Expansions of numbers in multiplicatively independent bases: Furstenberg's conjecture, Mahler's method, and finite automata

Boris Adamczewski
Joint work with Colin Faverjon

CNRS, Institut Camille Jordan, Lyon

European Research Council
Established by the European Commission

Reminder

Two natural numbers p and q are multiplicatively independent if

$$(p^n = q^m, n, m \in \mathbb{Z}) \implies n = m = 0\,,$$

or, equivalently, if $\log p/\log q \notin \mathbb{Q}$.

For instance, 2 and 10, or 2 and 3, are multiplicatively independent, but 36 and 216 are not.

A general heuristic

Le bonheur n'est pas chose aisée.

It is commonly expected that expansions of numbers in multiplicatively independent bases should have no common structure.

However, it seems particularly difficult to confirm this naive heuristic principle in some way or another.

Two examples

The binary Thue-Morse number τ is defined as follows. Its nth binary digit is equal to 0 if the sum of digits in the binary expansion of n is even, and to 1 otherwise.

The binary expansion of τ is

$$\langle\tau\rangle_2 = 0.011\,010\,011\,001\,011\,010\,010\,110\,011\,010\,011\,001\,011\cdots$$

while its decimal expansion is

$$\langle\tau\rangle_{10} = 0.412\,454\,033\,640\,107\,597\,783\,361\,368\,258\,455\,283\,089\cdots.$$

The binary expansion of 2^{61} is

$$\langle 2^{61}\rangle_2 = 1\,000\,000\,000\,\cdots\,000\,000$$

while its decimal expansion is

$$\langle 2^{61}\rangle_{10} = 2\,305\,843\,009\,213\,693\,952\,.$$

Part I. Furstenberg's conjecture and finite automata

The dynamical point of view: Furstenberg's conjecture

Let T_q denote the map defined on $\mathbb{R}/\mathbb{Z}$ by $x \mapsto qx$.

Let $\mathcal{O}_q(x)$ denote the forward orbit of x under T_q, that is

$$\mathcal{O}_q(x) := \left\{x, T_q(x), T_q^2(x), \ldots\right\}.$$

Conjecture (Furstenberg, 1969)

Let p and q be two multiplicatively independent natural numbers, and let $x \in [0,1)$ be an irrational real number. Then

$$\dim_H \overline{\mathcal{O}_p(x)} + \dim_H \overline{\mathcal{O}_q(x)} \geq 1.$$

This conjecture beautifully expresses the expected balance between the complexity of expansions of a real number in independent bases:

> *If an irrational number x has low complexity in one base, then it should have high complexity in every other independent base.*

Comments on Furstenberg's conjecture

Conjecture (Furstenberg, 1969)

Let p and q be two multiplicatively independent natural numbers, and let $x \in [0,1)$ be an irrational real number. Then

$$\dim_H \overline{\mathcal{O}_p(x)} + \dim_H \overline{\mathcal{O}_q(x)} \geq 1.$$

- Furstenberg's conjecture holds true *generically*.

- In fact, all the strength of this conjecture takes shape when x has a simple expansion in one base, especially when x has *zero entropy*.

The binary Thue-Morse number τ

$$\langle \tau \rangle_2 = 0.011\,010\,011\,001\,011\,010\,010\,110\,011\,010\,011\,001\,011 \cdots$$

has zero entropy in base 2 and hence its decimal expansion

$$\langle \tau \rangle_{10} = 0.412\,454\,033\,640\,107\,597\,783\,361\,368\,258\,455\,283\,089 \cdots$$

should have full entropy!

Yet another astonishing consequence

1	2
10	4
100	8
1000	16
10000	32
100000	64
1000000	128
⋮	⋮
100 000 000 000 000 000 000	2 097 152
1 000 000 000 000 000 000 000	4 194 304
⋮	⋮

As observed by Furstenberg, his conjecture implies that any finite block of digits occurs in the decimal expansion of 2^n, as soon as n is large enough.

A related conjecture of Erdős claims that the digit 2 occurs in the ternary expansion of 2^n for all $n > 8$.

The works of Shmerkin and Wu

Recently, Shmerkin and Wu proved independently the following remarkable result (both papers are published in the same issue of the *Annals of Math.*).

Theorem (Shmerkin-Wu, 2019)

The set of exceptions to Furstenberg's conjecture has Hausdorff dimension zero.

Though this contribution marks significant progress, Furstenberg's conjecture remains far out of reach of current methods.

Unfortunately, this theorem does not tell us anything about expansions of real numbers with zero entropy in some base...

The computational point of view

While expansion of computable numbers can be generated by general Turing machines, *automatic real numbers* are those whose expansion can be generated by a finite automaton. From a computational point of view, this provides another relevant notion of a number with low complexity.

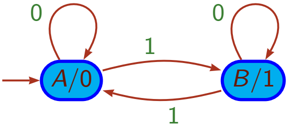
Definition

A real number x is automatic in base b if there exists a finite automaton that takes as input the expansion of n in some fixed base and produces as output the nth digit of x in base b.

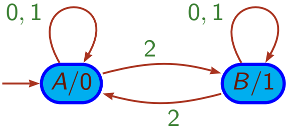
Example 1. The binary Thue–Morse number

$$\langle \tau \rangle_2 = 0.011\,010\,011\,001\,011\,010\,010\,110\,011\,010\,011\,001\,011\cdots$$

is automatic in base 2.



Example 2.



This automaton generates the binary automatic number

$$\langle \tau' \rangle_2 = 0.001\,001\,110\,001\,011\,110\,110\,110\,011\,001\,001\,110\,001\cdots$$

Three conjectures involving automata

According to our general heuristic, we expect the following result.

Conjecture 1

Let p and q be two multiplicatively independent natural numbers, and let x be an irrational real number. If x is automatic in base p, then it cannot be automatic in base q.

With a more Diophantine flavour, Conjecture 1 can be strengthened as follows.

Conjecture 2

Let p and q be two multiplicatively independent natural numbers, x_1 be automatic in base p, and x_2 be automatic in base q, both irrational. Then x_1 and x_2 are algebraically independent over $\overline{\mathbb{Q}}$ (the field of algebraic numbers).

It would not only show that τ cannot be automatic in base 10, but also that this is the case for any number obtained from τ by using algebraic numbers and algebraic operations (addition, multiplication, division, taking nth roots...).

The two previous conjectures can even be generalized as follows.

Conjecture 3

Let $x_1, ..., x_r$ be irrational automatic numbers with respect to some multiplicatively independent bases $b_1, ..., b_r$. Then $x_1, \ldots, x_r$ are algebraically independent over $\overline{\mathbb{Q}}$.

Reminder. Complex numbers $\alpha_1, \ldots, \alpha_r$ are multiplicatively independent if there is no non-zero tuple of integers $(n_1, \ldots, n_r)$ such that $\alpha_1^{n_1} \cdots \alpha_r^{n_r} = 1$.

For instance, 2, 3, and 10 are multiplicatively independent, while 2, 5, and 10 are not.

Part II. Mahler's method

M-functions

In 1929, Mahler initiated a new method in transcendental number theory. It aims at proving results about transcendence and algebraic independence of values of the so–called M-functions at algebraic points.

Definition

Let $q \geq 2$ be a natural number. A formal power series $f(z) \in \overline{\mathbb{Q}}[[z]]$ is a q-Mahler function if there exist $p_0(z), \ldots, p_m(z) \in \overline{\mathbb{Q}}[z]$, not all zero, such that

$$p_0(z)f(z) + p_1(z)f(z^q) + \cdots + p_d(z)f(z^{q^m}) = 0\,.$$

We say that $f(z)$ is an M-function if it is a q-Mahler function for some $q \geq 2$.

The function $\mathfrak{f}(z) := \sum_{n=0}^{\infty} z^{2^n}$ satisfies the inhomogeneous 2-Mahler equation

$$\mathfrak{f}(z^2) = \mathfrak{f}(z) - z\,. \tag{1}$$

Mahler used (1) to prove that $\mathfrak{f}(\alpha)$ is transcendental for all $\alpha \in \overline{\mathbb{Q}}$, $0 < |\alpha| < 1$.

Connection between Mahler's method and automatic numbers

The Thue-Morse sequence $\mathbf{t} := t(n)$ is the 2-automatic sequence defined by:
$t(n) = 0$ if the sum of digits in the binary expansion of n is even,
$t(n) = 1$ otherwise.

Hence $t(2n) = t(n)$ while $t(2n+1) = 1 - t(n)$.

It follows that the generating series $\mathfrak{f}_{\mathbf{t}}(z) := \sum t(n)z^n$ satisfies

$$\begin{aligned} \mathfrak{f}_{\mathbf{t}}(z) &= \sum t(2n)z^{2n} + \sum t(2n+1)z^{2n+1} \\ &= \mathfrak{f}_{\mathbf{t}}(z^2) + \frac{z}{1-z^2} - z\mathfrak{f}_{\mathbf{t}}(z^2), \end{aligned}$$

leading to the inhomogeneous linear 2-Mahler equation of order one:

$$\frac{z}{1-z^2} - \mathfrak{f}_{\mathbf{t}}(z) + (1-z)\mathfrak{f}_{\mathbf{t}}(z^2) = 0 .$$

We obtain that $\mathfrak{f}_{\mathbf{t}}(z)$ is an M-function and that the binary Thue-Morse number $\tau = \mathfrak{f}_{\mathbf{t}}(1/2)$.

Connection between Mahler's method and automatic numbers

In 1968, Cobham noticed the following fundamental connection between automatic numbers and M-functions.

If $x = a_0.a_1a_2\cdots$ is automatic in base b, then the generating series

$$f(z) := \sum_{n=0}^{\infty} a_n z^n$$

is an M-function. Hence, then there exists an M-function $f(z) \in \mathbb{Q}[[z]]$ such that $x = f(1/b)$.

Consequence. Problems concerning transcendence and algebraic independence of automatic numbers can be restated and extended as problems concerning transcendence and algebraic independence of values of M-functions at algebraic points, which is precisely the aim of Mahler's method.

First fundamental question. If $f(z)$ is a transcendental M-function and $\alpha, 0 < |\alpha| < 1$, is algebraic, can we decide whether $f(\alpha)$ is transcendental?

Mahler's first results imply that the Thue–Morse number is transcendental and in fact that $\mathfrak{f}_{\mathfrak{t}}(\alpha)$ is transcendental for all algebraic α, $0 < |\alpha| < 1$.

Warning. The infinite product $\mathfrak{g}(z) := \prod_{n\geq 0}(1 - 2z^{3^n})$ is a transcendental M_3-function solution to

$$\mathfrak{g}(z) = (1 - 2z^3)\mathfrak{g}(z^3)$$

but $\mathfrak{g}(\alpha) = 0$ for every α such that $\alpha^{3^n} = 1/2$ for some n.

Transcendence of values of M-functions at algebraic points

After various works including contributions of Mahler, Kubota, Loxton and van der Poorten, Nishioka, and Philippon, the problem of the transcendence of values of M-functions at algebraic points has been settled recently.

Theorem (A. and Faverjon, 2017)

Let $f(z)$ be an M-function and $\alpha \in \overline{\mathbb{Q}}$ be such that f is well-defined at α. Let $\mathbb{K}$ be the number field generated by the coefficients of $f(z)$ and α.
Then either $f(\alpha) \in \mathbb{K}$ or $f(\alpha)$ is transcendental.

Furthermore, the proof is effective and provides an algorithm that is able to settle this alternative.

The case $\mathbb{K} = \mathbb{Q}$ was conjectured by Cobham in 1968.

Consequence. The base-b expansion of an algebraic irrational number, such as $\sqrt{2}$, cannot be generated by a finite automaton.

Our main result

Let $r \geq 1$ be an integer. For every i, $1 \leq i \leq r$, we let:

- $f_i(z) \in \overline{\mathbb{Q}}[[z]]$ be a q_i-Mahler function,
- $\alpha_i \in \overline{\mathbb{Q}}$, $0 < |\alpha_i| < 1$, be such that $f_i(z)$ is well-defined at α_i.
- $\mathbb{K} \subset \overline{\mathbb{Q}}$ be the number field generated by the coefficients of all the $f_i(z)$ and the α_i.

Main Theorem (A. and Faverjon, 2020)

Let us assume that one the two following properties hold.

(i) *The numbers $\alpha_1, \ldots, \alpha_r$ are multiplicatively independent.*

(ii) *The numbers $q_1, \ldots, q_r$ are pairwise multiplicatively independent.*

Then the numbers $f_1(\alpha_1), f_2(\alpha_2), \ldots, f_r(\alpha_r)$ are algebraically independent over $\overline{\mathbb{Q}}$, unless one of them belongs to $\mathbb{K}$.

The case $r = 1$ corresponds to the previous theorem.

Consequence of point (i) of our main theorem

Assumption. Let $f_1(z), \ldots, f_r(z) \in \overline{\mathbb{Q}}[[z]]$ be M-functions, $\alpha_1, \ldots, \alpha_r \in \overline{\mathbb{Q}}$, $0 < |\alpha_i| < 1$, be such that $f_i(z)$ is well-defined at α_i, and $\mathbb{K} \subset \overline{\mathbb{Q}}$ be the number field generated by the coefficients of all the $f_i(z)$ and the α_i.

Main Theorem (Part (i))

Let us assume that $\alpha_1, \ldots, \alpha_r$ are multiplicatively independent. Then the numbers $f_1(\alpha_1), f_2(\alpha_2), \ldots, f_r(\alpha_r)$ are algebraically independent over $\overline{\mathbb{Q}}$, unless one of them belongs to $\mathbb{K}$.

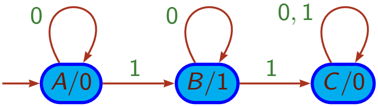
Proof of Conjectures 1–3. Let $x_1, \ldots, x_r$ be irrational automatic numbers with respect to some multiplicatively independent bases $b_1, \ldots, b_r$.
Since x_i is automatic in base b_i, there exists an M-function $f_i(z) \in \mathbb{Q}[[z]]$ such that $x_i = f_i(1/b_i)$.

Set $\alpha_i := 1/b_i$ and $\mathbb{K} = \mathbb{Q}$. By assumption, the numbers $\alpha_1, \ldots, \alpha_r$ are multiplicatively independent and none of the numbers $x_1, \ldots, x_r$ belongs to $\mathbb{K}$.

The theorem implies that the numbers $x_1 = f_1(\alpha_1), \ldots, x_r = f_r(\alpha_r)$ are algebraically independent over $\overline{\mathbb{Q}}$, as wanted. □

As with Furstenberg's conjecture, our theorem has also valuable consequences about expansions of natural numbers.

A set $\mathcal{E} \subset \mathbb{N}$ is q-automatic if there exists a finite automaton taking as input the base-q expansion of n and that outputs 1 when $n \in \mathcal{E}$ and 0 otherwise.



The set of powers of 2 is a typical example of a 2-automatic set.

Theorem (Cobham, 1969)

Let p and q be multiplicatively independent natural numbers. A set $\mathcal{E} \subset \mathbb{N}$ is both p- and q-automatic if and only if it is the union of finitely many arithmetic progressions.

Cobham's theorem implies that, when written in base 10, the set of powers of 2 cannot be recognized by a finite automaton.

If $\mathcal{E} \subset \mathbb{N}$, its generating series is $\sum_{n\in\mathcal{E}} z^n$.

Rephrasing of Cobham's theorem in terms of generating series. Let $\mathcal{E}_p$ be a p-automatic set and $\mathcal{E}_q$ be a q-automatic set. Assume that $\log p/\log q \notin \mathbb{Q}$.

$$\sum_{n\in\mathcal{E}_p} z^n = \sum_{n\in\mathcal{E}_q} z^n \implies \text{these series are rational functions.}$$

In 1987, Loxton and van der Poorten conjectured the following generalizations:

(i) A power series cannot satisfy a p-Mahler equation and a q-Mahler equation, unless it is a rational function.
(A. and Bell 2017 and Schäfke and Singer 2019)

(ii) Let $f(z)$ be a solution to a p-Mahler equation and $g(z)$ be a solution to a q-Mahler equation, both irrational. Then $f(z)$ and $g(z)$ are algebraically independent over $\overline{\mathbb{Q}}(z)$.
(A., Dreyfus, Hardouin, and Wibmer, 2020)

Consequence of point (ii) of our main theorem

Theorem (A. & Faverjon, 2020)

Let $r \geq 1$ be an integer. For every i, $1 \leq i \leq r$, let $f_i(z) \in \overline{\mathbb{Q}}[[z]]$ be an irrational solution to a q_i-Mahler equation. Assume that $q_1, \ldots, q_r$ are pairwise multiplicatively independent. Then $f_1(z), \ldots, f_r(z)$ are algebraically independent over $\overline{\mathbb{Q}}(z)$.

Proof. Let us assume that the functions $f_1(z), \ldots, f_r(z)$ are all irrational. Then, they are all transcendental over $\overline{\mathbb{Q}}(z)$.

As a consequence of a theorem of Nishioka, it is known that any transcendental M-function takes transcendental values at all algebraic points in some suitable punctured neighborhood of 0. Hence, there exists $r > 0$ such that for all $\alpha \in \overline{\mathbb{Q}}$, $0 < |\alpha| < r$, the numbers $f_1(\alpha), \ldots, f_r(\alpha)$ are all transcendental.

Let us pick such α. Applying Part (ii) of our main theorem with $\alpha_1 = \cdots = \alpha_r = \alpha$, we obtain that the numbers $f_1(\alpha), \ldots, f_r(\alpha)$ are algebraically independent over $\overline{\mathbb{Q}}$. Hence the functions $f_1(z), \ldots, f_r(z)$ are algebraically independent over $\overline{\mathbb{Q}}(z)$. □