant term of P (with coefficients relatively prime in their set).

In particular, we get the lower bound $B_n(\sqrt{2}) \geq \sqrt{\frac{n}{2}}\,(1+o(1))$. The proof of (3.1) given in [3] is rather involved and will not be reproduced here. Given the binary expansion $\alpha = \sum_n a_n 2^{-n}$, the problem is to control the carries when one tries to transform the identity

$$\alpha^k = \sum_n \left(\sum_{i_1+\cdots+i_k=n} a_{i_1}\cdots a_{i_k} \right) \frac{1}{2^n}$$

into a valid binary expansion for α^k. This is obviously a difficult problem, which they succeed to solve (partially) by elementary arguments, except at one point where Roth's Theorem is used to get the inequality (2.4) with $\mu(x) = 2$. It seems that using Ridout's Theorem instead of Roth's Theorem enables one to increase the constant $(2a_d)^{-1/d}$ to $a_d^{-1/d}$ in (3.1). In the other direction, it is also possible to use Liouville's Theorem (i.e., that (2.4) holds with d instead of $\mu(x) = 2$) to get the worse constant $(da_d)^{-1/d}$; this presents the advantage that the whole proof of the lower bound analogous to (3.1) is completely elementary ([1]).

In the rest of these notes, I present a sketch of the proof of a slightly better inequality than (3.1) but which holds for a smaller class of algebraic numbers.

Theorem 4. *Let $\alpha > 0$ be an irrational algebraic of degree d whose minimal polynomial $P(X) = \sum_{j=0}^{d} a_j X^j$ is such that $a_0 \leq 0$ and $a_j \geq 0$ for $j \geq 1$. Then,*

$$B_n(\alpha) \geq B(a_d)^{-1/d} n^{1/d}(1+o(1)). \tag{3.2}$$

Sketch of proof. In [3], the following inequalities are used: for any integers $n, m \geq 0$,

$$B(m+n) \leq B(m) + B(n) \tag{3.3}$$

$$B(m\cdot n) \leq B(m)\cdot B(n). \tag{3.4}$$

They are very simple but seem to have been unnoticed before [3]. Their proofs are based on the even simpler equalities: for any positive integer $m = (m_k \cdots m_1 m_0)_2$,

$$B(m+2^j) = B(m) + 1 - L_j \ (\leq B(m)+1) \tag{3.5}$$

$$B(2^j m) = B(m), \tag{3.6}$$

where L_j is the number of consecutive digits equal to 1 from m_j to m_k. Eq. (3.6) is obvious while Eq. (3.5) is proved by the usual "add with carry" algorithm. The proof of (3.3) follow from (3.5) by induction on the bits of n and for (3.6), we see that

$$B(mn) = B(m\sum_{\ell=1}^{s} 2^{j_\ell}) \overset{(3.3)}{\leq} \sum_{\ell=1}^{s} B(m2^{j_\ell}) \overset{(3.6)}{=} \sum_{\ell=1}^{s} B(m) = B(m)B(n).$$

We want to extend (3.3) and (3.4) to real numbers. The following inequalities will be enough.

Proposition 3. *Let x and y be positive irrational numbers.*
(i) If $x+y$ is irrational, then

$$B_n(x+y) \leq B_n(x) + B_n(y) + 1.$$

This also holds if y is a positive integer.
(ii) If xy is irrational, then

$$B_n(x\cdot y) \leq B_n(x)\cdot B_n(y) + c_p(x,y),$$

where $c_p(x,y) > 0$ is independent of n. That inequality also holds if y is a positive integer.
(iii) Let A be a positive integer. We have

$$B_n(x)\cdot B_n(A/x) \geq n - c_i(x,y),$$

where $c_i(x,y) > 0$ is independent of n.

[1] I am indebted to B. Adamczewski for this remark.

All these inequalities are sharp, up to multiplicative and additive constants. The constants c_p and c_i can be made explicit but this not necessary here. We omit the proof of this lemma, which can be found in [9].

We now complete the proof of Theorem 4. By hypothesis, we have

$$\frac{|a_0|}{\alpha} = a_1 + a_2\alpha + \cdots + a_d\alpha^{d-1}.$$

Using Proposition 3(i), iteratively on the right hand side ([2]), we get the first inequality in

$$B_n(a_1 + a_2\alpha + \cdots + a_d\alpha^{d-1}) \leq \sum_{j=1}^{d} B_n(a_d\alpha^{j-1})(1+o(1)) \leq \sum_{j=1}^{d} B(a_d)B_n(\alpha)^{j-1}(1+o(1)),$$

where the second inequality holds using Proposition 3(ii). On the other hand, Proposition 3(iii) implies that

$$B_n(\alpha)B_n\left(\frac{|a_0|}{\alpha}\right) \geq n - c,$$

for some c independent of n. Hence, since $B_n(\alpha) \to +\infty$, we deduce that

$$n - c \leq B(\alpha)\sum_{j=1}^{d} B(a_d)B_n(\alpha)^{j-1}(1+o(1)) = B(a_d)B_n(\alpha)^d.$$

This completes the sketch of the proof. □

It would be interesting to obtain a complete proof of Theorem 3 in the spirit of that of Theorem 4. For this, it would be desirable to have a good control of $B_n(x-y)$ in terms of $B_n(x)$ and $B_n(y)$ or a control of $B(m-n)$ in terms of $B(m)$ and $B(n)$. Unfortunately, this does not seem to be easy when one considers the examples $m = (1000000)_2$, $n = (1)_2$: we have $B(m) = B(n) = 1$ but $B(m-n) = B((111111)_2) = 6$. Another approach would be to split the positive coefficients of the minimal polynomial of α from the negative ones to get an identity like

$$\sum_{i\in I} b_{k_i}\alpha^{k_i} = \sum_{i\in J} b_{k_i}\alpha^{k_i}$$

where I and J form a partition of $0, 1, \ldots, d$ and all $b_k \geq 0$. But it is not clear how to get a proof of Theorem 4 very different from that of [3].

Needless to say, it would be even more desirable to increase the exponent $1/d$ in $n^{1/d}$ to a value closer to 1 (which would be a result very close to normality). By analogy with diophantine approximation, we can say that BBCP Theorem is to simple normality in base 2 what Liouville's Theorem is to Roth's Theorem.

4. Applications to transcendental numbers

As mentioned in [3], Theorem 3 can be used to prove the transcendence of real numbers, sometimes for numbers not amenable to more classical methods.

Theorem 5 (BBCP)**.** *Let ξ be a real irrational number such that for some $d \geq 2$ we have*

$$\liminf_{n\to+\infty} \frac{B_n(\xi)}{n^{1/d}} = 0$$

Then ξ is not an algebraic number of degree $\leq d$. If this holds for all $d \geq 2$, then ξ is transcendental.

This is an immediate consequence of Theorem 3. For example, this shows the transcendence of the number

$$\xi_\phi = \sum_{n=0}^{\infty} \frac{1}{2^{\phi(n)}}$$

for any ϕ such that

$$\limsup_{n\to+\infty} \frac{\phi(n)}{n^k}$$

[2]For $k = 2, \ldots, d$, the numbers $a_k\alpha^{k-1}$ and $\sum_{j=k+1}^{d} a_d\alpha^{j-1}$ are irrational numbers

for any $k > 0$. This applies to $\phi(n) = \lfloor n^{\log\log(n+3)} \rfloor$: for that ϕ, the transcendence of ξ_ϕ was not known before [3].

One also gets a new proof of the transcendence of the number $\mathcal{K} = \sum_{n\geq 0} 2^{-2^n}$, first obtained by Kempner [6]. (Another proof in the digital spirit of [3] was also given by Knight [7]; see [2] for a presentation of many distinct proofs). This number is interesting for other reasons as well. Indeed, clearly $B_n(\mathcal{K}) \sim \log_2(n)$ and it is not difficult to prove that

$$B_n(\mathcal{K}^2) \sim \frac{1}{2}\log_2(n)^2$$

as $n \to +\infty$ (see [9]). This shows that Proposition 3(ii) is optimal. The same proposition also shows that $B_n(\mathcal{K}^j) \ll \log_2(n)^j$ for any integer $j \geq 1$ with the consequence that we thus have an example of a transcendental number for which none of its powers are simply normal in base 2. It seems likely that

$$B_n(\mathcal{K}^j) \sim k_j \log_2(n)^j$$

as $n \to +\infty$ for some $k_j > 0$. Is it true that $k_j = \frac{1}{j!}$ for any integer $j \geq 1$?

Bibliography

[1] B. Adamczewski and Y. Bugeaud, *On the complexity of algebraic numbers. I. Expansions in integer bases*, Ann. of Math. (2) **165** (2007), no. 2, 547–565.

[2] B. Adamczewski, *The many faces of* $\sum_{n\geq 0} 2^{-2^n}$, slides of a talk given at the conference "Diophantine Approximation and related topics" (Tokyo) in march 2009.

[3] D. H. Bailey, J. M. Borwein, R. E. Crandall and C. Pomerance, *On the binary expansions of algebraic numbers*, J. Théor. Nombres Bordeaux **16**(3) (2004), 487–518.

[4] E. Borel, Sur les probabilités dénombrables et leurs applications arithmétiques, Rend. Circ. Mat. Palermo **27** (1909), 247–271.

[5] D. G. Champernowne, *The construction of decimals normal in the scale of ten*, J. Lond. Math. Soc bf 8 (1933), 254–260.

[6] A. J. Kempner, *On transcendental numbers*, Trans. Amer. Math. Soc. **17** (1916), 476–482.

[7] M.J. Knight, *An "oceans of zeros" proof that a certain non-Liouville number is transcendental*, Amer. Math. Monthly **98** (1991), no. 10, 947–949.

[8] D. Ridout, *Rational approximations to algebraic numbers*, Mathematika **4** (1957), 125–131.

[9] T. Rivoal, *On the bits counting function of real numbers*, J. Aust. Math. Soc. **85** (2008), no. 1, 95–111.

[10] T. Rivoal, *Convergents and irrationality measures of logarithms*, Rev. Mat. Iberoamericana **23**.3 (2007), 931–952.

[11] K. F. Roth, *Rational approximations to algebraic numbers*, Mathematika **2** (1955), 1–20; corrigendum, 168.

[12] W. Sierpiński, *Démonstration élémentaire du théorème de M. Borel sur les nombres absolument normaux et détermination effective d'une tel nombre*, Bull. SMF **45** (1917), 125–132.

T. Rivoal, Institut Fourier, CNRS UMR 5582, Université Grenoble 1, 100 rue des Maths, BP 74, 38402 Saint-Martin d'Hères cedex, France. • `http://www-fourier.ujf-grenoble.fr/~rivoal`