Lecture notes on automatic sequences Krakow October 2013

J.-P. Allouche
CNRS, Institut de Mathématiques de Jussieu
Équipe Combinatoire et Optimisation
Université Pierre et Marie Curie, Case 247
4 Place Jussieu
F-75252 Paris Cedex 05 France
allouche@math.jussieu.fr

1 Introduction

In two seminal papers dated 1906 and 1912 [50, 51], Thue, starting with a seemingly innocent question (is it possible to find an infinite sequence on two symbols that has no cubes in it, i.e., no three consecutive occurrences of the same "block" of terms?), founded what became half a century later the field of "combinatorics of words". His answer to this question involves the infinite sequence

$$0\ 1\ 1\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 0\ 1\ 0\ 1\ 1\ 0\ \ldots$$

which is now known as the (Prouhet)-Thue-Morse sequence. The sequence was rediscovered by Morse in 1921 [40], but was already used by Prouhet in 1851 [41] for what is now known as the Prouhet-Tarry-Escott problem. This sequence about which more will be said below is somehow *ubiquitous* [16]. In particular it is one of the simplest non-periodic "automatic sequences".

The notion of "automatic sequence" or sequence generated by a finite automaton (more precisely a finite automaton with output function, also called a "uniform tag system") was introduced and studied by Cobham in 1972 (see [27]; see also [32]). In 1979 Christol [25] (also see the paper by Christol, Kamae, Mendès France and Rauzy in 1980 [26]), proved that a sequence with values in a finite field is "automatic" if and only if the corresponding formal power series is algebraic over the field of rational functions with coefficients in this field: this was the starting point of numerous results relating automata theory, combinatorics and number theory. We will survey results in this area, including some transcendence results, and provide the reader with examples of automatic sequences. We will also give a bibliography where more detailed studies can be found. See in particular the survey of Dekking, Mendès France and van der Poorten [30], or the author's [4], where many relations between finite automata and number theory (and between finite automata and other mathematical fields) are described. For early applications of finite automata to physics see [8]. In 2003 a book by the author and Shallit [17] gathered (or at least tried to gather) the results available at that time for automatic sequences in mathematics, computer science and physics. We are not going to update the book in this much shorter paper, but we will try to point at least a few significant more recent references, in particular for the transcendence of "automatic real numbers".

In the first part of this paper we will recall the basic definitions and give several typical examples of sequences generated by finite automata. We will then state and prove the theorem of Christol.

In a second part we will discuss transcendence results related to automata theory, giving in particular some results concerning the Carlitz zeta function. This part will also describe results on transcendence of real numbers.

We will indicate in a third part of this paper possible generalizations of automatic sequences.

A part will be devoted to automatic Dirichlet series through the example of the ± 1 Thue-Morse Dirichlet series.

A penultimate part will discuss some open questions.

Finally in an appendix we will give an elementary "automatic" proof of the transcendence of the Carlitz formal power series Π.

2 Generalities, examples, the main theorem

2.1 Alphabets, words, free monoids, and morphisms

We first introduce some notation.

Definition 1 An *alphabet* is a finite set. We let A^* denote the set of all finite sequences of elements of the alphabet A. The elements of A^* are called *words* over A. The empty word is an element of A^*. The set A^* is equipped with the *concatenation law* which is clearly associative and admits the empty word as unit, making A^* a monoid. This is the *free monoid* generated by the set A.

The next step is to define the functions "preserving" the structure of monoid: they are called "morphisms" (or "substitutions", or "inflation rules").

Definition 2 Let A and B two alphabets. Let A^* and B^* the free monoids generated by A resp. B. A morphism from A^* to B^* is a map f from A^* to B^* such that for any two words u and v in A^*, we have $f(u.v) = f(u).f(v)$ [concatenation of words is denoted by "." in both monoids], and f sends the empty word to the empty word.

Remark 1 A morphism is defined by the images of letters (hint: a word is the concatenation of its letters).

2.2 Sequences generated by finite automata

Definition 3 Let q be an integer ($q \geq 2$). A q-automaton consists of

- a finite set $S = \{a_1 = i, a_2, \cdots, a_d\}$, which is called the set of states. One of the states is denoted by i and called the initial state,

- q maps from S to itself, labelled $0, 1, \cdots, q-1$. The image of the state s by the map j is denoted by $j.s$,

- a map (the output function), say φ, from S to a set Y.

This automaton generates a sequence $(u_n)_{n\geq 0}$ with values in Y (called a **q-automatic sequence**) as follows: to compute the term u_n, one expands n in base q, say $n = \sum_{j=0}^{\ell} n_j q^j$, with $0 \leq n_j \leq q-1$; then each n_j is interpreted as one of the maps from S to itself; these maps are applied to i to obtain the state $n_\ell(n_{\ell-1}(\cdots(n_1(n_0.i))\cdots))$; and finally u_n is defined by $u_n = \varphi\,[n_\ell(n_{\ell-1}(\cdots(n_1(n_0.i))\cdots))]$.

2.3 Examples

1) The Prouhet-Thue-Morse sequence

This sequence was studied by Thue at the beginning of the last century to give an example of a binary sequence without cubes (i.e., without three consecutive identical blocks, see [50] and [51]), by Morse in 1921, (see [40]), but also by Prouhet in 1851 [41]). It can be defined by the following 2-automaton:

- the set of states is $S = \{i, a\}$,
- the maps 0 and 1 from S to S are defined by

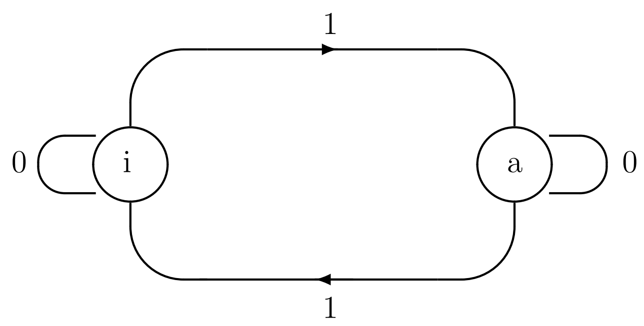
$$0.i = i \qquad 0.a = a \qquad 1.i = a \qquad 1.a = i.$$

- the output function is defined by

$$\varphi(i) = 0,\ \varphi(a) = 1.$$

Hence this sequence begins as follows:

$$0\,1\,1\,0\,1\,0\,0\,1\,1\,0\,0\,1\cdots$$



$\varphi(i) = 0,\ \varphi(a) = 1$

Figure 1: An automaton generating the Prouhet-Thue-Morse sequence

2) The Rudin-Shapiro sequence

Let $a = (a_n)_{n\geq 0}$ be any sequence of ± 1. What can be said about the asymptotic size of the supremum of its Fourier transform

$$F_N(a) = \sup_{x\in[0,1]} \left| \sum_{n=0}^{N-1} a_n e^{2i\pi nx} \right| ?$$

The following bounds are trivial:

$$\sqrt{N} = \left\| \sum_{n=0}^{N-1} a_n e^{2i\pi nx} \right\|_{L^2} \leq \left\| \sum_{n=0}^{N-1} a_n e^{2i\pi nx} \right\|_{L^\infty} = F_N(a) \leq N.$$

On the other hand it is known that, for almost all (in the sense of the Haar measure on $\{-1,+1\}^{\mathbb{N}}$) sequences of ± 1, one has

$$F_N(a) \leq \sqrt{N \log N}.$$

In other words, for a "random" sequence a, $F_N(a)$ behaves roughly like $\sqrt{N}$. Shapiro in 1951 [47] (also see Rudin in 1959 [42]) constructed a sequence a for which $F_N(a) \leq C\sqrt{N}$ and which is *deterministic* for any reasonable definition of this notion. Furthermore this sequence is 2-automatic, and can be generated by the following 2-automaton:

- set of states $S = \{i, a, b, c\}$,
- maps from S to S,

$$0.i = i,\ 0.a = i,\ 0.b = c,\ 0.c = c,$$

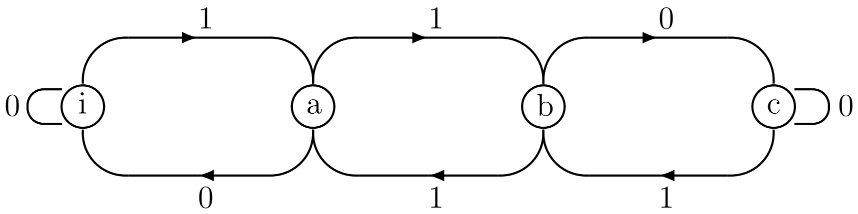
$$1.i = a,\ 1.a = b,\ 1.b = a,\ 1.c = b,$$

- output function,

$$\varphi(i) = \varphi(a) = +1,$$
$$\varphi(b) = \varphi(c) = -1.$$

Hence this sequence begins as follows:

$$+1\ +1\ +1\ -1\ +1\ +1\ -1\ +1\ +1 \cdots$$



$\varphi(i) = \varphi(a) = +1$, $\varphi(b) = \varphi(c) = -1$

Figure 2: An automaton generating the Rudin-Shapiro sequence

3) The paperfolding sequence

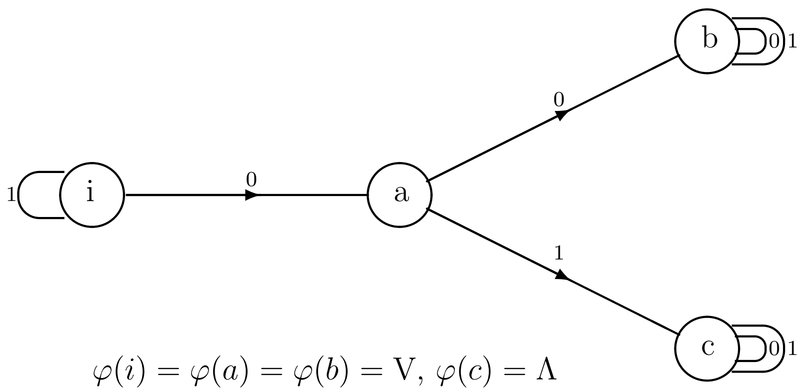
Folding repeatedly a sheet of paper yields a sequence of “peaks” Λ and “valleys” V which was studied by many authors since the paper of Davis and Knuth [29]. This sequence can indeed be generated by the following 2-automaton:

- set of states $S = \{i, a, b, c\}$,
- maps from S to S,

$$0.i = a,\ 0.a = b,\ 0.b = b,\ 0.c = c,\ \ 1.i = i,\ 1.a = c,\ 1.b = b,\ 1.c = c,$$

- output function, $\varphi(i) = \varphi(a) = \varphi(b) = \mathrm{V}$, $\varphi(c) = \Lambda$.

Hence this sequence begins as follows: $\mathrm{V}\,\mathrm{V}\,\Lambda\,\mathrm{V}\,\mathrm{V}\,\Lambda\,\Lambda\,\mathrm{V}\,\cdots$



$\varphi(i) = \varphi(a) = \varphi(b) = \mathrm{V}$, $\varphi(c) = \Lambda$

Figure 3: An automaton generating the paperfolding sequence

4) The Baum-Sweet sequence

It is well known that, if a real number is quadratic over the rationals, then its continued fraction expansion is periodic or ultimately periodic. But nothing is known for algebraic numbers of degree ≥ 3: no example is known with bounded partial quotients, nor with unbounded quotients.

Replacing the real numbers by the field of Laurent series $\mathbb{F}_q((X^{-1}))$ over the finite field $\mathbb{F}_q$, the field of rational numbers by $\mathbb{F}_q(X)$, and the ring of integers $\mathbb{Z}$ by the ring of polynomials $\mathbb{F}_q[X]$, more is known. There is indeed a theory of continued fractions, and the property of bounded partial quotients has to be replaced by the property of quotients of bounded degree (or equivalently quotients taking a finite number of values).

A first result was given by Baum and Sweet in 1976 [18]: *there exists a Laurent series in $\mathbb{F}_2((X^{-1}))$, of degree 3 over $\mathbb{F}_2(X)$, such that its continued fraction has only finitely many partial quotients.* By Christol theorem (where the variable X is replaced by X^{-1}), the sequence of coefficients of the Baum-Sweet series is 2-automatic. Here is a 2-automaton which generates this sequence:

- set of states $S = \{i, a, b\}$,
- maps from S to S,

$$0.i = a,\ 0.a = i,\ 0.b = b,$$

$$1.i = i,\ 1.a = b,\ 1.b = b,$$

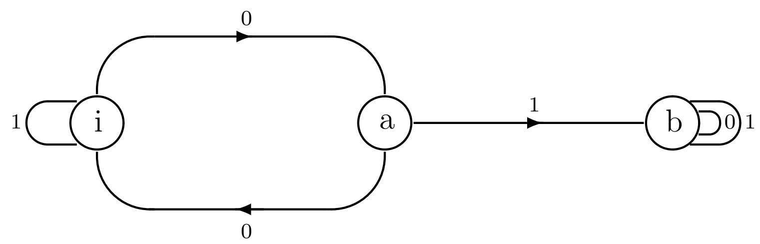
- output function,

$$\varphi(i) = 1,\ \varphi(a) = \varphi(b) = 0.$$

Hence this sequence begins as follows:

$$1\,1\,0\,1\,1\,0\,0\,1\,0\,\cdots$$

It can be proven that the term u_n of the Baum-Sweet sequence u is equal to 1 if and only if there is no string of 0's of odd length in the binary expansion of n. Other examples were given by Mills and Robbins for all characteristics [38]. A natural question due to Mendès France arises: given an algebraic Laurent series whose partial quotients take only a finite number of values, is the sequence of these partial quotients automatic? (remember that the sequence



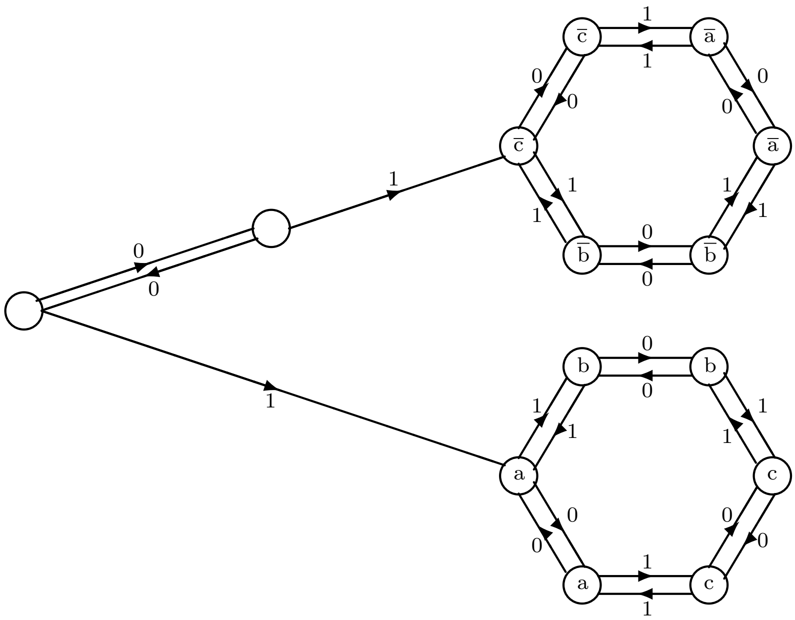
$\varphi(i) = 1,\ \varphi(a) = \varphi(b) = 0$

Figure 4: An automaton generating the Baum-Sweet sequence

of coefficients of the series is itself automatic from Christol's theorem). The answer is yes for the example of Mills and Robbins in characteristic 3, (see [11]), and for their examples in characteristic $p \geq 3$, (see [5]). The sequence of partial quotients of the Baum-Sweet series was proved non-automatic by Mkaouar, [39], but this sequence can be generated by a non-uniform morphism. Many new results were obtained by Lasjaunias (see, e.g., [35] and the references therein).

5) The Hanoi sequence

The well known towers of Hanoi game is the following: N disks of diameter, say $1, 2, \cdots, N$, are stacked on the first of three vertical pegs. At each step one is allowed to pick the topmost disk on a peg and to put it on another one, provided it is not stacked on a smaller disk. The game is over when all the disks are on a (new) peg. A classical recursive algorithm gives a (finite) sequence of moves of length $2^N - 1$, which is optimal, to transfer N disks from the first peg to another one. If one chooses to transfer the disks to the second peg if N is odd, and to the third one if N is even, all the sequences of moves of length $2^N - 1$ given by the algorithm are prefixes of a unique infinite sequence of moves on the six-letter alphabet of all possible moves. It was proved in [13] that this infinite sequence is indeed 2-automatic, and that it can be generated by the 2-automaton given below. Note that in the cyclic towers of Hanoi, (where the pegs are on a circle and where only clockwise moves are allowed), the infinite sequence of moves resulting from the classical cyclic algorithm is NOT automatic, but can be generated by a non-uniform morphism, (see [10]).



(The - significant - states have been replaced by their images by φ)

Figure 5: An automaton generating the Hanoi sequence

2.4 Sequences generated by uniform morphisms

Definition 4 A sequence $u = (u_n)_{n \geq 0}$ with values in a finite set Y is said to be the image of a fixed point of a uniform morphism of length q, (q being an integer ≥ 2), if there exists:

- a set A,

- a uniform morphism σ of length q on A, i. e. a map which associates to each letter in A a q-letter word on A. This map is extended by concatenation to a morphism of the free monoid A^* generated by A, and by continuity to the infinite sequences with values in A,

- a sequence $v = (v_n)_{n \geq 0}$ with values in A, which is a fixed point of σ,

- a map ψ from A to Y such that $\forall n \in \mathbb{N},\ \psi(v_n) = u_n$.

2.5 Examples

The patient reader can check (or prove) that the five examples given previously are images of fixed points of uniform morphisms of length 2, indeed:

1) The Prouhet-Thue-Morse sequence

This sequence is the fixed point of the 2-morphism on $\{0,1\}$ given by:

$$\begin{array}{rcl} \sigma(0) & = & 01, \\ \sigma(1) & = & 10. \end{array}$$

2) The Rudin-Shapiro sequence

Let $A = \{a, b, c, d\}$, define σ on A by:

$$\begin{array}{rcl} \sigma(a) & = & ab, \\ \sigma(b) & = & ac, \\ \sigma(c) & = & db, \\ \sigma(d) & = & dc, \end{array}$$

and let ψ be the map:

$$\psi(a) = \psi(b) = +1,\ \psi(c) = \psi(d) = -1.$$

Then the sequence $v = (v_n)_{n\geq 0}$ defined by $v = \lim_{k\to\infty} \sigma^k(a)$ is a fixed point of σ, and the Rudin-Shapiro sequence is the pointwise image of the sequence v by the map ψ.

3) The paperfolding sequence

Let $A = \{a, b, c, d\}$, define σ on A by:

$$\begin{array}{rcl} \sigma(a) & = & ab, \\ \sigma(b) & = & cb, \\ \sigma(c) & = & ad, \\ \sigma(d) & = & cd, \end{array}$$

and let ψ be the map:

$$\psi(a) = \psi(b) = \mathrm{V},\ \psi(c) = \psi(d) = \Lambda.$$

Then the sequence $v = (v_n)_{n\geq 0}$ defined by $v = \lim_{k\to\infty} \sigma^k(a)$ is a fixed point of σ, and the paperfolding sequence is the pointwise image of the sequence v by the map ψ.

4) The Baum-Sweet sequence

Let $A = \{a, b, c, d\}$, define σ on A by:

$$\begin{array}{rcl} \sigma(a) & = & ab, \\ \sigma(b) & = & cb, \\ \sigma(c) & = & bd, \\ \sigma(d) & = & dd, \end{array}$$

and let ψ be the map:

$$\psi(a) = \psi(b) = 1,\ \psi(c) = \psi(d) = 0.$$

Then the sequence $v = (v_n)_{n\geq 0}$ defined by $v = \lim_{k\to\infty} \sigma^k(a)$ is a fixed point of σ, and the Baum-Sweet sequence is the pointwise image of the sequence v by the map ψ.

5) The Hanoi sequence

This sequence is the fixed point of the 2-morphism σ defined on the alphabet $A = \{a, b, c, \overline{a}, \overline{b}, \overline{c}\}$ by:

$$\begin{array}{rcl} \sigma(a) & = & a\overline{c}, \\ \sigma(b) & = & c\overline{b}, \\ \sigma(c) & = & b\overline{a}, \\ \sigma(\overline{a}) & = & ac, \\ \sigma(\overline{b}) & = & cb, \\ \sigma(\overline{c}) & = & ba. \end{array}$$

2.6 The main theorem

It is not by chance that our five examples are simultaneously 2-automatic and images of fixed points of uniform morphisms of length 2. Indeed a theorem due to Cobham, [27], asserts that this is general:

Theorem 1 [27]. *A sequence is q-automatic if and only if it is the image of a fixed point of a q-substitution.*

The proof of this theorem uses a combinatorial property of these sequences: both properties above are equivalent to saying that the set of subsequences $N_q(u)$ defined by:

$$N_q(u) = \left\{n \to u_{q^k n+a},\ k \geq 0,\ 0 \leq a \leq q^k - 1\right\},$$

(also called the q-kernel of the sequence u, see [44]), is finite.

Christol in 1979 [25], then Kamae, Mendès France and Rauzy in 1980 [26], gave an arithmetical condition which is equivalent to the theoretical-computer-science condition and to the combinatorial condition given above:

Theorem 2 [25, 26]. *Let u be a sequence with values in the finite field $\mathbb{F}_q$, (q is a power of a prime number p). Then the sequence u is q-automatic if and only if the formal power series $\sum_{n=0}^{+\infty} u_n X^n$ is algebraic over the field $\mathbb{F}_q(X)$ of rational functions with coefficients in $\mathbb{F}_q$.*

Remarks

- this theorem has, of course, nothing to do with the Chomsky-Schützenberger theorem, [24];

- to give the flavour of this theorem, let us consider again the Prouhet-Thue-Morse sequence quoted above. Recall that this sequence is the fixed point of the 2-morphism σ defined by:

$$\begin{aligned} \sigma(0) &= 01, \\ \sigma(1) &= 10. \end{aligned}$$

We consider from now on 0 and 1 as the two elements of $\mathbb{F}_2$ and we make all computations modulo 2. The definition of our sequence u by the morphism σ shows that:

$$\forall n \in \mathbb{N},\ u_{2n} = u_n,\ u_{2n+1} = 1 + u_n.$$

Hence:

$$\begin{aligned} F(X) &:= \sum_{n=0}^{+\infty} u_n X^n = \sum_{n=0}^{+\infty} u_{2n} X^{2n} + \sum_{n=0}^{+\infty} u_{2n+1} X^{2n+1} \\ &= \sum_{n=0}^{+\infty} u_n X^{2n} + \sum_{n=0}^{+\infty} (1 + u_n) X^{2n+1} \end{aligned}$$

$$
\begin{aligned}
&= \left(\sum_{n=0}^{+\infty} u_n X^n\right)^2 + X\left(\sum_{n=0}^{+\infty} u_n X^n\right)^2 + \frac{X}{(1+X)^2} \\
&= F^2(X) + XF^2(X) + \frac{X}{(1+X)^2}.
\end{aligned}
$$

One sees that F satisfies the equation:

$$(1+X)^3 F^2 + (1+X)^2 F + X = 0,$$

which shows that F is algebraic (quadratic) on $\mathbb{F}_2(X)$.

Another condition can be given for the automaticity of a sequence with values in a finite field. This is a theorem of Furstenberg's, which he proved in 1967, [33]:

Theorem 3 [33]. *Let $u = (u_n)_{n\geq 0}$ be a sequence with values in the finite field $\mathbb{F}_q$. Then the series $\sum u_n X^n$ is algebraic over the field $\mathbb{F}_q(X)$ if and only if there exists a double formal power series $\sum_{m,n\geq 0} a_{m,n} X^m Y^n$ such that*
- this series is a rational function, i.e., belongs to the field $\mathbb{F}_q(X, Y)$,
- the sequence u is the diagonal of the sequence a, i.e., $\forall n \in \mathbb{N}, u_n = a_{n,n}$.

Putting all these conditions together one obtains the following fundamental theorem:

Fundamental Theorem *Let $u = (u_n)_{n\geq 0}$ be a sequence with values in the finite field $\mathbb{F}_q$. Then the following conditions are equivalent:*
i) the q-kernel of the sequence u, i.e., the set of subsequences

$$N_q(u) = \left\{n \to u_{q^k n + a},\ k \geq 0,\ 0 \leq a \leq q^k - 1\right\},$$

is finite,
ii) the sequence u is q-automatic,
iii) the sequence u is the image of a fixed point of a uniform morphism of length q,
iv) the formal power series $\sum_{n=0}^{+\infty} u_n X^n$ is algebraic over the field $\mathbb{F}_q(X)$,
v) there exists a double sequence $a = (a_{m,n})_{m,n}$ with values in $\mathbb{F}_q$ such that the formal power series $\sum_{m,n\geq 0} a_{m,n} X^m Y^n$ is a rational function, (i.e., an element of $\mathbb{F}_q(X, Y)$), and such that u is the diagonal of a, (i.e., $\forall n \in \mathbb{N}, u_n = a_{n,n}$).

2.7 Proof of Christol's theorem

We prove the following.

Let p be a prime number. Let q be a power of p. Let $\mathbf{a} = (a_i)_{i\geq 0}$ be a sequence over $\mathbb{F}_q$. Then $\mathbf{a}$ is q-automatic if and only if the formal power series $\sum_{i\geq 0} a_i X^i$ is algebraic over $\mathbb{F}_q(X)$.

($\Rightarrow$): Let us prove that $\sum_{i\geq 0} a_i X^i$ is algebraic over $\mathbb{F}_q(X)$.

Since $(a_i)_{i\geq 0}$ is q-automatic its q-kernel $K_q(\mathbf{a})$ is finite, say $K_q(\mathbf{a}) = \{\mathbf{a}^{(1)}, \mathbf{a}^{(2)}, \ldots, \mathbf{a}^{(d)}\}$, with $\mathbf{a}^{(1)} = \mathbf{a}$. Write $\mathbf{a}^{(i)} = (a_n^{(i)})_{n\geq 0}$. Define

$$F_j(X) = \sum_{n\geq 0} a_n^{(j)} X^n \quad \text{for } 1 \leq j \leq d.$$

Then, for $1 \leq j \leq d$

$$\begin{aligned} F_j(X) &= \sum_{0\leq r\leq q-1} \sum_{m\geq 0} a_{qm+r}^{(j)} X^{qm+r} \\ &= \sum_{0\leq r\leq q-1} X^r \sum_{m\geq 0} a_{qm+r}^{(j)} X^{qm}. \end{aligned}$$

But the sequence $(a_{qm+r}^{(j)})_{m\geq 0}$ is one of the $a^{(i)}$'s, which shows that $F_j(X)$ is a $\mathbb{F}_q[X]$-linear combination of the power series $F_i(X^q)$. In other words $F_j(X)$ belongs to the $\mathbb{F}_q(X)$-vector space generated by the series $F_i(X^q)$:

$$\forall j \in [1,d],\ F_j(X) \in \langle F_1(X^q), F_2(X^q), \ldots, F_d(X^q)\rangle.$$

But this implies that

$$\forall j \in [1,d],\ F_j(X^q) \in \langle F_1(X^{q^2}), F_2(X^{q^2}), \ldots, F_d(X^{q^2})\rangle,$$

and also, by transitivity, that

$$\forall j \in [1,d],\ F_j(X) \in \langle F_1(X^{q^2}), F_2(X^{q^2}), \ldots, F_d(X^{q^2})\rangle.$$

Hence

$$\forall j \in [1,d],\ F_j(X) \text{ and } F_j(X^q) \in \langle F_1(X^{q^2}), F_2(X^{q^2}), \ldots, F_d(X^{q^2})\rangle.$$

This implies that

$$\forall j \in [1,d],\ F_j(X^q) \text{ and } F_j(X^{q^2}) \in \langle F_1(X^{q^3}), F_2(X^{q^3}), \ldots, F_d(X^{q^3})\rangle.$$

Hence

$$\forall j \in [1,d],\ F_j(X),\ F_j(X^q) \text{ and } F_j(X^{q^2}) \in \langle F_1(X^{q^3}), F_2(X^{q^3}), \ldots, F_d(X^{q^3})\rangle.$$

Iterating the reasoning we finally have

$$\forall j \in [1,d],\ \forall k \in [0,d],\ F_j(X^{q^k}) \in \langle F_1(X^{q^{d+1}}), F_2(X^{q^{d+1}}), \ldots, F_d(X^{q^{d+1}})\rangle.$$

But the dimension of $\langle F_1(X^{q^{d+1}}), F_2(X^{q^{d+1}}), \ldots, F_d(X^{q^{d+1}})\rangle$ as a vector space over $\mathbb{F}_q(X)$ is at most d, the number of generators, so for any $j \in [1,d]$, the formal power series

$$F_j(X), F_j(X^q), \ldots, F_j(X^{q^d})$$

are linearly related over $\mathbb{F}_q(X)$. In particular for $j = 1$, this gives that $F_1(X) = \sum_{i\geq 0} a_i^{(1)} X^i$ is algebraic over $\mathbb{F}_q(X)$.

($\Rightarrow$): Suppose that $F(X) = \sum_{i\geq 0} a_i X^i$ is algebraic over $\mathbb{F}_q(X)$. Then there exist polynomials $B_0(X), \ldots, B_t(X)$ such that

$$\sum_{0\leq i\leq t} B_i(X) F(X)^{q^i} = 0,$$

and $B_0 \neq 0$. Namely suppose that we have a relation

$$\sum_{j\leq i\leq t} B_i(X) F(X)^{q^i} = 0,$$

with $a_j \neq 0$ and j is minimal. If j were not equal to 0, applying Λ_r would give

$$\sum_{j\leq i\leq t} \Lambda_r(B_i)(X)^{q^{i-1}} = 0,$$

But there exists $r \in [0, q-1]$ such that $\Lambda_r(B_j) \neq 0$, (otherwise one would have $B_j = 0$) thus the relation above would contradict the definition of j.

Now put $G = \frac{F(X)}{B_0(X)}$; then

$$G = \sum_{1\leq i\leq t} C_i G^{q^i} \quad \text{where } C_i = -B_i B_0^{q^i-2}.$$

Now let

$$N = \max(\deg B_0, \max_i \deg C_i)$$

and let $\mathcal{H}$ be defined as follows:

$$\mathcal{H} = \left\{ H \in \mathbb{F}_q[[X]] : H = \sum_{0 \le i \le t} D_i G^{q^i} \text{ with } D_i \in \mathbb{F}_q[X] \text{ and } \deg D_i \le N \right\}.$$

Now $\mathcal{H}$ is a finite set and $F = B_0 G$ belongs to $\mathcal{H}$. We now prove that $\mathcal{H}$ is mapped into itself by Λ_r. Let $H \in \mathcal{H}$. Then

$$\begin{array}{rcl} \Lambda_r(H) & = & \Lambda_r\left(D_0 G + \sum_{1 \le i \le t} D_i G^{q^i}\right) = \Lambda_r\left(\sum_{1 \le i \le t} (D_0 C_i + D_i) G^{q^i}\right) \\ & = & \sum_{1 \le i \le t} \Lambda_r(D_0 C_i + D_i) G^{q^{i-1}} \end{array}$$

Since $\deg D_0, \deg D_i, \deg C_i \le N$, it follows that $\deg(D_0 C_i + D_i) \le 2N$, and so

$$\deg(\Lambda_r(D_0 C_i + D_i)) \le \frac{2N}{q} \le N.$$

Then considering the set of sequences of coefficients of elements of $\mathcal{H}$ we see that this set is finite, contains the sequence $\mathbf{a}$, and is stable by the maps $(v_n)_{n \ge 0} \to (v_{qn+j})_{n \ge 0}$. Thus the q-kernel of $\mathbf{a}$ is finite and $\mathbf{a}$ is q-automatic $\square$

3 Transcendence results and finite automata

In this chapter we will see two kinds of transcendence results:

- transcendence over $\mathbb{F}_q(X)$ of formal power series with coefficients in $\mathbb{F}_q$, using Christol's theorem. In particular we will devote a paragraph to the Carlitz zeta function.

- transcendence of real numbers over the rational numbers.

3.1 Miscellaneous transcendental formal power series

- An old question of Mahler's asks whether a binary sequence $(a_n)_n$ such that both numbers $\sum_{n=0}^{+\infty} a_n 2^{-n}$ and $\sum_{n=0}^{+\infty} a_n 3^{-n}$ are algebraic over the rational numbers is necessary an ultimately periodic sequence, (i.e., whether both numbers are "trivial", indeed whether they are both rational). Actually, although this question is still open, the result is true if one replaces the usual operations by operations without carries:

Theorem 4 *Let $(a_n)_n$ be a binary sequence such that the formal power series $\sum_{n=0}^{+\infty} a_n X^n$ is algebraic over $\mathbb{F}_2(X)$ when considered as an element of $\mathbb{F}_2[[X]]$, and algebraic over $\mathbb{F}_3(X)$ when considered as an element of $\mathbb{F}_3[[X]]$. Then this sequence is ultimately periodic, i.e., both formal power series are indeed rational functions.*

The proof of this result is an easy consequence of the theorem of Christol and of a (far from easy to prove!) result of Cobham which asserts that a sequence which is both q-automatic and q'-automatic, with q and q' multiplicatively independent (i.e., $\log q / \log q'$ irrational), must be ultimately periodic, [28].

- Let $s_q(n)$ be the residue modulo q of the sum of the digits of the integer n in its q-ary expansion. It is not hard to see that the sequence $(s_q(an+b))_n$ is q-automatic; in particular for $q = 2$, $a = 1$, $b = 0$, one gets the Prouhet-Thue-Morse sequence. But what can be said of $(s_q(n^2))$? A result of the author [3], states that this sequence is NOT q-automatic.

Theorem 5 [3]. *Let P be a polynomial of degree ≥ 2, such that $P(\mathbb{N}) \subset \mathbb{N}$. Then the sequence $(s_q(P(n))_n$ is not q-automatic. Hence, if q is a prime number, the formal power series $\sum s_q(P(n))X^n$ is transcendental over $\mathbb{F}_q(X)$.*

- As seen previously, the paperfolding sequence is 2-automatic, hence the paperfolding series is algebraic over $\mathbb{F}_2(X)$. Now suppose that at each step you choose to fold either up or down arbitrarily; you thus obtain an uncountable number of paperfolding sequences. Of course they cannot be all automatic, as the set of automatic sequences is countable. It can be proven that such a sequence is 2-automatic if and only if the sequence of its "folding instructions" (i e., the sequence of choices to fold one way or the other way) is ultimately periodic: in other words any non-ultimately periodic sequence of folding instructions yields a formal power series which is transcendental over $\mathbb{F}_2(X)$.

3.2 The Carlitz zeta function

In 1935 Carlitz introduced a function now known as the Carlitz zeta function which ressembles the Riemann zeta function (see for instance [23]). This function from $\mathbb{N}^*$ to $\mathbb{F}_q[[X^{-1}]]$ is defined by:

$$\forall n \in \mathbb{N}^*,\ \zeta(n) = \sum_{P \text{ monic } \in \mathbb{F}_q[X]} \frac{1}{P^n}.$$

Furthermore there exists a formal Laurent series denoted by Π such that:

$$\forall n \equiv 0 \bmod (q-1),\ n \neq 0,\ \exists r_n \in \mathbb{F}_q(X),\ \zeta(n) = \Pi^n r_n.$$

The expression for Π is:

$$\Pi = \prod_{j=1}^{+\infty} \left(1 - \frac{X^{q^j} - X}{X^{q^{j+1}} - X}\right).$$

Note that this property can be compared to the classical result on the values of the Riemann zeta function at the even integers.

One can ask whether this formal Laurent series Π, the values of this zeta function, and the values $\frac{\zeta(n)}{\Pi^n}$ are transcendental over $\mathbb{F}_q(X)$. Recall that the real number π is transcendental over the field of rational numbers, hence the values of the Riemann zeta function at the even integers are also transcendental, as the numbers $\zeta(2n)/\pi^{2n}$ are rational. For the other values of the Riemann zeta function, (divided by a suitable power of π or not), the only thing which is known is the irrationality of $\zeta(3)$ proved by Apéry in 1978.

Four methods are available for the Carlitz zeta function and the related series:

- the original method due to Wade in the 40's, (he proved many transcendence results, in particular *the transcendence of the formal power series* Π), ressembles transcendence methods for the case of real numbers. This method has been extended recently by Dammame and Hellegouarch, who proved the *transcendence of all the values* $\zeta(n)$, $\forall n \in \mathbb{N}^*$;

- the method of diophantine approximation is worked out by de Mathan and Chérif and gives *irrationality measures for the values of the Carlitz zeta function*;

- the method of Yu uses Drinfeld modules and gives the most complete results, indeed $\zeta(n)$ *is transcendental* $\forall n \in \mathbb{N}^*$ *and* $\frac{\zeta(n)}{\Pi^n}$ *is transcendental for every* $n \not\equiv 0 \bmod (q-1)$;

- the "automatic method". This method was proposed by the author to give *an "elementary" proof of the transcendence of the formal series* Π, (see

[7]). The reader will find in the appendix a different (but even simpler) proof of the transcendence of this series Π. This "automatic" method was extended by Berthé: she gave an elementary automatic proof of *the transcendence of* $\zeta(n)$, $\forall n \leq q-2$, (see [19]), as well as *linear independence results for these series*, [20], and *transcendence results for the Carlitz logarithm*, (see [21]).

3.3 Transcendence of real numbers and finite automata

The consequence of Cobham's theorem quoted above (Theorem 4) can be described, roughly speaking, by saying: *"changing bases kills algebraicity"*. Hence a natural question posed in [26] asks whether every real number $\sum a_n 2^{-n}$ such that the sequence of coefficients in its base-2 expansion is 2-automatic and not ultimately periodic is indeed a transcendental number. The answer is yes. Partial results were proven by Loxton and van der Poorten, (also see the work of Nishioka). The final result is due to Adamczeski and Bugeaud [1] (also see [2]).

Theorem 6 [1]. *If the coefficients of the base-q expansion of a real number form an automatic sequence, then this number is either rational or transcendental.*

In other words a number like $\sqrt{2}$ cannot have an automatic expansion in any base. Note that this theorem gives the transcendence of a countable set of "ad hoc" real numbers, and that one should not hope to get that way the transcendence of classical numbers like the Euler constant (!), even for numbers which are known to be transcendental: a reasonable but out of reach conjecture is that the real numbers π and e are not automatic. Note also that Mendès France and van der Poorten proved that a real number whose base-2 expansion is any paperfolding sequence is transcendental, (see [37]), this gives an uncountable (but "thin") set of numbers, (which of course are not all automatic numbers), for which the transcendence can be proved using this kind of methods.

4 Generalizations

In this chapter we will survey quickly some possible generalizations of the automatic sequences. The interested reader can find an early survey with more details in [9], in particular what is kept and what is lost in each of these generalizations.

4.1 The multidimensional case

Instead of considering one-dimensional morphisms which consist of replacing a letter by a word, one can imagine of a multidimensional morphism. Thus a two-dimensional morphism associates to each letter a "square", for instance:

$$0 \to \begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array}, \quad 1 \to \begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array}.$$

This can be extended as previously, iterating this map gives:

$$0 \to \begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array} \to \begin{array}{cccc} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{array} \to \cdots$$

The reader can find in [43] and [44] more details, in particular a theorem analogous to Christol's holds true.

4.2 Non-uniform morphisms

A non-uniform morphism maps each letter of a finite alphabet on a word with letters in this alphabet, but all these words do not have necessarily the same length. A classical example is the Fibonacci morphism defined on $\{0, 1\}$ by:

$$0 \to 01, \ 1 \to 0.$$

Iterating this morphism gives:

$$0 \to 01 \to 010 \to 01001 \to 01001010 \to \cdots$$

The arithmetic properties of the infinite sequences which are (images of) fixed points of these morphisms are not very simple as the numeration base associated to them is not the base q for some integer $q \geq 2$. For instance, in the above example, the numeration base is the Fibonacci base: $F_0 = 1$, $F_1 = 2$, $F_2 = 3$, $F_3 = 5$, $\cdots$

On this subject one can read the paper of Shallit [45], and also the work of Fabre.

4.3 From finite fields to fields of positive characteristic

Recall that the theorem of Christol can be stated in the following way, (see Theorem 2):

Let q be an integer ≥ 2. For a sequence $u = (u_n)_n$ define its q-kernel as the set of subsequences

$$N_q(u) = \left\{n \to u_{q^k n + a},\ k \geq 0,\ 0 \leq a \leq q^k - 1\right\}.$$

Suppose that u takes its values in the finite field $\mathbb{F}_q$. Then the series $\sum u_n X^n$ is algebraic over $\mathbb{F}_q(X)$ if and only if its q-kernel $N_q(u)$ is finite.

The main result obtained by Sharif and Woodcock in [48] and Harase in [34] (see also the survey of the author [6]), can be stated as follows:

Theorem 7 [48], [34]. *Let u be a sequence with values in a field K of positive characteristic p. Let s be any integer ≥ 1, $q = p^s$, and let $\overline{K}$ be a perfect field containing K, (for instance its algebraic closure).*

Then the series $\sum u_n X^n$ is algebraic over $K(X)$ if and only if the vector space spanned over $\overline{K}$ by the "modified" q-kernel of u

$$N'_q(u) = \left\{n \to u_{q^k n + a}^{1/q^k},\ k \geq 0,\ 0 \leq a \leq q^k - 1\right\}.$$

has finite dimension.

Note that this theorem contains Christol's theorem, and that it can be easily extended to the multidimensional case. Note also that two interesting corollaries can been proved, using the work of Salon for a finite field, or more generally the above theorem for a field of positive characteristic, (these results were first given by Deligne by a non-elementary method in [31]):

- *the Hadamard product of two algebraic formal power series with coefficients in a field of positive characteristic, $\sum u_n X^n$ and $\sum v_n X^n$, i.e., the "naive" product $\sum u_n v_n X^n$, is itself an algebraic formal power series.*

- *let $\sum u_{m,n} X^m Y^n$ be a double formal power series in $K[[X,Y]]$, algebraic over $K(X,Y)$, (where K is a field of positive characteristic). Then its diagonal $\sum u_{n,n} X^n$ is algebraic over the field $K(X)$.*

4.4 q-regular sequences

Let $s(n)$ be the sum of the digits of n in the binary expansion, then the sequence $(s(n))_n$ mod 2 is the Prouhet-Thue-Morse sequence, hence is a 2-automatic sequence. What can be said of the sequence $(s(n))_n$ not reduced modulo 2?

The notion of q-regular sequence was introduced by Shallit and the author in [15] *inter alia* in order to answer this question.

Let q be an integer ≥ 2. Let $u = (u_n)_n$ be a sequence with values in a Nœtherian ring R. This sequence is said to be q-regular if its kernel $N_q(u)$ generates a module of finite type.

Recall the definition of the q-kernel of the sequence u:

$$N_q(u) = \left\{ n \to u_{q^k n+a},\ k \geq 0,\ 0 \leq a \leq q^k - 1 \right\}.$$

The reader is referred to [15] for the properties of these sequences and for numerous examples of such sequences, together with "their Sloane numbers" for the sequences which are quoted in Sloane's book [49].

5 Automatic Dirichlet series

A motivation for introducing automatic Dirichlet series was the following relation (here ε_n is the Thue-Morse sequence with values ± 1 obtained by replacing in the Thue-Morse sequence above 0's by 1's and 1's by -1's)

$$\prod_{n \geq 0} \left(\frac{2n+1}{2n+2} \right)^{\varepsilon_n} = \frac{\sqrt{2}}{2}.$$

We will address the case of the Dirichlet series with coefficients ε_n. For more details the reader can look at the papers(s) [12] and [14].

Theorem 8 *Let f the Dirichlet series be defined for $\Re(s) > 1$ by $f(s) = \sum_{n \geq 0} \frac{\varepsilon_n}{(n+1)^s}$. Then f can be continued to an entire function which satisfies the infinite functional equation $f(s) = \sum_{k \geq 1} \binom{s+k-1}{k} \frac{s+k}{2^{s+k}}$. Furthermore $f(0) = f(-1) = f(-2) = ... = 0$ and $f(2ik\pi/\log 2) = 0$ for all integers k.*

Proof. Using the relations $\varepsilon_{2n} = \varepsilon_n$ and $\varepsilon_{2n+1} = -\varepsilon_n$, we can write for $\Re(s) > 1$

$$\begin{aligned}
f(s) &= \sum_{n\geq 0} \frac{\varepsilon_n}{(2n+1)^s} - \sum_{n\geq 0} \frac{\varepsilon_n}{2^s(n+1)^s} \\
&= \sum_{n\geq 0} \frac{\varepsilon_n}{2^s(n+1)^s} \left(\left(1 - \frac{1}{2(n+1)}\right)^{-s} - 1 \right) \\
&= \sum_{n\geq 0} \frac{\varepsilon_n}{2^s(n+1)^s} \left(\sum_{k\geq 1} \binom{s+k-1}{k} \frac{1}{2^k(n+1)^k} \right) \\
&= \sum_{k\geq 1} \binom{s+k-1}{k} \frac{f(s+k)}{2^{s+k}}
\end{aligned}$$

But the right side of this equality converges for $\Re(s) > 0$ (note that $f(s)$ tends to 1 as s goes to infinity), hence this equality gives an analytic continuation of f for $0 < \Re(s) \leq 1$ which satisfies the same infinite functional equation. This in turn give an analytic continuation of f for $-1 < \Re(s) \leq 0$ satisfying the same infinite functional equation... and finally an analytic continuation of f to $\mathbb{C}$ which still satisfies this infinite functional equation.

The fact that $f(0) = 0$ is due to $\binom{s+k-1}{k} = 0$ for all $k \geq 1$. The values $f(-r) = 0$ for r any positive integer are obtained by "propagating" the value $f(0)$.

We then introduce another Dirichlet series, namely $g(s) = \sum_{n\geq 1} \frac{\varepsilon_n}{(n+1)^s}$. Decomposing g into two sums as was done for f gives

$$g(s) = \sum_{n\geq 1} \frac{\varepsilon_n}{2^s n^s} - \sum_{n\geq 0} \frac{\varepsilon_n}{(2n+1)^s}.$$

This first gives that

$$g(s)\left(1 - \frac{1}{2^s}\right) = -f(s)\left(1 + \frac{1}{2^s}\right)$$

and second that, mimicking the for f, that g can be continued to an entire function that satisfies an infinite functional equation somehow similar to the one satisfied by f. Then $g(0) = -1$ and $g(-r) = 0$ for r any positive integer. The relation between f and g shows that the numbers $2ik\pi/\log 2$ are zeros of f. $\square$

6 Some open questions

Several open questions were given in thh book [17]. Some of them were solved in the last years (see [46]). We give here a short list of questions.

- The theorem of Christol gives a relation between a combinatorial property of the coefficients of a formal power series (over a finite field) and an algebraic property of the series. Is there a similar statement relating in a combinatorial way the sequences $(a_n)_n$ and $(b_n)_n$ and the fact that the formal power series $\sum a_n X^n$ and $\sum b_n X^n$ are algebraically dependent?

- [Christol] A formal power series with is said to be *D-finite* (i.e., *differentially finite*) or *holonomic* if there is a non-trivial linear relation with polynomial coefficients between the series and its derivatives. Is it true that the reduction modulo p of a D-finite series with coefficients in $\mathbb{Z}$ is algebraic over $\mathbb{F}_p(X)$ for all but finitely many primes p (hence that its coefficients modulo p form a p-automatic sequence)?

- Is there a "conceptual" link between Drinfeld modules (that are a powerful tool to address questions of transcendence à la Carlitz) and Christol's theorem?

- Study the relation between q-regular formal power series and series satisfying Mahler equations (see in particular the work of P. Dumas). Is there a characterization of Mahler series in terms of the kernel of the sequence of their coefficients?

- Is there a characterization of "k-synchronized" series (see in particular [22]) in terms of the kernel of the sequence of their coefficients?

- Must a real number whose base-b expansion is morphic (i.e., generated by iterating a morphism, and taking a pointwise image, where the morphism is not necessarily uniform) be either rational or transcendental (i.e., never algebraic irrational)?

- Must a real number whose continued fraction expansion is morphic (i.e., generated by iterating a morphism, and taking a pointwise image, where the morphism is not necessarily uniform) be either quadratic or transcendental (i.e., never algebraic of degree ≥ 3)?

- Are there other zeros than the non-positive integers and the complex numbers $2ik\pi/\log 2$ for the ± 1 Thue-Morse Dirichlet series $\sum_{n\geq 1} \frac{\varepsilon_n}{(n+1)^s}$?
- Is the Flajolet-Martin constant $\prod_{n\geq 1} \left(\frac{2n}{2n+1}\right)^{\varepsilon_n}$ transcendental? (where, as above, ε_n is the ± 1 Thue-Morse sequence).
- [Allouche-Cosnard-Han-Niu-Wen] Describe all the automatic (or morphic) sequences belonging to the set

  $$\Gamma := \{A \in \{0,1\}^{\mathbb{N}},\ \forall k \ \ \overline{A} \leq S^k A \leq A\}$$

  ($\leq$ is the lexicographical order, S is the shift, $\overline{A}$ is obtained from A by changing 0's into 1's and 1's into 0's).

7 Appendix: an easy "automatic" proof of the transcendence of the formal power series Π

As said in chapter 3.2 the Carlitz formal power series Π, given by

$$\Pi = \prod_{j=1}^{+\infty} \left(1 - \frac{X^{q^j} - X}{X^{q^{j+1}} - X}\right).$$

was proved transcendental by Wade in the 40's. We gave an "automatic" proof of this result in [7]. We want to present now another - still simpler - "automatic" proof.

The first step consists of a remark due to Laurent Denis concerning an expression for $\frac{\Pi'}{\Pi}$. Indeed taking the derivative of the expression of $\Pi \in \mathbb{F}_q((X^{-1}))$, one has:

$$\frac{\Pi'}{\Pi} = \sum_{j=1}^{+\infty} \frac{\left(1 - \frac{X^{q^j}-X}{X^{q^{j+1}}-X}\right)'}{\left(1 - \frac{X^{q^j}-X}{X^{q^{j+1}}-X}\right)} = \sum_{j=1}^{+\infty} \frac{1}{X^{q^{j+1}} - X}.$$

A traditional notation is $[j] = X^{q^j} - X$, hence the above equality can be written

$$\frac{\Pi'}{\Pi} = \sum_{j=1}^{+\infty} \frac{1}{[j+1]}.$$

If Π were algebraic, that would be the case also for Π', (the proof is left to the reader who might use - for instance - the Christol theorem, where the variable X is replaced by X^{-1}), hence for $\frac{\Pi'}{\Pi}$.

Finally to prove the transcendence of Π it suffices to prove the transcendence of the series $\sum_{j=1}^{+\infty} \frac{1}{[j]}$. This series is known as the "bracket" series and was proved transcendental by Wade, but we gave in [7] an "automatic" proof for the transcendence of slightly more general series. We rewrite here this - easy - proof in the case of the bracket series. One has:

$$\sum_{j=1}^{+\infty} \frac{1}{[j]} = \sum_{j=1}^{+\infty} \frac{1}{X^{q^j} - X} = \sum_{j=1}^{+\infty} \frac{1}{X^{q^j}} \left(1 - \left(\frac{1}{X}\right)^{q^j-1}\right)^{-1}$$

$$= \sum_{\substack{j\geq 1 \\ m\geq 0}} \left(\frac{1}{X}\right)^{q^j+m(q^j-1)} = \frac{1}{X} \sum_{\substack{j\geq 1 \\ m\geq 1}} \left(\frac{1}{X}\right)^{m(q^j-1)} = \frac{1}{X} \sum_{n\geq 1} \left(\sum_{\substack{j,m \\ m(q^j-1)=n}} 1 \right) \frac{1}{X^n}.$$

This last expression can also be written

$$\frac{1}{X} \sum_{n\geq 1} \left(\sum_{\substack{j \\ (q^j-1)|n}} 1 \right) \frac{1}{X^n}.$$

Using the theorem of Christol one sees that the series above is algebraic over $\mathbb{F}_q(X)$ if and only if the sequence

$$n \to \sum_{\substack{j \\ (q^j-1)|n}} 1$$

is q-automatic. So we have to prove that it is not.

But if a sequence v is q-automatic, then the subsequence $n \to v_{q^n-1}$ is ultimately periodic, (hint: the base-q expansion of $q^n - 1$ consists of n digits all equal to $q - 1$). It thus suffices to show that the sequence:

$$n \to \sum_{\substack{j \\ (q^j-1)|(q^n-1)}} 1$$

is not ultimately periodic. But it is well known that $(q^j - 1) \mid (q^n - 1)$ if and only if $j \mid n$. Hence, using the classical notation $\tau(n)$ to denote the number of divisors of the integer n, it suffices to show that the sequence

$$n \to \tau(n)$$

is not ultimately periodic. OF COURSE THIS SEQUENCE HAS TO BE TAKEN modulo p, where p is the characteristic of $\mathbb{F}_q$.

Now, suppose that $(\tau(n))_n \bmod p$ is ultimately periodic. Then there exist two integers $T \geq 1$ and $n_0 \geq 1$ such that:

$$\forall n \geq n_0,\ \forall k \in \mathbb{N},\ \tau(n + kT) \equiv \tau(n) \bmod p.$$

This implies

$$\forall n \geq n_0,\ \forall k \in \mathbb{N},\ \tau(n(1 + kT)) = \tau(n + knT) \equiv \tau(n) \bmod p.$$

Now choose k large enough such that $(1 + kT) \geq n_0$ and $(1 + kT)$ is a prime number, say $\overline{\omega}$: this is possible from the arithmetic progression theorem for prime numbers, (note that this case, i.e., the existence of arbitrarily large prime numbers in the progression $1 + kT$, can be proved in a very elementary way, using cyclotomic polynomials). Taking $n = (1 + kT) = \overline{\omega}$, one gets:

$$\tau(\overline{\omega}^2) \equiv \tau(\overline{\omega}) \bmod p,$$

i.e.,

$$3 \equiv 2 \bmod p,$$

which yields the desired contradiction.

References

[1] B. Adamczewski, Y. Bugeaud, *On the complexity of algebraic numbers I. Expansions in integer bases*, Annals of Math. **165** (2007) 547–565.

[2] B. Adamczewski, Y. Bugeaud, F. Luca, *Sur la complexité des nombres algébriques*, C. R. Acad. Sci. Paris **339** (2004) 11–14.

[3] J.-P. Allouche, *Somme des chiffres et transcendance*, Bull. Soc. Math. France **110** (1982) 279–285.

[4] J.-P. Allouche, *Automates finis en théorie des nombres*, Expo. Math. **5** (1987) 239–266.

[5] J.-P. Allouche, *Sur le développement en fraction continue de certaines séries formelles*, C. R. Acad. Sci. Paris, Série I, **307** (1988) 631–633.

[6] J.-P. Allouche, *Note sur un article de Sharif et Woodcock*, Séminaire de Théorie des Nombres de Bordeaux, Série II, **1** (1989) 163–187.

[7] J.-P. Allouche, *Sur la transcendance de la série formelle* Π, Séminaire de Théorie des Nombres de Bordeaux, Série II, **2** (1990) 103–117.

[8] J.-P. Allouche, *Finite automata in* 1*-dimensional and* 2*-dimensional physics*, Number theory and physics, J.-M. Luck, P. Moussa, M. Waldschmidt (Eds.), Proceedings in Physics, Springer, **47** (1990) 177–184.

[9] J.-P. Allouche, *q-regular sequences and other generalizations of q-automatic sequences*, Lecture Notes in Computer Science, **583** (1992) 15–23.

[10] J.-P. Allouche, *Note on the cyclic towers of Hanoi*, in Number theory, combinatorics and applications to computer science (Marseille, 1991), Theoret. Comput. Sci. **123** (1994) 3–7.

[11] J.-P. Allouche, J. Bétréma and J. Shallit, *Sur des points fixes de morphismes d'un monoïde libre*, Inform. Théor. Appl. **23** (1989) 235–249.

[12] J.-P. Allouche, H. Cohen, *Dirichlet series and curious infinite products*, Bull. Lond. Math. Soc. **17** (1985) 531–538.

[13] J.-P. Allouche and F. Dress, *Tours de Hanoï et automates*, Inform. Théor. Appl. **24** (1990) 1–15.

[14] J.-P. Allouche, M. Mendès France, J. Peyrière, *Automatic Dirichlet series*, J. Number Theory **81** (2000) 359–373.

[15] J.-P. Allouche and J. Shallit, *The ring of k-regular sequences*, Theoret. Comput. Sci. **98** (1992) 163–197.

[16] J.-P. Allouche, J. Shallit, *The ubiquitous Prouhet-Thue-Morse sequence*, in Sequences and their Applications (Singapore, 1998), 1–16, Springer Ser. Discrete Math. Theor. Comput. Sci., Springer, London, 1999.

[17] J.-P. Allouche, J. Shallit, *Automatic Sequences. Theory, Applications, Generalizations*, Cambridge University Press, Cambridge, 2003.

[18] L. E. Baum and M. M. Sweet, *Continued fractions of algebraic power series in characteristic* 2, Ann. of Math. **103** (1976) 539–610.

[19] V. Berthé, *De nouvelles preuves "automatiques" de transcendance pour la fonction zéta de Carlitz*, Journées arithmétiques de Genève, Astérisque **209** (1992) 159–168.

[20] V. Berthé, *Combinaisons linéaires de* $\frac{\zeta(s)}{\Pi^s}$ *sur* $\mathbb{F}_q(x)$, *pour* $1 \leq s \leq (q-2)$, J. Number Theory **53** (1995) 272–299.

[21] V. Berthé, *Automates et valeurs de transcendance du logarithme de Carlitz*, Acta Arithmetica **66** (1994) 369–390.

[22] A. Carpi,C. Maggi, *On synchronized sequences and their separators*, RAIRO Inform. Théor. App. **35** (2001), 513–524.

[23] L. Carlitz, *On certain functions connected with polynomials in a Galois field*, Duke Math. J. **1** (1935) 137–168.

[24] N. Chomsky and M. P. Schützenberger, *The algebraic theory of context-free languages*, in Computer programming and formal languages, 118–161, North Holland, Amsterdam, 1963.

[25] G. Christol, *Ensembles presque périodiques k-reconnaissables*, Theoret. Comput. Sci. **9** (1979) 141–145.

[26] G. Christol, T. Kamae, M. Mendès France, G. Rauzy, *Suites algébriques, automates et substitutions*, Bull. Soc. Math. France **108** (1980) 401–419.

[27] A. Cobham, *Uniform tag sequences*, Math. Systems Theory **6** (1972) 164–192.

[28] A. Cobham, *On the base-dependence of sets of numbers recognizable by finite automata*, Math. Systems Theory **3** (1969) 186–192.

[29] C. Davis and D. E. Knuth, *Number representations and dragon curves, I, II*, J. Recr. Math. **3** (1970) 161–181 and 133–149.

[30] M. Dekking, M. Mendès France and A. van der Poorten, *FOLDS!*, Math. Intell. **4** (1982) 130–138, 173–181 and 190–195.

[31] P. Deligne, *Intégration sur un cycle évanescent*, Invent. Math. **76** (1984) 129–143.

[32] S. Eilenberg, *Automata, Languages and Machines*, vol. A, Acad. Press, New York, 1974.

[33] H. Furstenberg, *Algebraic functions over finite fields*, J. Algebra **7** (1967) 271–277.

[34] T. Harase, *Algebraic elements in formal power series rings*, Israel J. Math. **63** (1988) 281–288.

[35] A. Lasjaunias, *Algebraic continued fractions in* $\mathbb{F}_q((T^{-1}))$ *and recurrent sequences in* $\mathbb{F}_q$, Acta Arith. **133** (2008) 251–265.

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

[37] M. Mendès France and A. van der Poorten, *Arithmetic and analytic properties of paperfolding sequences*, dedicated to K. Mahler, Bull. Austral. Math. Soc. **24** (1981) 123–131.

[38] W. H. Mills and D. P. Robbins, *Continued fractions for certain algebraic power series*, J. Number Theory **23** (1986) 388–404.

[39] M. Mkaouar, Thèse, Lyon, 1993.

[40] M. Morse, *Recurrent geodesics on a surface of negative curvature*, Trans. Amer. Math. Soc. **22** (1921) 84–100.

[41] E. Prouhet, Comptes-Rendus de l'Académie des Sciences, Paris, **33** (1851), 225.

[42] W. Rudin, *Some theorems on Fourier coefficients*, Proc. Amer. Math. Soc. **10** (1959) 855–859.

[43] O. Salon, *Suites automatiques à multi-indices et algébricité*, C. R. Acad. Sci. Paris, Série I, **305** (1987) 501–504.

[44] O. Salon, *Suites automatiques à multi-indices*, Séminaire de Théorie des Nombres de Bordeaux, Exposé 4, 1986–1987.

[45] J. Shallit, *A generalization of automatic sequences*, Theoret. Comput. Sci. **61** (1988) 1–16.

[46] J. Shallit, `https://cs.uwaterloo.ca/ shallit/as-addenda.pdf`

[47] H. S. Shapiro, *Extremal problems for polynomial and power series*, Thesis, M.I.T., 1951.

[48] H. Sharif and C. F. Woodcock, *Algebraic functions over a field of positive characteristic and Hadamard products*, J. Lond. Math. Soc. **37** (1988) 395–403.

[49] N. J. A. Sloane, *A Handbook of Integer Sequences*, Academic Press, New York, 1973. See the electronic version "OEIS" at `http://oeis.org`.

[50] A. Thue, *Über unendliche Zeichenreihen*, Norske vid. Selsk. Skr. I. Mat. Kl. Christiana **7** (1906) 1–22.

[51] A. Thue, *Lage gleicher Teile gewisse Zeichenreihen*, Norske vid. Selsk. Skr. I. Mat. Kl. Christiana, **1** (1912) 1–67.