ON A PROPERTY OF PISOT NUMBERS AND RELATED QUESTIONS

Yann BUGEAUD

In all what follows q denotes a real number satisfying $1 < q < 2$. First we define two sequences of positive numbers which depend on q.

Definition 1. *Let k be a positive integer and let*

$$0 =: y_0^{(k)} < y_1^{(k)} < y_2^{(k)} \dots$$

be the increasing sequence of those real numbers y which have at least one representation of the form

$$y = \varepsilon_1 q + \varepsilon_2 q^2 + \dots + \varepsilon_i q^i,$$

where $i \geq 1$ and $\varepsilon_1, \dots, \varepsilon_i \in \{0, 1, \dots, k\}$.

Definition 2. *Let $\left(y_n^{(k)}\right)_{n \geq 0}$ be a sequence as above. We define the difference sequence $\left(u_n^{(k)}\right)_{n \geq 0}$ by*

$$u_n^{(k)} = y_{n+1}^{(k)} - y_n^{(k)}.$$

In order to simplify the notations, it is convenient to write y_n for $y_n^{(1)}$ and also u_n for $u_n^{(1)}$.

Those sequences have already been studied by P. Erdős, I. Joó, M. Joó and V. Komornik [3, 4], we recall here some of their results. According to them, we denote by A the golden number, i.e. the positive root of the polynomial $X^2 - X - 1$.

Theorem A. [4] *For all integer n, we have $u_n \leq 1$. Moreover, if $q \geq A$, then* $\limsup(u_n) = 1$.

Theorem B. [3] *Let $r \geq 2$ be an integer and let ζ_r be the only root in $]1, 2[$ of the polynomial $X^{r+1} - X^r - \dots - 1$. Then for $q = \zeta_r$ we have* $\liminf(u_n) = \dfrac{1}{\zeta_r}$.

Theorem A leads to the following two questions :

- Is there a $q \in]1, A[$ for which $\limsup(u_n) = 1$?
- Is there a $q \in [A, 2[$ for which $\limsup\left(u_n^{(2)}\right) = 1$?

One of the purposes of this note is to give negative answers to both problems.

Theorem B was proved by combinatorical methods and at the end of their paper the authors asked (*Problem 5*) whether we have $\liminf(u_n) = 0$ for the other values of q. Another aim of this note is to disprove this conjecture.

We recall that an algebraic integer is a Pisot number if its conjugates have modulus strictly less than 1. The ζ_r occuring in Theorem B are example of Pisot numbers.

Statement of the results

Theorem 1. *The real $q \in]1, 2[$ is a Pisot number if and only if we have $\liminf\left(u_n^{(k)}\right) > 0$ for all positive integers k.*

Independently and by means of another method, P. Erdős, I. Joó and V. Komornik [5] proved a weaker result, namely that we have $\liminf(u_n)_n > 0$ for all Pisot numbers in $]1, 2[$.

Remark 1 : As we will see during the proof, we obtain a lower bound for $\liminf\left(u_n^{(k)}\right) > 0$. Numerical estimates show that this bound seems to be far away from the exact value.

Remark 2 : If q is not a root of a polynomial with coefficients 0, 1 or -1, we obtain immediately (e.g. by the pigeon hole principle) that $\liminf(u_n) = 0$.

Theorem 2. *Let $q \in]1, A[$, for all $n \geq 1$ we have*

$$u_n \leq \mathrm{Max}\{q^2 - q, 1 + q - q^2\}.$$

In particular, $\limsup(u_n) < 1$.

Theorem 3. *Let $q \in [A, 2[$, for all $n \geq 1$ we have*

$$u_n^{(2)} \leq \mathrm{Max}\{q - 1, 2 - q\}.$$

In particular, $\limsup\bigl(u_n^{(2)}\bigr) < 1$.

Remark 3 : It is easy to prove that for $q = A$ we have $\limsup\bigl(u_n^{(2)}\bigr) = A - 1$ and $\liminf\bigl(u_n^{(2)}\bigr) = 2 - A$.

A result from the theory of automata

We now recall some results obtained by C. Frougny and D. Berend [1, 6].

Let c be a positive integer and let $C = \{-c, \ldots, 0, \ldots, c\}$; we consider the set $Z(q, c)$ of infinite words on $C^{\mathbf{N}}$ which correspond to 0 in base q in the following way :

$$Z(q, c) = \Bigl\{ s = (s_n)_{n \geq 0} \in C^{\mathbf{N}} \mid \sum_{n \geq 0} s_n q^{-n} = 0 \Bigr\}.$$

We denote by $LF(Z(q, c))$ the set of left factors of words of $Z(q, c)$, i.e. $\{w \in C^* \mid \exists s \in C^{\mathbf{N}}, ws \in Z(q, c)\}$, where C^* is the set of words of finite length over the alphabet $\{-c, \ldots, 0, \ldots, c\}$.

To every element $f_0 f_1 \ldots f_n$ of $LF(Z(q, c))$ is associated a polynomial $F(X) = f_o X^n + \ldots + f_n$. The remainder of the Euclidean division of F by $X - q$ is $F(q)$, which is bounded. Indeed, we know that there exist $f_{n+1}, f_{n+2}, \ldots$ elements of C satisfying $\sum_{i=0}^{\infty} f_i q^{-i} = 0$; then we can deduce that

$$|F(q)| = \Bigl| - \sum_{i=n+1}^{\infty} f_i q^{n-i} \Bigr| \leq \frac{c}{q - 1}.$$

Proposition 1. *[6] The set $Z(q, c)$ is recognizable by a finite automaton if and only if the number of remainders of the Euclidean division by $X - q$ of polynomials associated to words of $LF(Z(q, c))$ is finite.*

Proposition 2. *[1] The set $Z(q, c)$ is recognizable by a finite automaton for every positive integer c if and only if q is a Pisot number.*

We derive at once from those two propositions the following result.

Proposition 3. *The real number q is a Pisot number if and only if for every positive integer c the number of remainders of the Euclidean division by $X - q$ of polynomials associated to words of $LF(Z(q, c))$ is finite.*

Remark 4 : G. Rauzy [7] pointed out that the theory of automata can be used to solve a problem stated by Erdős about the expansions of 1 in bases q.

Proofs

Proof of Theorem 1 :

The condition is necessary. To show this, we use the same argument as A. Bogmér, M. Horváth and A. Sövegjártó [2], based on algebraic number theory. Let q be a Pisot number and k be a positive integer. It suffices to prove that $(u_n^{(k)})$ only takes a finite number of distinct values. Let n be a positive integer, we can write

$$u_n^{(k)} = \sum_{j=0}^{\infty} \eta_j q^j,$$

where the η_i are relative integers of absolute value bounded by k, equal to 0 if i is large enough.

Denote by $\mathbf{K}$ the number field $\mathbf{Q}(q)$ and by d its degree. Let $q =: \alpha_1, \ldots, \alpha_d$ be the conjugates of q; to each α_i is associated a unique monomorphism $\sigma_i : \mathbf{K} \mapsto \mathbf{C}$ satisfying $\sigma_i(q) = \alpha_i$. The algebraic integer $u_n^{(k)}$ is positive, belongs to $\mathbf{K}$ and, according to Lemma 1, is less or equal to 1. Let i be an integer, $2 \leq i \leq d$, we have

$$|\sigma_i(u_n^{(k)})| \leq \sum_{j=0}^{\infty} k|\sigma_i(q)|^j \leq \frac{k}{1-|\sigma_i(q)|}.$$

Since q is a Pisot number, there exists a real number $a > 0$ satisfying $1 - |\sigma_i(q)| \geq a$, for $i = 2, \ldots, d$. Hence the Mahler measure of $u_n^{(k)}$ is bounded above by $(k/a)^{d-1}$. But for all real numbers $C > 1$, the set of elements of $\mathbf{K}$ of measure less than C is finite; consequently the sequence $(u_n^{(k)})$ only takes a finite number of distinct values. Since by definition $u_n^{(k)}$ is never 0, necessity is proved.

We can easily derive a lower bound for $l_k := \liminf(u_n^{(k)})$. Indeed, denote by $\mathrm{M}(\alpha)$ the Mahler measure of a non-zero algebraic number α, we have $\mathrm{M}(\alpha) = \mathrm{M}(\alpha^{-1})$ and

$$l_k \geq \mathrm{M}\big(1/u_n^{(k)}\big)^{-1} = \mathrm{M}\big(u_n^{(k)}\big)^{-1} \geq k^{-d+1} \prod_{j=2}^{d} \big(1 - |\sigma_j(q)|\big).$$

The condition is sufficient. Let now suppose that q is not a Pisot number; according to Proposition 3, there exists an integer $c \geq 1$ for which the number of remainders of the Euclidean division by $X - q$ of polynomials associated to words of $LF(Z(q,c))$ is infinite. But we have seen that the absolute value of such a remainder is bounded by $\dfrac{c}{q-1}$. Hence, for fixed $\varepsilon > 0$, there exist two polynomials $P(X)$ et $Q(X)$, with coefficients in $\{-c, \ldots, 0, \ldots, c\}$ and with degree bounded, say, by D, satisfying

$$0 \neq |P(q) - Q(q)| < \varepsilon.$$

This can also be written

$$0 \neq \Big|\sum_{i=0}^{D} \varepsilon_i q^i - \sum_{j=0}^{D} \varepsilon'_j q^j\Big| < \varepsilon,$$

where the ε_i and the ε'_j belong to the set $\{0, 1, \ldots, 2c\}$. This shows that

$$\liminf\big(u_n^{(2c)}\big) = 0,$$

and the proof is complete.

Proof of Theorem 2 :

The idea is to build a sequence $\big(P_k(X)\big)_{k\geq 1}$ of polynomials with coefficients 0 or 1, in such a way that the polynomials $P_{k+1}(X) - P_k(X)$ take small values over the interval $]1, A[$.

Let define $P_1(X) = 1$, $P_2(X) = X$, $P_3(X) = X^2$, $P_4(X) = X + 1$, $P_5(X) = X^2 + 1$ and $P_6(X) = X^2 + X$. We use induction on the degree of the polynomials. Let $k \geq 2$ be an integer. For all l, with $2 \leq l \leq k$, we suppose that the polynomials of degree l are built and that the last two are $X^l + X^{l-2} + X^{l-4} + \ldots$ and $X^l + X^{l-1}$. We then enumerate the polynomials of degree $k+1$: those are $X^{k+1} + P_1(X)$, $X^{k+1} + P_2(X), \ldots$, until the polynomial $X^{k+1} + X^{k-1} + X^{k-3} + \ldots$, which exists by induction hypothesis, and at last $X^{k+1} - X^k$.

The sequence (P_k) is now well defined, it is easy to see that the polynomials $P_{k+1} - P_k$ belong to the set

$$\{1 + X - X^2\} \bigcup_{r\geq 2} \{X^{r+1} - X^r - X^{r-1} + 1\} \bigcup_{r\geq 0} \{X^{2r+1} - X^{2r} - X^{2r-2} \ldots - 1, X^{2r} - X^{2r-1} - X^{2r-3} \ldots - X\}.$$

We shall bound the value of all those polynomials for $q \in]1, A[$.

Let $r \geq 2$, we use $r-2$ times the inequality $q^2 < 1+q$, which is true because $q < A$, and so obtain

$$\begin{aligned} q^{r+1} - q^r - q^{r-1} + 1 &= (q-1)(q^r - q^{r-2} - q^{r-3} \ldots - 1) \\ &\leq (q-1)(q^2-1) \leq q(q-1). \end{aligned}$$

In the same way, if $r \geq 0$, by repeated use of the inequality $q^2 < 1+q$, we get

$$q^{2r+1} - q^{2r} - q^{2r-2} \ldots - 1 \leq q^3 - q^2 - 1 \leq q - 1,$$

and

$$q^{2r} - q^{2r-1} - q^{2r-3} \ldots - q \leq q(q-1).$$

Thus we have built a sequence $\big(P_k(q)\big)_{k\geq 1}$ satisfying, for all $k \geq 1$,

$$P_{k+1}(q) - P_k(q) \leq \mathrm{Max}\{q^2 - q, 1 + q - q^2\}.$$

It is clear that this sequence is not increasing; nevertheless, we extract a strictly increasing subsequence, which we can write $(y_{n_i})_{i\geq 1}$, and which satisfies

$$0 < y_{n_{i+1}} - y_{n_i} \leq \mathrm{Max}\{q^2 - q, 1 + q - q^2\}.$$

Hence Theorem 2 is proved.

Proof of Theorem 3 :

We use the same idea as in the proof of Theorem 2 : we build a sequence $\big(Q_k(X)\big)_{k\geq 1}$ of polynomials with coefficients 0, 1 or 2 as follow.

Let define $Q_1(X) = 1$, $Q_2(X) = X$, $Q_3(X) = 2$, $Q_4(X) = X + 1$, $Q_5(X) = 2X$ and $Q_6(X) = X^2 + 1$. We use induction on the degree of the polynomials. Let $k \geq 2$ be an integer. For all l, with $1 \leq l \leq k$, we suppose that the polynomials of degree l are built and that the last two are $X^l + X^{l-1} + X^{l-2} + \ldots + 1$ and $2X^l$. We then enumerate the polynomials of degree $k+1$: those are $X^{k+1} + Q_1(X)$, $X^{k+1} + Q_2(X), \ldots$, until the polynomial $X^{k+1} + X^k + X^{k-1} + \ldots + 1$, which exists by induction hypothesis, and at last $2X^{k+1}$.

We easily compute that for all $k \geq 1$ and all $q \in [A, 2[$ we have

$$Q_{k+1}(q) - Q_k(q) \leq \mathrm{Max}\{q - 1, 2 - q\}.$$

Theorem 3 immediately follows.

Acknowledgements : I would like to thank M. Mignotte and also V. Komornik, who introduced me to those questions.

References :

[1] D. Berend and C. Frougny, Computability by finite automata and Pisot bases, *Math. Systems Theory*, **27** (1994), 275-282.

[2] A. Bogmér, M. Horváth and A. Sövegjártó, On some problems of I. Joó, *Acta Math. Hung.*, **58** (1991), 153-155.

[3] P. Erdős, I. Joó and M. Joó, On a problem of Tamás Varga, *Bull. Soc. Math. France*, **120** (1992), 507-521.

[4] P. Erdős, I. Joó and V. Komornik, Characterization of the unique expansion $1 = \sum q^{-n_i}$ and related problems, *Bull. Soc. Math. France*, **118** (1990), 377-390.

[5] P. Erdős, I. Joó and V. Komornik, *In preparation.*

[6] C. Frougny, Representations of number and finite automata, *Math. Systems Theory*, **25** (1992), 37-60.

[7] G. Rauzy, Sur les développements en base non entière, *Colloque de théorie des nombres* (Alger, 21-23 octobre 1989).

Yann Bugeaud
Université Louis Pasteur
7, rue René Descartes
67084 STRASBOURG
(FRANCE)

e-mail : bugeaud@pari.u-strasbg.fr