4. Automata and transcendence in positive characteristic

The aim of this chapter is to investigate the connections between automata theory and transcendence in fields of positive characteristic. We first recall in Sec. 4.1 some definitions concerning the transcendence of Laurent formal power series with coefficients in a finite field and then state in Sec. 4.2 the main theorem of transcendence of this chapter (the Christol, Kamae, Mendès France and Rauzy theorem). We also consider some generalizations of this theorem, to the multidimensional case and to general fields of positive characteristic. We introduce in Sec. 4.3 some functions defined by Carlitz (exponential, logarithm, zeta) which are analogous to the corresponding real functions and which give us examples of application of the Christol, Kamae, Mendès France and Rauzy theorem. For this purpose, we will recall the notions of absolute value and valuation. We then briefly review transcendence results for these functions as well as methods of proofs, and emphasize the results involving automata. We end this chapter by going into the details of the most representative automata proofs of transcendence.

4.1 Introduction

The first results of classical transcendence theory concerned special values of the exponential and the logarithm function. Analogous results in the field of p-adic numbers or in positive characteristic fields have been introduced later, as for instance the Carlitz functions, that we define in the next section.

Let us first recall some basic definitions concerning transcendence. A complex number α is called *algebraic over* $\mathbb{Q}$ if there exists a nontrivial polynomial P with coefficients in $\mathbb{Q}$ such that $P(\alpha) = 0$. Otherwise, α is called *transcendental over* $\mathbb{Q}$. For instance the real number π is transcendental over $\mathbb{Q}$ whereas $\sqrt{2}$ is algebraic.

We can similarly extend these notions to Laurent formal power series with values in a finite field. For this purpose, let us define the sets which play respectively the role of $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$. Let $\mathbb{F}_q$ be the finite field with q elements, and let p denote its characteristic. We thus have p prime and $q = p^s$, where s is a nonzero natural integer. If the reader is not familiar with these notions, he can suppose in all that follows that $s = 1$, i.e., that $\mathbb{F}_q$ is the field $\mathbb{Z}/p\mathbb{Z}$ of the integers reduced modulo p. The analogue of $\mathbb{Z}$ will thus be the ring $\mathbb{F}_q[X]$ of polynomials with coefficients in $\mathbb{F}_q$, the analogue of $\mathbb{Q}$ will be its fraction field $\mathbb{F}_q(X)$ and the analogue of $\mathbb{R}$ will be the field $\mathbb{F}_q((1/X))$ of formal power series defined below. Note that the coefficients in $\mathbb{F}_q$ play the role of "digits" in the numeration basis given by the powers of the indeterminate X.

Definition 4.1.1. *The field $\mathbb{F}_q((1/X))$ of* Laurent formal power series *with coefficients in $\mathbb{F}_q$ is the field of series of the form*

$$u_{-d}X^d + \cdots + u_0 + u_1X^{-1} + \cdots ,$$

where u_i belongs to $\mathbb{F}_q$. We furthermore denote by $\mathbb{F}_q[[1/X]]$ the ring of series of the form

$$u_0 + u_1X^{-1} + u_2X^{-2} + \cdots ,$$

where u_i belongs to $\mathbb{F}_q$.

We similarly denote by $\mathbb{F}_q((X))$ the field of formal power series of the form $u_{-d}X^{-d} + \cdots + u_0 + u_1X + \cdots$, and by $\mathbb{F}_q[[X]]$ the ring of formal power series of the form $u_0 + u_1X + u_2X^2 + \cdots$, where the coefficients u_i belongs to $\mathbb{F}_q$.

We work in Sec. 4.1 and 4.2 with series of $\mathbb{F}_q((X))$, for simplicity of notations, whereas Carlitz's functions are defined in Sec. 4.3 with respect to series of $\mathbb{F}_q((1/X))$.

We can now define the notion of transcendence on $\mathbb{F}_q(X)$ for formal power series of $\mathbb{F}_q((1/X))$ or $\mathbb{F}_q((X))$.

Definition 4.1.2. *A formal power series F is* algebraic over $\mathbb{F}_q(X)$ *if there exists a nontrivial polynomial P with coefficients in $\mathbb{F}_q(X)$ such that $P(F) = 0$. Otherwise, F is called* transcendental over $\mathbb{F}_q(X)$.

This definition holds for series of $\mathbb{F}_q((X))$ as well as for series belonging to $\mathbb{F}_q((1/X))$.

In fact, we can restrict ourselves in the definition of algebraicity to *linear polynomials*, i.e., to polynomials with coefficients in $\mathbb{F}_q(X)$ of the form $\sum_{j=0}^{k-1} a_jT^{q^j}$, as stated in the following lemma, called *Ore's Lemma.* Note that the q-power of a series with coefficients in $\mathbb{F}_q$ has a very simple expression. Recall that the Frobenius map $x \mapsto x^p$ is a morphism over any field of characteristic p, i.e., $(u+v)^p = u^p + v^p$, for any two elements u, v of such a field. We have furthermore a^q, for any $a \in \mathbb{F}_q$. Hence $(\sum u_iX^i)^q = \sum u_iX^{qi}$, where the coefficients $u_i \in \mathbb{F}_q$.

Lemma 4.1.1 (Ore). *Every polynomial P of $\mathbb{F}_q[X][T]$ divides a linear polynomial of $\mathbb{F}_q[X][T]$ of the form $\sum_{j=0}^{k} a_jT^{q^j}$, where the coefficients a_j belong to $\mathbb{F}_q(X)$. In particular, if a series F is algebraic over $\mathbb{F}_q(X)$ then there exists $a_0, \ldots, a_k$ in $\mathbb{F}_q[X]$ such that $a_0F + a_2F^q + \ldots + a_kF^{q^k} = 0$.*

Proof. Consider the Euclidean division of T^{q^i} by P, for $0 \leq i \leq d = \deg P$. There exist Q_i and R_i in $\mathbb{F}_q(X)[T]$, with $\deg_T R_i < d$ such that $T^{q^i} = PQ_i + R_i$. We thus can eliminate the powers T^{q^i}, for $0 \leq i \leq d-1$, in these $d+1$ equations. Indeed, there exist $a_0, a_1, \ldots, a_d$ in $\mathbb{F}_q[X]$ (after multiplication by a suitable polynomial in $\mathbb{F}_q[X]$) such that $a_0R_0 + a_1R_1 + \ldots + a_dR_d = 0$. We thus have $\sum_{i=0}^d a_i T^{q^i} = P \times (\sum_{i=0}^d a_i Q_i)$. ■

Example. Consider the Morse sequence $u = (u_n)_{n\in\mathbb{N}}$: recall that u is defined over $\mathbb{F}_2$ as $u_n = s_2(n)$, where $s_2(n)$ is the sum modulo 2 of the coefficients of the digits in the base 2 expansion of the integer n (for more details, see Chap. 2). We thus have $u_0 = 0$, $u_{2n} = u_n$ and $u_{2n+1} = 1 + u_n$, for every integer n. Recall that in characteristic 2, we have $(\sum_{n\geq 0} u_n X^n)^2 = \sum_{n\geq 0} u_n X^{2n}$. Let $F(X) = \sum_{n\geq 0} u_n X^n$. We have

$$\begin{aligned} F(X) = \textstyle\sum_{n\geq 0} u_n X^n &= \textstyle\sum_{n\geq 0} u_{2n} X^{2n} + \sum u_{2n+1} X^{2n+1} \\ &= \textstyle\sum_{n\geq 0} u_n X^{2n} + \sum (1+u_n) X^{2n+1} \\ &= (\textstyle\sum_{n\geq 0} u_n X^n)^2 + X(\sum u_n X^n)^2 + \frac{X}{1+X^2} \\ &= F(X)^2(1+X) + \frac{X}{1+X^2}. \end{aligned}$$

Hence the series $F(X)$ is algebraic over $\mathbb{F}_2((1/X))$ and satisfies

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

by using $(1+X)^2 = 1 + X^2$.

Exercise 4.1.1. Prove that if $v = (v_n)_{n\in\mathbb{N}}$ denotes the Rudin-Shapiro sequence (see Chap. 2 and 3), then $G(X) = \sum_{n\geq 0} v_n X^n$ satisfies in $\mathbb{F}_2((X))$

$$(1+X)^5 G^2(X) + (1+X)^4 G(X) + X^3 = 0.$$

4.2 The Christol, Kamae, Mendès France and Rauzy theorem

The automata proofs of transcendence are based on the following theorem due to Christol, Kamae, Mendès France and Rauzy (see [98] and also [99]) which gives a necessary and sufficient condition of algebraicity for a formal power series with coefficients in a finite field.

Theorem 4.2.1 (Christol, Kamae, Mendès France and Rauzy).

Let $u = (u(n))_{n\in\mathbb{N}}$ be a sequence with values in $\mathbb{F}_q$. The following conditions are equivalent:

1. *the formal power series $\sum_{n\geq 0} u(n) X^n$ is algebraic over the field $\mathbb{F}_q(X)$,*

2. *the* q-kernel $N_q(u)$ *of the sequence* u *is finite, where* $N_q(u)$ *is the set of subsequences of the sequence* $(u(n))_{n\in\mathbb{N}}$ *defined by*

$$N_q(u) = \{(u(q^k n + r))_{n\in\mathbb{N}};\ k \geq 0;\ 0 \leq r \leq q^k - 1\},$$

3. *the sequence* u *is* q*-automatic,*
4. *the sequence* u *is the image by a letter-to-letter projection of a fixed point of a substitution of constant length* q.

Remarks.

- Let us recall that the last equivalence is actually due to Cobham (see [101]; for a proof see Chap. 1). The equivalence between 2 and 3 dates back to Eilenberg in [135]. This theorem is also called Chritol's theorem since the equivalence between 1 and 2 can be found in [99].
- We consider here, except otherwise stated, automata in reverse reading.
- We easily deduce from the Christol, Kamae, Mendès France and Rauzy theorem the following facts. The notion of k-automaticity is stable by finite modification (as for instance changing a finite number of terms, see [101]) or by applying the shift $T((u_n)_{n\in\mathbb{N}}) = (u_{n+1})_{n\in\mathbb{N}}$. Furthermore a ultimately periodic sequence is k-automatic.
- The notion of p-automaticity can also be expressed as follows in terms of first-order logic: a sequence is generated by a p-substitution if and only if it is p-definable (it can be defined in the theory $(\mathbb{N}, +, V_p)$, where V_p is the function "valuation" that associates with x the highest power of p that divides x (or 1 if $x = 0$)). For more details, the reader is referred to the survey [83].
- The same theorem holds by considering a series $\sum u_n X^{-n}$ in $\mathbb{F}_q((1/X))$ with the same definition for the q-kernel. Indeed, $\sum u_n X^{-n}$ is transcendental over $\mathbb{F}_q(X)$ if and only if $\sum u_n X^n$ is transcendental over $\mathbb{F}_q(X)$.

Exercise 4.2.1. 1. Show that a sequence is p-automatic if and only if it is p^k-automatic for any nonzero power of the prime p.

2. Build a d-automaton generating the characteristic sequence of the set of powers of a fixed positive integer d.
3. Build a d-automaton generating the characteristic sequence of the set of integers divisible by d.
4. Build a 2-automaton generating the characteristic sequence of the set of integers with base 2-expansion of the form 1^n0^m1, for $n, m > 0$ and $n+m$ odd.
5. Prove that the characteristic sequence of the set of integers with base 2-expansion of the form $1^n0^{n+1}1$, for $n > 0$, is not 2-automatic.

4.2.1 Proof of the theorem

The proof of Theorem 4.2.1 we give here is exactly the proof of [8]. We also refer the reader to the original proof in [99].

- Let us first prove that the q-kernel of an algebraic series is finite.
  The idea of the proof is the following. Suppose we have a finite set $\mathcal{N}$ of subsequences of a given sequence u such that u belongs to this set and such that $\mathcal{N}$ is stable under the maps $\mathcal{A}_r$ $(0 \leq r \leq q-1)$, where $\mathcal{A}_r$ associates with a subsequence $(v(n))_{n\in\mathbb{N}}$ the subsequence $(v(qn+r))_{n\in\mathbb{N}}$. As this set contains the q-kernel of u, hence the q-kernel is finite.
  Let us work here on the (algebraic) formal power series $\sum u(n)X^n$ and let us introduce the corresponding maps $\mathcal{A}_r$. Let r be an integer in $[0, q-1]$. Let $A_r : \mathbb{F}_q[[X]] \to \mathbb{F}_q[[X]]$ defined by:
  $$A_r(\sum_{n\geq 0} u(n)X^n) = \sum_{n\geq 0} u(qn+r)X^n,$$
  where $u(n)$ belongs to $\mathbb{F}_q$, for all n. Let $F = \sum_{n\geq 0} u(n)X^n$; we have $F = \sum_{r=0}^{q-1} A_r(F)^q X^r$. We deduce from this that for any polynomial P in $\mathbb{F}_q[X]$ and for any formal power series F: $A_r(PF^q) = A_r(P)F$. Namely, $P = \sum_{r=0}^{q-1} A_r(P)^q X^r$ and $PF^q = \sum_{r=0}^{q-1}(A_r(P)F)^q X^r$. Note furthermore that $A_r(P)$ is a polynomial and that $\deg A_r(P) \leq \deg P/q$.
  Let $F = \sum u(n)X^n$ be an algebraic formal power series. From Ore's lemma (Lemma 4.1.1), there exists an integer j and polynomials a_0, $a_1, \cdots, a_k$ in $\mathbb{F}_q[X]$ such that
  $$\sum_{i=j}^{k} a_i F^{q^i} = 0. \tag{4.1}$$
  We can furthermore suppose $a_0 \neq 0$. Indeed, let j be the smallest index such that a relation of type (4.1) holds with $a_j \neq 0$. Let us show that $j = 0$. We have $a_j = \sum_{r=0}^{q-1} A_r(a_j)^q X^r$. As $a_j \neq 0$, there exists an integer r such that $A_r(a_j) \neq 0$. Suppose $j \neq 0$. We have
  $$0 = A_r(\sum_{i=j}^{k} a_i F^{q^i}) = \sum_{i=j}^{k} A_r(a_i)F^{q^{i-1}},$$
  which is of type (4.1) and which contradicts the minimality of j.
  Suppose now that F satisfies equality (4.1) with $a_0 \neq 0$. Let $G = F/a_0$. We thus have:
  $$G = \sum_{i=1}^{k} b_i G^{q^i},$$
  with $b_i = -a_i a_0^{q^i-2}$. We want to show that there exists a finite set of formal power series $\mathcal{H}$ stable under the maps A_r and containing the series F.
  Let $\mathcal{H}$ denote the set of formal power series of the form
  $$\sum_{i=0}^{k} c_i G^{q^i}, \text{ with } c_i \in \mathbb{F}_q[X] \tag{4.2}$$

$$\text{and } \deg c_i \leq \sup(\deg a_0, \deg b_1, \cdots, \deg b_k).$$

Let H be a series of type (4.2). For any integer r in $[0, q-1]$, we have

$$\begin{aligned} A_r(H) &= A_r(c_0 G + \textstyle\sum_{i=1}^{k} c_i G^{q^i}) \\ &= A_r(\textstyle\sum_{i=1}^{k} (c_0 b_i + c_i) G^{q^i}) \\ &= \textstyle\sum_{i=1}^{k} A_r(c_0 b_i + c_i) G^{q^i - 1}. \end{aligned}$$

As

$$\deg(c_0 b_i + c_i) \leq 2 \sup(\deg a_0, \deg b_1, \cdots, \deg b_k),$$

which implies that

$$\deg A_r(c_0 b_i + c_i) \leq 2 \sup(\deg a_0, \deg b_1, \cdots, \deg b_k)/q,$$

the set $\mathcal{H}$ is stable under the action of the maps A_r. We conclude the proof by noticing that $\mathcal{H}$ is finite and that $\mathcal{H}$ contains $F = a_0 G$.

- Let us prove now the converse implication. Suppose that the q-kernel $N_q(u)$ of the sequence $u = (u(n))_{n \in \mathbb{N}}$ with values in $\mathbb{F}_q$ is finite. Let $F = \sum u(n) X^n$. Note $u = u_1, u_2, \cdots, u_d$ the sequences of $N_q(u)$ and for any integer j in $[1, d]$, put $F_j = \sum u_j(n) X^n$. We have, for any integer r in $[0, q-1]$:

$$F_j = \sum_{r=0}^{q-1} A_r(F_j)^q X^r,$$

and

$$A_r(F_j)^q = \sum u_j(qn + r) X^{qn} = \sum (u_j(qn + r) X^n)^q.$$

Let i ($i = i(j, r)$) be such that $(u_j(qn+r))_{n \in \mathbb{N}} = u_i$. We thus have $A_r(F_j) = F_i^q$. Hence, for any j, the series F_j belongs to the vector space spanned over $\mathbb{F}_q(X)$ by $F_1(X)^q, \cdots, F_d(X)^q$.
Similarly, for any j, the series F_j^q, and hence the series F_j, belong to the vector space spanned over $\mathbb{F}_q(X)$ by $F_1(X)^{q^2}, \cdots, F_d(X)^{q^2}$.
We thus prove by induction that the $(d+1)$ series $F, F^q, \cdots, F^{q^d}$ belong to the vector space spanned over $\mathbb{F}_q(X)$ by $F_1(X)^{q^{d+1}}, \cdots, F_d(X)^{q^{d+1}}$. This vector space has dimension less than or equal to d. We deduce from this the algebraicity of F.

- Suppose that the q-kernel $N_q(u)$ of the sequence $u = (u(n))_{n \in \mathbb{N}}$ with values in $\mathbb{F}_q$ is finite. Let us prove that the sequence u is q-automatic by exhibiting a q-automaton (in reverse reading) recognizing the sequence u.
We denote by $u = u_1, u_2, \cdots, u_d$ the sequences of $N_q(u)$. Consider a finite set of d states $\mathcal{S} = \{a_1, \cdots, a_d\}$ in bijection with $N_q(u)$ (a_j denotes the state in bijection with the sequence u_j). Define, for any r in $[0, q-1]$, the map $r : \mathcal{S} \to \mathcal{S}$ which associates with any state a_i the state $r.a_i$ in bijection with the sequence of the q-kernel $(u_i(qn+r))_{n \in \mathbb{N}}$. Let $n = \sum_{j=0}^{k} n_j q^j$ be the base q expansion of any positive integer n, with $n_j \in [0, q-1]$ and $n_k \neq 0$.

We define the map n from $\mathcal{S}$ into itself by $n(a_i) = n_k(n_{k-1}(\cdots(n_0(a_i))))$, if $n \neq 0$, otherwise the map 0 equals the identity. It is easily seen that $n.a_1$ is the state in bijection with $(u(q^{k+1}l + n))_{n\in\mathbb{N}}l$. Hence if $n.a_1 = m.a_1$, then $u(n) = u(m)$, by considering the first term of the two corresponding subsequences. We thus can define as output function the map φ (which is well defined) which associates with a state a_i the value $u(n)$ if there exists an integer n such that $n.a_1 = a_i$ and 0 (for instance) otherwise. The sequence u is hence generated by the automaton with states $\mathcal{S}$, initial state a_1, transition maps $0, 1, \cdots, q-1$ and output function φ.

- Let us show that a q-automatic sequence $u = (u(n))_{n\in\mathbb{N}}$ has a finite q-kernel. Let $\mathcal{A}$ be a finite automaton which generates the sequence u of initial state i. The subsequence $(u(q^k n + r))_{n\geq 1}$, where $k \geq 1$ and $0 \leq r \leq q^k - 1$, is generated by $\mathcal{A}$ with the initial state $\overline{r}.i$, where $\overline{r}$ is the word of k letters obtained by concatenating in front of the base q expansion of r as many zeros as necessary. As the automaton $\mathcal{A}$ has a finite number of states, we hence obtain a finite number of subsequences.
- Let us prove that the image by a letter-to-letter projection of the fixed point of a substitution of constant length q has a finite q-kernel. It suffices to prove this result for the fixed point $(u(n))_{n\in\mathbb{N}}$ of a substitution σ of constant length q defined over the alphabet X. Define $\sigma = \sigma_0 \cdots \sigma_{q-1}$, where σ_i is a map from X to X. We have $\sigma_i(u(n)) = u(qn+i)$, for any integer n and for any $i \in [0, q-1]$. Let $k \geq 0$, $0 \leq r \leq q^k - 1$. Write $r = \sum_{j=0}^{k-1} r_j q^j$, where $0 \leq r_j \leq q-1$. We thus have $u(q^k n + r) = \sigma_{r_0}\sigma_{r_1}\cdots\sigma_{r_{k-1}}(u(n))$. As there are at most $(\mathrm{Card}(X))^{\mathrm{Card}(X)}$ such maps, this concludes the proof.
- Conversely, suppose that the q-kernel $N_q(u)$ of the sequence u is finite. We denote by $u = u_1, u_2, \cdots, u_d$ the sequences of $N_q(u)$. Let $U = (U(n))_{n\in\mathbb{N}}$ be the sequence with values in $\mathbb{F}_q^d$ defined by $U(n) = (u_1(n), \cdots, u_d(n))$. Let us construct a substitution σ of constant length q defined on $\mathbb{F}_q^d$ with U as fixed point. As $N_q(u)$ is stable by the maps $\mathcal{A}_r$ $(\mathcal{A}_r(v(n))_{n\in\mathbb{N}} = v(qn+r))_{n\in\mathbb{N}})$, then, for any $0 \leq r \leq q-1$, $U(qn+r) = U(qm+r)$, if $U(n) = U(m)$. Let us define, for $0 \leq r \leq q-1$, σ_r: $\mathbb{F}_q^d \to \mathbb{F}_q^d$, $U(n) \mapsto (u_1(qn+r), \cdots, u_d(qn+r))$, if there exists n such that $(a_1, \cdots, a_r) = U(n)$, and otherwise $(a_1, \cdots, a_r) \mapsto (0, \cdots, 0)$. The sequence U is thus the fixed point of the substitution of constant length $\sigma = \sigma_0 \cdots \sigma_{q-1}$ and the sequence u is the image of U by the projection on the first coordinate from $\mathbb{F}_q$ into $\mathbb{F}_q^d$. ∎

Remarks.

- The proof of the equivalence between Condition 2 and 3 in Theorem 4.2.1 is thus constructive, i.e., given the q-kernel of a sequence, then one can compute a q-automaton in reverse reading, generating the sequence u, the states of which are in bijection with the subsequences of the q-kernel. Recall that a q-automaton in direct reading can be derived from a substitution of constant length generating u as in Condition 3 (see Proposition 1.5.1). Note

furthermore that one deduces from Theorem 4.2.1 (and more precisely, from Condition 2, 3, 4) the equivalence between being generated by a q-automaton in direct reading and being generated by a q-automaton in reverse reading.
- The equivalences between Condition 2, 3 and 4 is true whatever the cardinality of the alphabet.
- Several results of k-automaticity (see for instance [27]) or more generally of k-regularity [22] appear in the literature, with proofs in a similar vein to that of the one of the equivalence between Condition 1 and 2.

4.2.2 Applications

The aim of this section is to give some applications of Theorem 4.2.1. The first two are easy consequences of the theorem.

- Let $\sum_{n\geq 0} u(n)X^n$ be an algebraic formal power series. Let a and b be two natural integers. The series $\sum_{n\geq 0} u(an+b)X^n$ is algebraic.
- Let $p \geq 2$ be a prime. Let $S_p(n)$ be the sum modulo p of the digits of n in base p. The series $\sum_{n\geq 0} S_p(n)X^n$ is algebraic.

Remark. It can be proved that the series $\sum_{n\geq 0} S_p(n^2)X^n$ is transcendental. More generally, let R be a polynomial with coefficients in $\mathbb{Q}$ such that $R(\mathbb{N}) \subset \mathbb{N}$. The formal power series $\sum_{n\geq 0} S_p(R(n))X^n$ is algebraic over $\mathbb{F}_p$ if and only if the degree of R is less than or equal to 1 (see [6]).

Note that the following theorem, due to Cobham (see [100]), produces more examples of transcendental series. We do not give here the proof of this theorem, which is rather difficult.

Theorem 4.2.2 (Cobham). *Let u be a sequence which is both k-automatic and k'-automatic. If k and k' are multiplicatively independent (i.e., if $\frac{\log(k)}{\log(k')}$ is irrational), then the sequence u is ultimately periodic.*

Remark. This theorem has received numerous generalizations and has given rise to much literature. See for instance the survey [83], see also [279, 82].

Exercise 4.2.2. Give an example of a 6-automatic sequence which is neither 3-automatic nor 2-automatic.

We deduce from Cobham's theorem the following result of transcendence, which resembles an open question of Mahler: let $(u_n)_{n\in\mathbb{N}}$ be a binary sequence such that the series $\sum u_n 2^{-n}$ and $\sum u_n 3^{-n}$ are algebraic over $\mathbb{Q}$; is this sequence ultimately periodic?

Proposition 4.2.1. *Let $(u_n)_{n\in\mathbb{N}}$ be a binary sequence such that $\sum u_n X^n$ considered as an element of $\mathbb{F}_2[[X]]$ and $\sum u_n X^n$ considered as an element of $\mathbb{F}_3[[X]]$ are algebraic. Then, this sequence is ultimately periodic, i.e., both series are rational.*

The *Hadamard product* of two series $\sum u_n X^n$ and $\sum v_n X^n$ is defined as the series $\sum u_n v_n X^n$. In particular, the Hadamard product of the characteristic series of a subset A of $\mathbb{N}$ (defined as $\sum_{n \in A} X^n$) by the characteristic series of a subset B is equal to the characteristic series of $A \cap B$. By considering the notion of q-kernel, we easily deduce the following.

Theorem 4.2.3. *The Hadamard product of two algebraic formal power series with coefficients in a finite field is algebraic.*

Another application of Cobham's theorem (Theorem 4.2.2) is the following (see for instance [11]).

Theorem 4.2.4. *Let r be an integer greater than or equal to 2. The series $\sum_{k=0}^{+\infty} X^{r^k}$ is algebraic over $\mathbb{F}_q(X)$ if and only if r is a power of p.*

Proof. Write

$$\sum_{k=0}^{+\infty} X^{r^k} = \sum_{n \geq 1} u_n X^n,$$

where $u = (u_n)_{n \in \mathbb{N}}$ is the characteristic sequence of the set of powers of r. The series $\sum_{k=0}^{+\infty} X^{r^k}$ is algebraic over $\mathbb{F}_q(X)$ if and only if the sequence u is p-automatic. But it is easily seen that the sequence u is r-automatic (Exercise 4.2.1) and not ultimately periodic. Hence the series $\sum_{k=0}^{+\infty} X^{r^k}$ is algebraic over $\mathbb{F}_q(X)$ if and only if r is a power of p. ∎

Remark. The formal power series $\sum u_n X^n$ belongs to $\mathbb{F}_q(X)$ if and only if the sequence $(u_n)_{n \in \mathbb{N}}$ is ultimately periodic. Note that in the real case we just have the following implication: if the sequence $(u_n)_{n \in \mathbb{N}}$ is ultimately periodic, then the series $\sum u_n X^n$ belongs to $\mathbb{Q}(X)$. The rational series $\sum n X^n$ shows that the converse is not true.

4.2.3 Some transcendence results

It is natural to look for connections between transcendence in the real case and in positive characteristic. Indeed, a formal power series is algebraic in positive characteristic if the sequence of its coefficients has some kind of order, whereas irrational algebraic real numbers cannot have an expansion which is too regular. Loxton and van der Poorten [230] have partially proved the following conjecture (this conjecture is often quoted as a theorem, but there seems to be a gap in the proof):

Conjecture 4.2.1. If the sequence of the coefficients in the base q-expansion of a real number is automatic, then this number is either rational or transcendental.

This conjecture illustrates, like Cobham's theorem, the fact that transcendence deeply depends on the frame in which it is considered. Some partial results in the direction of this conjecture have been obtained in [28].

Theorem 4.2.5. *Let α be a positive real number whose base k digit expansion is a fixed point of a binary morphism. If the morphism is either of constant length greater than or equal to 2 or primitive, then α is either rational or transcendental.*

See also [146] (and Chap. 5) for the corresponding results of transcendence involving real numbers with a Sturmian dyadic expansion. These proofs involve a clever use of Ridout's theorem [299]. This theorem is an improvement of Roth's theorem [303]. See in a similar vein [107, 287, 18] for transcendence results concerning those real numbers whose sequence of partial quotients in their continued fraction expansion is automatic. For a survey of these results, see [15].

4.2.4 The multidimensional case

Christol, Kamae, Mendès France and Rauzy's theorem was generalized by Salon to the multidimensional case, i.e., to the case of a formal power series with a finite number of indeterminates and with coordinates in a finite field, say $\sum_{n_i \geq 0} u(n_1, n_2, \cdots, n_d) X_1^{n_1} \cdots X_d^{n_d}$ (see for instance [308] and [307]). The generalized q-kernel is given in this case by:

$$N_q(u(n_1, n_2, \cdots, n_d)) = \{u(q^k n_1 + r_1, q^k n_2 + r_2, \cdots, q^k n_d + r_d),$$
$$k \geq 0,\ 0 \leq n_i \leq q^k - 1, \text{ for } \ i = 1 \text{ to } \ d\}.$$

Recall that a formal power series $F = \sum_{n_i \geq 0} u(n_1, n_2, \cdots, n_d) X_1^{n_1} \cdots X_d^{n_d}$ is called *algebraic* over $\mathbb{F}_q(X_1, X_2, \cdots, X_d)$ if there exists a nontrivial polynomial P with coefficients in $\mathbb{F}_q(X_1, X_2, \cdots, X_d)$ such that $P(F) = 0$. We thus have the following theorem due to Salon (see [308] and [307]).

Theorem 4.2.6. *The power series $\sum u(n_1, n_2, \cdots, n_d) X_1^{n_1} \cdots X_d^{n_d}$ is algebraic over $\mathbb{F}_q(X_1, X_2, \cdots, X_d)$ if and only if the q-kernel of the sequence u is finite.*

The following results are easy applications of this theorem.

- Let $\sum u(n) X^n$ be an algebraic formal power series. The double formal power series $\sum u(n+m) X^n Y^m$ is algebraic.
- Let $\sum u(n, m) X^n Y^m$ be algebraic. Let a, b, c, d be four integers. The series $\sum u(an + b, cm + d) X^n Y^m$ is algebraic.

The notions of automaton and substitution can also be generalized into two dimensions. A *two-dimensional substitution* of constant length k associates with each letter a square array of letters of size (k, k). A *two-dimensional k-automaton* is defined similarly as a one-dimensional k-automaton but in this case the edges are labelled by pairs of integers in $[0, k-1]^2$. A sequence $(U(n, m))$ is generated by the automaton $\mathcal{A}$ by reading simultaneously the digits of the base k expansions of n and m, the shortest expansion being completed with leading zeroes to get two strings of symbols of the length of the longest expansion (without leading zeroes).

Exercise 4.2.3. Consider the substitution $\sigma : \{0,1\} \to \{0,1\} \times \{0,1\}$ defined by

$$\sigma(0) = \begin{matrix} 00 \\ 00 \end{matrix},$$

$$\sigma(1) = \begin{matrix} 11 \\ 10 \end{matrix}.$$

Prove that the two-dimensional sequence defined over $\mathbb{N}^2$ as the fixed point of this substitution generated by the successive images of 1 is equal to Pascal's triangle reduced modulo 2. Find the substitution generating Pascal's triangle modulo p, where p is a prime integer.

Remarks.

- More generally, the two-dimensional sequence corresponding to Pascal's triangle modulo an integer d is automatic if and only if d is a power of a prime (for more details, see [27, 25, 26]). See also [16] for an expression of the rectangular complexity of the two-dimensional sequence associated with Pascal's triangle modulo 2.
- Note that it seems more difficult to generalize to the multidimensional case the notion of substitution of non-constant length. For examples of such substitutions in connection with a notion of two-dimensional Sturmian sequences, see [34].

4.2.5 Diagonals

Another interesting consequence of this generalization to the multidimensional case is given by the following results. The *diagonal* of a double formal power series $\sum u_{m,n} X^n Y^m$ is defined as the series $\sum u_{n,n} X^n$.

Theorem 4.2.7. *The diagonal of an algebraic formal power series with coefficients in a finite field is algebraic.*

Proof. Consider either the notion of q-kernel or the one-dimensional substitution defined by associating with each letter the "diagonal" of the square array of letters associated through the initial substitution. ■

Theorem 4.2.7 was first proved by Furstenberg in [155] and can be compared to the following theorem, also due to Furstenberg.

Theorem 4.2.8. *A series with coefficients in a finite field is algebraic if and only if there exists a rational double formal power series such that the initial series is the diagonal of this double series.*

Observe that this result still holds for $\mathbb{C}$ when considering two-indeterminate series but is false for series involving more indeterminates. For a survey of the subject, the reader is referred to [10].

Exercise 4.2.4. 1. Let $(u_n)_{n\in\mathbb{N}}$ be the Morse sequence. Prove that the series $\sum u_n X^n$ is the diagonal of the rational function in $\mathbb{F}_2(X,Y)$ defined by $Y(1+Y(1+XY)+X(1+XY)^{-2})^{-1}$ (for details, see [8]).

2. Let $(v(n))_{n\in\mathbb{N}}$ be a sequence with values in the finite set S. Prove that if $\sum v(n)X^n$ is algebraic, then, for any $s \in S$, $\sum\limits_{v(n)=s} X^n$ is algebraic.
3. Let $(v_n)_{n\in\mathbb{N}}$ be the characteristic sequence of the set of powers of the prime p. Prove that the series $\sum v_n X^n$ is the diagonal of the rational function in $\mathbb{F}_p(X,Y)$ $G(X) = X/(1-(X^{p-1}+Y))$.
4. Let $(w_n)_{n\in\mathbb{N}}$ be the characteristic sequence of the set of integers with base 2-expansion of the form 1^n0^m1, for $n,m>0$ and $n+m$ odd. Let $(x_n)_{n\in\mathbb{N}}$ be the characteristic sequence of the set of integers with base 2-expansion of the form $1^n0^{n+1}1$, for $n>0$. Let $(y_n)_{n\in\mathbb{N}}$ be the characteristic sequence of the set of squares. Prove that the Hadamard product of the series $\sum_{n\geq 0} w_n X^n$ and $\sum_{n\geq 0} y_n X^n$ is equal to $\sum_{n\geq 0} x_n X^n$. Deduce from Exercise 4.2.1 that the sequence $(y_n)_{n\in\mathbb{N}}$ is not 2-automatic (for more details, see [301] and the survey [351]).

4.2.6 Fields of positive characteristic

Christol, Kamae, Mendès France and Rauzy's theorem can also be extended to a general field of positive characteristic, which is not necessarily finite. Such a generalization is due to Sharif and Woodcock (see [10]) and Harase (see [166]).

Theorem 4.2.9. *Let u be a sequence with values in a field K of positive characteristic p. Let s be any nonzero integer, $q = p^s$, and let $\overline{K}$ be a perfect field (i.e., a field in which the map $x \mapsto x^p$ is onto) containing K. 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 following set of subsequences*

$$N_q(u) = \{(u^{1/q^k}(q^k n + r))_{n\in\mathbb{N}}, k \geq 0,\ 0 \leq r \leq q^k - 1\}$$

has a finite dimension.

Remarks.

- The set $N_q(u)$, which plays here the role of a generalized q-kernel, is exactly the q-kernel of the sequence u, when the field K is finite and this theorem reduces in this case to the theorem of Christol, Kamae, Mendès France and Rauzy.
- We have seen that the notions of substitution and finite automaton can also be extended to the multidimensional case when the ground field is finite. In the general case of a field with nonzero characteristic, only the notion of substitution can be extended (for more details, see the survey [10]).
- The results for the Hadamard product and for the diagonal still hold in this context as consequences of Theorem 4.2.9. In fact we can deduce the following corollary first proved by Deligne in [121].

  Corollary 4.2.1. *The Hadamard product of two algebraic formal power series with coefficients in a field of positive characteristic is algebraic. The diagonal of an algebraic formal power series with coefficients in a field of positive characteristic is algebraic.*

- Fresnel, Koskas and de Mathan give a quantitative version of Christol, Kamae, Mendès France and Rauzy's Theorem in the case of an infinite ground field (see [150]).

4.2.7 Continued fraction expansions and automaticity

Let us end this section by surveying related results of automaticity concerning the "digits" in the continued fraction expansion of formal power series with coefficients in a finite field.

In the real case very few explicit examples of continued fraction expansions are known; one can mostly expand power series or roots of some particular equations. Furthermore, it is a still open problem to determine if the set of partial quotients in the expansion of an algebraic number of degree greater than 2 is bounded. Only a few examples of such expansions are known (for more references see the survey [324]). The situation is drastically different for formal power series with coefficients in a finite field. Indeed Baum and Sweet [48] have produced a cubic series the continued fraction expansion of which has partial quotients with bounded degree (see also Chap. 2 and [47]). Mills and Robbins have extended Baum and Sweet's approach to produce in [251] explicit expansions of algebraic elements in characteristic $p > 2$ for which the degrees of the partial quotients are bounded.

The algebraic series with bounded partial quotients produced respectively by Baum and Sweet [48], and by Mills and Robbins [251], have raised many interrogations, in particular concerning the automaticity of their coefficients. In the case where the partial quotients in the continued fraction expansion of an algebraic Laurent formal power series take finitely many values, Mendès

France asked whether this sequence is itself p-automatic. A positive answer to this question has been given in [9, 17] in the case of Mills and Robbins examples [251] in characteristic > 2. But Mkaouar [252] (see also [382]) showed that the Baum and Sweet series [48] provides a negative answer to the question asked by Mendès France. Note also Thakur's results on the continued fraction expansion of the Carlitz analogue of the exponential [346, 347, 348].

4.3 Some functions defined by Carlitz

In the preceding pages we used the following notion of transcendence: a formal power series F is algebraic over $\mathbb{F}_q(X)$ if there exists a nontrivial polynomial P with coefficients in $\mathbb{F}_q(X)$ such that $P(F) = 0$. By analogy with the real case, we have seen that the set which plays here the role of $\mathbb{Z}$ is the ring $\mathbb{F}_q[X]$ of polynomials with coefficients in $\mathbb{F}_q$ and the analogue of $\mathbb{Q}$ is the fraction field of $\mathbb{F}_q[X]$, i.e., the field $\mathbb{F}_q(X)$ of fractions with coefficients in $\mathbb{F}_q$.

Let us see in what respect the field $\mathbb{F}_q((1/X))$ is an analogue of $\mathbb{R}$. Let us recall that the field $\mathbb{R}$ is the *completion* of $\mathbb{Q}$ with respect to the usual absolute value. Hence our next step will be to define an *absolute value* over $\mathbb{F}_q(X)$. For more details on valuations, see [29, 386].

4.3.1 Absolute value and valuation

Definition 4.3.1. *An absolute value over a field K is a map (that we denote $|\ |$) from K to $\mathbb{R}^+$ which satisfies the following properties:*

- $|x| = 0$ *if and only if* $x = 0$*;*
- $|xy| = |x||y|$*;*
- $|x + y| \leq |x| + |y|$.

The classical absolute value over $\mathbb{R}$ or the function which associates with a complex number its modulus are examples of absolute values.

It is easily seen that the function which associates with a fraction R in $\mathbb{F}_q(X)$ the number $a^{\deg R}$ (denoted by $|R|$), where $a > 1$ and where $\deg R$ denotes the degree of R (with the convention that the degree of the zero fraction is equal to $-\infty$), is an absolute value over $\mathbb{F}_q(X)$. But this absolute value does not have the same properties as the classical real absolute value. In particular, this absolute value satisfies for any two fractions R and S:

$$|R + S| \leq \max(|R|, |S|),$$

$$|R + S| = \max(|R|, |S|), \text{ if } |R| \neq |S|.$$

The degree obviously satisfies the same property inducing consequences which refute our intuition based on the real case.

Definition 4.3.2. *An absolute value over a field K is called* non-Archimedean *if for any two elements x, y of K, we have:*

$$|x+y| \leq \max(|x|, |y|).$$

Lemma 4.3.1. *A non-Archimedean absolute value satisfies for any two elements x, y of K with $|x| \neq |y|$:*

$$|x+y| = \max(|x|, |y|).$$

Proof. Let us suppose $|x| < |y|$. We have $|x+y| \leq \max(|x|, |y|) = |y|$. But $|y| \leq \max(|-x|, |x+y|)$. Since $|-1|^2 = |1|$, we have $|-1| = |1|$ and $|-x| = |x|$. As $|x| < |y|$, we thus have $\max(|-x|, |x+y|) = |x+y|$, from which the lemma follows. ∎

Lemma 4.3.2. *An absolute value is non-Archimedean if and only if the set of values*

$$\{|n.1_K|,\ n \in \mathbb{Z}\},$$

where 1_K denotes the unit of the field K, is bounded.

Proof. Let M be such that $|n.1_K| \leq M$, for any $n \in \mathbb{Z}$. Let x, y be in K with $|x| \leq |y|$. We have:

$$|x+y|^n = |(x+y)^n| = |x^n + \binom{n}{1} x^{n-1} y + \cdots + \binom{n}{n-1} x y^{n-1} + y^n|.$$

Thus

$$|x+y|^n \leq (n+1) M |y|^n,$$

i.e.,

$$|x+y| \leq |y| ((n+1)M)^{1/n}.$$

Letting n tend towards $+\infty$, we obtain the desired property:

$$|x+y| \leq |y| = \max(|x|, |y|).$$

The converse is immediate. ∎

Remark. An absolute value defined over a field of positive characteristic is non-Archimedean. Namely, the set of values $\{|n.1_K|,\ n \in \mathbb{Z}\}$ is finite in this case.

Definition 4.3.3. *A valuation over a field K is a map (that we denote v) from K to $\mathbb{R}$ which satisfies the following properties:*

- $v(x) = +\infty$ *if and only if* $x = 0$;
- $v(xy) = v(x) + v(y)$;
- $v(x+y) \geq \min(v(x), v(y))$.

For instance, the function $v : \mathbb{F}_q(X) \to \mathbb{F}_q(X)$, $R \mapsto -\deg R$, is a valuation over $\mathbb{F}_q(X)$. This valuation is called the $1/X$-adic valuation, by analogy with the p-adic valuation v_p which is defined as follows over $\mathbb{Z}$: $v_p(x)$ is the exponent of the greatest power of p which divides x. The completion of $\mathbb{Z}$ with respect to this valuation is called the ring of *p-adic integers*.

Proposition 4.3.1. *Let v be a valuation defined over the field K. Let $0 < a < 1$. The function a^v is an absolute value over K. Conversely, if $|\ |$ is an Archimedean absolute value defined over the field K and if $b > 0$, then, the function v defined over K by $v(0) = +\infty$ and $v(x) = -\log(|x|)$, if $x \neq 0$, is a valuation.*

Recall that the field $\mathbb{F}_q((1/x))$ of Laurent formal power series with coefficients in $\mathbb{F}_q$ is the set of series of the form

$$a_{-d}X^d + \cdots + a_0 + a_1X^{-1} + \cdots ,$$

where a_i belongs to $\mathbb{F}_q(X)$. The notion of degree can be easily extended to this field: we define the degree of $a_{-d}X^d + \cdots + a_0 + a_1X^{-1} + \cdots$, with $a_{-d} \neq 0$, as d. The function v which associates the quantity $v(z) = -\deg z$ with a formal power series z, is still a valuation over $\mathbb{F}_q((1/X))$.

In fact, the field $\mathbb{F}_q((1/X))$ is the completion of $\mathbb{F}_q(X)$ with respect to this valuation. For more details, the reader is referred to [29, 386].

The question now is to define an analogue of $\mathbb{C}$. The field $\mathbb{C}$ is algebraically closed and complete. Let $\mathbf{R}$ be the field $\mathbb{F}_q((1/X)$; this field is complete but not algebraically closed; let $\mathbf{C}$ be the completion of an algebraic closure of $\mathbf{R}$; a fundamental property here is that $\mathbf{C}$ is still algebraically closed (see [29]). This field will be an analogue of $\mathbb{C}$.

4.3.2 Convergence in $\mathbb{F}_q((1/X))$

One particular point of the non-Archimedean nature of the absolute value in $\mathbb{F}_q((1/X))$ (which is a consequence of the fact that we work on the finite field $\mathbb{F}_q$) is the following property.

Proposition 4.3.2. *A series $\sum_{n\geq 0} u_n$ with coefficients in $\mathbb{F}_q(X)$ converges if and only if its general term u_n tends to 0, i.e., if and only if its degree tends to $-\infty$.*

Proof. The field $\mathbb{F}_q((1/X)$ is complete. We thus have to check that if u_n tends to 0, then the series $\sum u_n$ is a Cauchy sequence, which is an easy consequence of the non-Archimedean nature of the valuation. ■

Example. For instance, the series $\displaystyle\sum_{k=1}^{+\infty} \frac{1}{X^{q^k} - X}$ converges in $\mathbb{F}_q((1/X))$. Indeed, the degree of its general term is equal to $-q^k$. We will see in the following that this series, called the *bracket series*, is transcendental over $\mathbb{F}_q(X)$.

Proposition 4.3.3. *A product $\prod_{n\geq 0}(1+u_n)$ with coefficients in $\mathbb{F}_q(X)$ is convergent if and only if u_n tends to 0, i.e., if and only if the degree of u_n tends to $-\infty$.*

Proof. It is easily seen that the condition is necessary. Suppose now that u_n tends to 0. Let $P_N = \prod_{n=0}^{N}(1+u_n)$. We have $P_{N+1} - P_N = P_N u_{N+1}$. There exists an integer n_0 such that for $n \geq n_0$, we have $|u_n| \leq 1$, $|1+u_n| \leq 1$ (since the absolute value is non-Archimedean) and thus $P_n \leq P_{n_0}$. We deduce from this that $|P_{N+1} - P_N| \leq |u_{N+1}||P_{n_0}|$, for $N \geq n_0$, which implies that the sequence $(P_{N+1} - P_N)_{N\in\mathbb{N}}$ tends towards 0 and thus the convergence of P_N, from Proposition 4.3.2. ∎

Application. The series

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

is convergent. This product is called Π and was introduced by Carlitz in [89]. We will see in the sequel in what respect this product is the analogue of the real number π.

4.3.3 The Carlitz functions

In 1935 Carlitz defined two functions ψ and λ analogous respectively to the exponential and to the logarithm (see [89]). These functions are defined as follows:

$$\psi(t) = \sum_{k=0}^{+\infty} \frac{(-1)^k t^{q^k}}{F_k} \quad \text{for all } t \text{ in } \mathbf{C},$$

$$\lambda(t) = \sum_{k=0}^{+\infty} \frac{t^{q^k}}{L_k} \quad \text{for every } t \text{ such that } \deg t < \frac{q}{q-1},$$

$$\begin{aligned} \text{with } [k] &= X^{q^k} - X, \\ F_k &= [k][k-1]^q \dots [1]^{q^{k-1}} \text{ and } F_0 = 1, \\ L_k &= [k][k-1]\dots[1] \text{ and } L_0 = 1. \end{aligned}$$

It is easily seen that $\psi(t)$ is convergent for all t. Indeed $\deg(\frac{1}{F_j}t^{q^j}) = q^j(\deg t - j)$, which tends to $-\infty$, when j tends to $+\infty$. But $\lambda(t)$ is convergent if and only if $\deg t < \frac{q}{q-1}$. Indeed, $\deg(\frac{1}{L_j}t^{q^j}) = q^j(\deg t - \frac{q}{q-1}) + \frac{q}{q-1}$.

Theorem 4.3.1. *The function ψ satisfies the following properties.*

- *It is $\mathbb{F}_q$-linear, i.e., $\psi(t+u) = \psi(t) + \psi(u)$ and $\psi(ct) = c\psi(t)$, for any t, u in $\mathbf{C}$ and c in $\mathbb{F}_q$.*

- *It is periodic, i.e.,*

$$\forall t \in \mathbf{R},\ \forall E \in \mathbf{Z},\ \psi(t+E\xi) = \psi(t),$$

$$\textit{with } \xi = (X^q - X)^{1/(q-1)} \varPi \quad \textit{and} \quad \varPi = \prod_{j=0}^{+\infty}(1 - \frac{X^{q^j} - X}{X^{q^{j+1}} - X}).$$

- *For any t in $\mathbf{C}$, $\psi(t) = 0$ if and only if $t = E\xi$, with E in $\mathbb{F}_q[X]$.*
- *For any t in $\mathbf{C}$, $\psi(t) = t \prod_{E \in \mathbb{F}_q[X],\ E \neq 0} (1 - \frac{t}{E\xi})$.*
- *The function ψ satisfies the following functional equation for any t in $\mathbf{C}$:*

$$\psi(Xt) = X\psi(t) - \psi(t)^q.$$

The formal power series $\varPi$ is of course the analogue of the real number π and ξ (which is defined up to multiplication by an element of $\mathbb{F}_q^\star$) is the analogue of $2i\pi$.

Theorem 4.3.2. *The function λ satisfies the following properties.*

- *The function λ is $\mathbb{F}_q$-linear.*
- *For any t in $\mathbf{C}$ such that $\deg t < \frac{q}{q-1}$, $\psi\lambda(t) = t$.*
- *The function λ satisfies the following functional equation for any t in $\mathbf{C}$ such that $\deg t < \frac{-1}{q-1}$:*

$$\lambda(Xt) - X\lambda(t) = \lambda(t^q).$$

Carlitz showed in [89] that one can extend the definition of λ to $\mathbf{C}$, by defining modulo ξ a function $\overline{\lambda}$ with values in $\mathbf{C}$, which is the inverse of the function ψ.

Proposition 4.3.4. *There exists a function $\overline{\lambda}$ with values in $\mathbf{C}$, defined modulo ξ for any t in $\mathbf{C}$, which satisfies the following properties.*

- *The function $\overline{\lambda}$ is $\mathbb{F}_q$-linear.*
- *For any t in $\mathbf{C}$ with $\deg t < \frac{q}{q-1}$, then $\lambda(t) = \overline{\lambda}(t)$.*
- *For any t in $\mathbf{C}$, $\psi(\overline{\lambda}(t)) = t$.*

Note that Theorem 4.3.1 and 4.3.2, and Proposition 4.3.4 are due to Carlitz [89].

Carlitz also introduces in [89] an analogue of the zeta function. The zeta Carlitz function is defined as follows:

$$\zeta(m) = \sum_{G \in \mathbb{F}_q[x] \text{ and } G \text{ unitary}} 1/G^m, \quad m \geq 1.$$

It is easily seen that $\zeta(m)$ is convergent for any $m \geq 1$.

4.3.4 Some results of transcendence

Let us note that most of the "classical" transcendence properties analogous to the real case as, for instance, the Hermite-Lindemann theorem and the Gelfond-Schneider theorem were stated in the 40's by Wade (see [365] and [364]).

Theorem 4.3.3. *If α is a nonzero element of $\mathbb{F}_q((1/X))$ algebraic over $\mathbb{F}_q(X)$, then $\psi(\alpha)$ and $\lambda(\alpha)$ are transcendental.*

We deduce from this theorem the transcendence of Π.

Theorem 4.3.4. *Suppose that α is nonzero and β is an irrational element of $\mathbb{F}_q((1/X))$. Then one of the three numbers α, β, $\psi(\beta\lambda(\alpha))$ is transcendental. If α is nonzero and if one replaces $\lambda(0)$ by $E\xi$, where E belongs to $\mathbb{F}_q[X]$, then the conclusion still holds.*

Carlitz showed in [89] that $\zeta(s)/\Pi^s \in \mathbb{F}_q(x)$, for any s multiple of $(q-1)$. This property is analogous to Euler's result on the even values of the Riemann ζ function, i.e., $\zeta(2n)/\pi^{2n}$ is rational for every nonzero integer n. Note that the group of units of $\mathbb{F}_q[X]$ is $\mathbb{F}_q^\star$ and has cardinality $q-1$, whereas the multiplicative group of $\mathbb{Z}$ is $\{+1, -1\}$ an has cardinality 2. The congruences modulo 2 in the complex case are replaced here by congruences modulo $q-1$. For more details, see the survey [366].

There are essentially four methods to prove transcendence results for these functions: the "classical" method which imitates the real case (see for instance [365, 106] and Sec. 4.3.5), the use of Drinfeld modules [125, 384, 349, 366, 160], the Diophantine approximation [112] and the finite-automata method [11, 12, 14, 24, 59, 58, 213, 150, 242, 350, 351].

Let us review the transcendence results obtained via automata theory concerning Carlitz functions. The first automata result states the transcendence of the period $\xi = (X^q - X)^{\frac{1}{q-1}}\Pi$ of the exponential. More precisely, Allouche shows in [11] the transcendence of $\frac{\alpha}{\Pi}$, where α is an algebraic series. Indeed the formal power series expansion of $\frac{\alpha}{\Pi}$ is particularly interesting, in the sense that the terms of this expansion are computable in an explicit way. Furthermore the sequence of its coefficients is lacunary, i.e., most of its coefficients are zero. We expose the proof of [11] of this result in Sec. 4.4.2.

One can also show the transcendence of every linear combination over $\mathbb{F}_q(X)$ of $\frac{\zeta(s)}{\Pi^s}$, for $1 \le s \le q-2$ or the transcendence of the quotients $\frac{\lambda(P)}{\Pi^s}$, with $1 \le s \le q-2$ and $P = \sum_{v \ge -1} p_v (1/x)^v$, where p_v belongs to $\mathbb{F}_q$ and is ultimately equal to zero (see [58]).

Allouche and Shallit introduced in [22] the notion of k-regular sequences which generalizes the concept of k-automatic sequences. Becker showed in [50] an analogue of the theorem of Christol, Kamae, Mendès France and Rauzy: more precisely, k-regular power series satisfy Mahler-type functional equations; the reciprocal is true under extra hypotheses. When k is a finite field, these Mahler-type functional equations lead naturally to transcendence results. In particular, Becker shows in [50] the transcendence of the series $\sum_{k\geq 0}\alpha^{r^k}$, where α is a non-zero power series in $\mathbb{F}_q[[x_1^{-1},\dots,X_d^{-1}]]$ with nonzero constant term, which is algebraic over $\mathbb{F}_q(X_1,\dots,X_d)$, and where r is not a power of the characteristic p. This result generalizes Theorem 4.2.4. See also [126, 288].

Results of transcendence concerning the Carlitz-Goss gamma function (see for instance [14] and [242]), the transcendence of the period of the Tate elliptic curve (see [350] and [24]) were also recently proved via automata (see also the surveys [12, 351]).

4.3.5 Proof of the transcendence of $\psi(1)$ by Wade's method

The aim of this section is to prove the transcendence of $\psi(1)$ by Wade's method [365]. This proof can be considered as classical in the sense that it is close to the real-case method.

Suppose that $\psi(1)$ is algebraic over $\mathbb{F}_q(X)$. From Ore's Lemma, there exist $a_l,\cdots,a_d$ in $\mathbb{F}_q[X]$, with $a_d\neq 0$ and $a_l\neq 0$, such that

$$\sum_{i=l}^{d} a_i\psi(1)^{q^i}=0.$$

We thus have

$$\sum_{i=l}^{d} a_i(-1)^k\frac{1}{F_k^{q^i}}=0.$$

Multiply this equality by F_j, where j will be chosen large enough. Let $I=\sum_{k+i\leq j}\frac{F_j a_i(-1)^k}{F_k^{q^i}}$ and $Q=\sum_{k+i\geq j+1}\frac{F_j a_i(-1)^k}{F_k^{q^i}}$. We thus have for j large enough

$$I+Q=0,\ I\in\mathbb{F}_q[X] \text{ and } \deg(Q)<0.$$

Let us prove that $I\neq 0$, in order to get the desired contradiction.

Consider modulo $[j-l]$ the quantity

$$\frac{F_j}{F_k^{q^i}}=\frac{[j][j-1]^q\dots[k]^{j-k}\dots[1]^{q^{j-1}}}{[k]^{q^i}\dots[1]^{q^{i+k-1}}},$$

for $k+i\leq j$. Recall that $a_i=0$, if $i<l$. If $k+i<j$ or if $k+i=j$, with $i\neq l$, then $k<j-l$ and $[j-l]$ divides $\frac{F_j}{F_k^{q^i}}$. If $i=l$ and $k=j-l$, then $\frac{F_j}{F_k^{q^i}}=[j][j-1]^q\dots[j-l+1]^{q^{l-1}}\not\equiv 0 \bmod [j-l]$. Thus

$$I\equiv a_l\frac{F_j}{F_{j-l}^{q^l}}\not\equiv 0 \mod [j-l],$$

hence the theorem. ∎

Theorem 4.3.5. *The series $\psi(1)$ is transcendental over $\mathbb{F}_q(X)$.*

4.4 Some examples of automata proofs

4.4.1 Transcendence and q-kernel

Let us first illustrate how to use Christol, Kamae, Mendès France and Rauzy's theorem by showing that the q-kernel is infinite. Indeed one can distinguish in some cases the subsequences of the q-kernel with respect to their first terms.

Suppose we have the following situation. Let $(v_k)_{k\in\mathbb{N}} = (v_k(n))_{k\in\mathbb{N}}$ be subsequences in the q-kernel of the sequence v satisfying the following three conditions:

1. there exists an integer $m(k)$ such that, for any $n < m(k) : v_k(n) = 0$;
2. the sequence $(m(k))_{k\in\mathbb{N}}$ tends to $+\infty$;
3. the sequences v_k's are not identically equal to 0 for infinitely many k.

Thus the set $\{v_k;\ k \in \mathbf{N}\}$ (and hence the q-kernel of v) is infinite.

Let us consider an example of formal power series for which one can exhibit subsequences of the q-kernel fulfilling Conditions 1, 2 and 3.

4.4.2 Transcendence of $\varPi$

Let us give here an automata proof of the following theorem:

Theorem 4.4.1. *The series $\varPi$ is transcendental over $\mathbb{F}_q(X)$.*

This proof is strongly inspired by the proof of [11]. Consider the series

$$\alpha = \prod_{j=0}^{+\infty}\left(1 - \frac{X^{q^j}}{X^{q^{j+1}}}\right).$$

It is easily seen that α is algebraic over $\mathbb{F}_q(X)$ (consider α^q). Hence the transcendence of $\frac{\alpha}{\varPi}$ will imply the transcendence of $\varPi$.

We have

$$\varPi = \prod_{j=0}^{+\infty}\left(1 - \frac{X^{q^j} - X}{X^{q^{j+1}} - X}\right).$$

We thus obtain

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

Note that if

$$n = \sum_{k=1}^{+\infty} \varepsilon_k (q^k - 1) \text{ with } \varepsilon_k = 0 \text{ or } 1, \varepsilon_k = 0 \text{ for } k \text{ large enough},$$

then such a decomposition is unique.

Let $(v(n))_{n\in\mathbb{N}}$ be the sequence defined by $\sum_{n\geq 0} v(n)X^{-n} = \frac{\alpha}{\Pi}$. If $n = \sum_{k=1}^{+\infty} \varepsilon_k(q^k - 1)$ with $\varepsilon_k = 0$ or $1, \varepsilon_k = 0$ for k large enough, then $v(n) = (-1)^{\sum_{k=1}^{+\infty} \varepsilon_k}$, else $v(n) = 0$.

Let $(v_k(n))_{n\in\mathbb{N}}$ be the sequence defined by:

$$\forall n \in \mathbb{N},\ v_k(n) = v(q^k n + q^k - k).$$

Let $k \geq 2$. Let $n \in \mathbb{N}$ such that $v_k(n) \neq 0$. Thus

$\exists\ (\varepsilon_j)_{j\in\mathbb{N}}$ with $\varepsilon_j = 0$ or $1, \varepsilon_j = 0$ for j large enough, such that

$$q^k n + q^k - k = \sum_{j=1}^{+\infty} \varepsilon_j (q^j - 1).$$

We set $\sigma = \sum_{j=1}^{+\infty} \varepsilon_j$. We have

$$q^k n + q^k - k = \sum_{1\leq j\leq k-1} \varepsilon_j q^j + \sum_{l\geq k} \varepsilon_l q^l - \sigma.$$

Hence there exists an integer $\lambda \in \mathbb{Z}$ such that

$$\sigma = \lambda q^k + \sum_{1\leq j\leq k-1} \varepsilon_j q^j - q^k + k.$$

We deduce that

$$n = -\lambda + \sum_{l\geq k \text{ and } \sum_{l\geq k}\varepsilon_l = \sigma - \sum_{j\leq k-1}\varepsilon_j} \varepsilon_l q^{l-k},$$

i.e.,

$$n = -\lambda + \sum_{l\geq k \text{ and } \sum_{l\geq k}\varepsilon_l = \mathcal{S}} \varepsilon_l q^{l-k}, \tag{4.3}$$

$$\begin{aligned} \text{with } \mathcal{S} &= \sigma - \sum_{j\leq k-1} \varepsilon_j \\ &= \lambda q^k - q^k + k + \sum_{j=1}^{k-1} (\varepsilon_j - 1) q^j. \end{aligned}$$

Conversely, any integer n of the form (4.3) satisfies $v_k(n) \neq 0$.
We have furthermore

$$\lambda q^k - q^k + k - q - ... - q^{k-1} \leq \mathcal{S} \leq \lambda q^k - q^k + k.$$

Thus the difference between two values of $\mathcal{S}$ corresponding respectively to two consecutive values of λ is strictly positive. Hence the smallest integer $m(k)$ of the form (4.3) (which is also the smallest integer m satisfying $v_k(m) \neq 0$) is necessarily obtained for $\lambda = 1$. (If $\lambda \leq 0$, then $\mathcal{S} < 0$.) We thus have

$$m(k) = q + ... + q^{k-1}, \text{ i.e.}$$

$$\varepsilon_j = 1 \text{ for } 1 \leq j \leq k-1, \ \varepsilon_l = 1 \text{ for } k \leq l \leq 2k-1, \ \varepsilon_l = 0 \text{ for } l \geq 2k.$$

The sequences v_k satisfy Conditions $1, 2, 3$, which ends the proof. ■

Remark. Hellegouarch has defined in [169] an exponential function associated with a periodic sequence of endomorphisms generalizing the Carlitz exponential. Inspired by the previous proof, Recher has shown in [297] the transcendence of the period of this generalized exponential for a certain choice of endomorphisms.

4.4.3 General case

Let us come back to Conditions $1, 2, 3$. In the examples we consider here (as illustrated by the previous example), the sequence v is equal (modulo p) to the number $u(n)$ of expansions of the integer n under a given form. But it is often a difficult combinatorial problem to give an expression of $u(n)$. It is easier to work with zero elements of the sequence $(u(n))$ (i.e., with integers n which cannot be expanded in the desired form). This explains why we consider zero elements in Conditions 1,2,3. The method can be applied when the sequence u, and thus the sequence v, has long ranges of consecutive zero elements. But this method cannot be used in the case where the sequence $u = (u_n)_{n\in\mathbb{N}}$ takes nonzero values for n large enough, as illustrated by the following example.

Consider $\lambda(1)$. We have

$$\lambda(1) = \sum_{k=0}^{+\infty} \frac{1}{L_k},$$

$$\text{with } [k] = X^{q^k} - X,$$
$$L_k = [k][k-1]...[1].$$

We thus have

$$\begin{aligned}\lambda(1) &= 1+\sum_{k\geq 1}\prod_{j=1}^{k}(\frac{1}{X^{q^j}-X}),\\ &= 1+\sum_{k\geq 1}(1/X)^{(q+\ldots+q^k)}\prod_{j=1}^{k}\frac{1}{(1-(\frac{1}{X})^{q^j-1})},\\ &= 1+\sum_{k\geq 1}(1/X)^{(q+\ldots+q^k)}\prod_{j=1}^{k}\sum_{n_j\geq 0}(1/X)^{n_j(q_j-1)},\\ &= 1+\sum_{n\geq 0}v(n)X^{-n},\end{aligned}$$

where $v(n)$ equals the value modulo p of the cardinality $u(n)$ of the set

$$\{(k,n_1,...,n_k) \text{ such that } k\geq 1,\ n_i\geq 0 \text{ for } 1\leq i\leq k \text{ and}$$

$$n = q+...+q^k+\sum_{j=1}^{k}n_j(q^j-1)\}. \tag{4.4}$$

It seems difficult to give an evaluation of this cardinality. Furthermore, every integer large enough is easily seen to have a decomposition under the form (4.4); namely, there is no limitation on the size of the coefficients n_j. The sequence u takes ultimately non-zero values. Let us introduce now a limitation on the size of the coefficients n_j. Let us multiply $\lambda(1)-1$ by the product $\mathcal{P}=\prod_{j=1}^{+\infty}(1-(\frac{1}{x})^{q^j-1})$. We thus obtain

$$\begin{aligned}\mathcal{P}(\lambda(1)-1) &= \sum_{k\geq 1}(1/x)^{(q+\ldots+q^k)}\prod_{j=k+1}^{+\infty}(1-(\frac{1}{x})^{q_j-1}),\\ &= \sum_{n\geq 0}v(n)x^{-n},\end{aligned}$$

with $(v(n))_{n\in\mathbb{N}}$ defined as follows: if $n=q+...+q^k+\sum_{j=k+1}^{+\infty}\varepsilon_j(q^j-1)$, with $k\geq 1$, $\varepsilon_j=0$ or $1, \varepsilon_j=0$ for k large enough, then $v(n)=(-1)^{\sum_{j=k+1}^{+\infty}\varepsilon_j}$, otherwise $v(n)=0$.

One can check that the family of subsequences of the q-kernel $(v(q^kn+1+q+\cdots+q^{k-1})_{n\in\mathbb{N}}$ satisfy Conditions 1,2 and 3 (see for instance [58, 59]). The quantity $\mathcal{P}$ is furthermore equal to the quotient $\frac{\alpha}{\Pi}$. We thus deduce the transcendence of $\frac{\lambda(1)-1}{\Pi}$.

Remarks.

- In fact one can also obtain using the same method the transcendence of $\frac{\alpha}{\Pi}\lambda(1)$. More generally, automata methods seem to suit particularly sums and products of transcendental formal power series, since we work with subsequences.
- The transcendence of every linear combination over $\mathbb{F}_q(X)$ of $\frac{\zeta(s)}{\Pi^s}$, for $1 \leq s \leq q-2$, can be shown in a similar way (see [59]), as well as the transcendence of the quotients $\frac{\lambda(P)}{\Pi^s}$, with $1 \leq s \leq q-2$ and $P = \sum_{v \geq -1} p_v (1/x)^v$, where p_v belongs to $\mathbb{F}_q$ and is ultimately equal to zero (see [58]). Here again, the idea is to exhibit an infinite family of subsequences of the q-kernel and also to work on these quantities multiplied by a suitable power of the algebraic series α. Let us note that the restriction $s \leq q-2$ is a combinatorial limitation due to the fact that the properties of unicity in the expansions used by working on explicit formal power series expansions do not hold for $s > q$. Recall that more generally the transcendence of $\frac{\zeta(s)}{\Pi^s}$ for $s \not\equiv 0$ modulo $q-2$ was proved by Yu in [384], by using Drinfeld modules.

4.4.4 Transcendence of the bracket series

The purpose of this section is to prove the following result, which gives us an example of an application of the Christol, Kamae, Mendès France and Rauzy theorem. This result was first proved by Wade in [364]; the proof below is due to Allouche (see [11] and also [242]).

Theorem 4.4.2. *The series* $\displaystyle\sum_{k=1}^{+\infty} \frac{1}{[k]}$ *is transcendental over* $\mathbb{F}_q(X)$.

This proof makes use of the following consequence of the Christol, Kamae, Mendès France and Rauzy theorem.

Proposition 4.4.1. *Let* $(u(n))_{n\in\mathbb{N}}$ *be a sequence with values in* $\mathbb{F}_q$. *If the series* $\sum_{n\geq 0} u(n)X^{-n}$ *is algebraic over* $\mathbb{F}_q(X)$, *then the sequence* $(u(q^n - 1))_{n\in\mathbb{N}}$ *is ultimately periodic.*

Proof. Suppose that the series $\sum_{n\geq 0} u_n X^{-n}$ is algebraic; the sequence $u = (u(n))_{n\in\mathbb{N}}$ is thus q-automatic. Let $\mathcal{A}$ denote a finite q-automaton which generates the sequence u. The subsequence $(u(q^n-1))_{n\in\mathbb{N}}$ is obtained by reading in the automaton $\mathcal{A}$ strings of ones. As the number of states of $\mathcal{A}$ is finite, a long enough string of ones meets the same state twice. The sequence of states met is thus ultimately periodic, which implies that $(u(q^n-1))_{n\in\mathbb{N}}$ is also ultimately periodic.

Remarks. Let $\overline{UT^nV}$ denote, for any natural integer n, the integer of base-q expansion UT^nV, where U, T, V are words defined over $\{0, 1, \cdots, q-1\}$.

We can similarly prove that if the series $\sum_{n\geq 0} u_n X^{-n}$ is algebraic, then the sequence $(u(\overline{UT^nV}))_{n\in\mathbb{N}}$ is ultimately periodic. ■

This result corresponds to the classical *pumping lemma* in automata theory.

Exercise 4.4.1. Give another proof of Proposition 4.4.1, by using the notion of q-kernel.

Let us prove Theorem 4.4.2. We have:

$$\begin{aligned}
\sum_{k\geq 1}\frac{1}{[k]} &= \sum_{k\geq 1}\frac{1}{(X^{q^k}-X)} \\
&= \sum_{k\geq 1}\frac{1}{X^{q^k}(1-(\frac{1}{X})^{q^k-1})} \\
&= \sum_{k\geq 1}\frac{1}{X^{q^k}}\sum_{j\geq 0}(\frac{1}{X})^{j(q^k-1)} \\
&= \frac{1}{X}\sum_{k\geq 1,\ j\geq 0}(\frac{1}{X})^{(j+1)(q^k-1)} \\
&= \frac{1}{X}\sum_{k\geq 1,\ j\geq 1}\frac{1}{X^{j(q^k-1)}} \\
&= \frac{1}{X}\sum_{n\geq 1} a(n)X^{-n},
\end{aligned}$$

where $a(n)$ is the number (modulo the characteristic p) of decompositions of the integer n as $n = j(q^k-1)$, with $k\geq 1$ and $j\geq 1$, i.e.,

$$a(n) = \sum_{k\geq 1,\ (q^k-1)|n} 1.$$

Clearly the series $\displaystyle\sum_{k\geq 1}\frac{1}{[k]}$ is transcendental over $\mathbb{F}_q(X)$ if and only if the series $X\sum_{k\geq 1}\frac{1}{[k]}$ is transcendental. Suppose that the series $\sum_{n\geq 1} a(n)X^{-n}$ is algebraic over $\mathbb{F}_q(X)$. This implies that the sequence $(a(n))_{n\in\mathbb{N}}$ is q-automatic and in particular that the subsequence $a((q^n-1))_{n\in\mathbb{N}}$ is ultimately periodic. This assertion leads to a contradiction.

Indeed, it is easily seen that q^k-1 divides q^n-1 if and only if k divides n. We thus have

$$a(q^n - 1) = \sum_{k \geq 1,\ (q^k-1)|(q^n-1)} 1 = \sum_{k \geq 1,\ k|n} 1.$$

The subsequence $a((q^n - 1))_{n \in \mathbb{N}}$ is supposed to be ultimately periodic. Thus there exist $n_0 \geq 1$ and $T \geq 1$ such that:

$$\forall n \geq n_0, \sum_{k \geq 1,\ k|n} 1 = \sum_{k \geq 1,\ k|n+T} 1 \mod p.$$

This implies

$$\forall n \geq n_0,\ \forall \mu \in \mathbb{N}, \sum_{k \geq 1,\ k|n} 1 = \sum_{k \geq 1,\ k|n(1+\mu T)} 1 \mod p.$$

By Dirichlet's theorem (on the primes in arithmetical progression), there exists a prime number $\omega > n_0$ and such that $\omega = 1 + \mu T$ for some integer μ. Then for $n = \omega$

$$\sum_{k \geq 1,\ k|\omega} 1 = \sum_{k \geq 1,\ k|\omega^2} 1 \mod p,$$

i.e.,

$$2 = 3 \mod p,$$

which is the desired contradiction.

Remark. By using the same kind of arguments it can be proved that the series $\frac{1}{\Pi} \sum_{k \geq 1} \frac{1}{[k][k+i]}$, where $i \geq 1$, is transcendental over $\mathbb{F}_q(X)$.

Exercise 4.4.2. The aim of this exercise is to give another proof of this result which does not involve Dirichlet's theorem. This very satisfactory proof is due to Mendès France and Yao ([242]).

1. Prove that for any positive integers u, v, w, the number $q^w - 1$ divides $q^u(q^v - 2) + 1$ if and only if w divides the greatest common divisor of u and v.
2. Define the sequence $a_u = (a(q^u n + 1))_{n \in \mathbb{N}}$, for a fixed positive integer u. Let u, v be two distinct positive integers. Let h be the smallest integer such that h divides u and h does not divide v. Prove that $a_u(q^h - 2) - a_v(q^h - 2) \equiv 1$.
3. Deduce from this the transcendence of $\sum_{n \geq 1} a(n) X^{-n}$.
4. Prove in the same way the following theorem ([242]).

   Theorem 4.4.3. *Let $(n_k)_{n \in \mathbb{N}} k$ be a sequence of elements of $\mathbb{F}_q$ which is not ultimately equal to zero. The formal power series $\sum_{k \geq 1} \frac{n_k}{[k]}$ is transcendental over $\mathbb{F}_q(X)$.*

4.4.5 Derivation and transcendence of Π

We will see in this section how to infer from the transcendence of the bracket series the transcendence of the series Π, by using the derivation of formal power series following the method of [12], see also [349] or [122].

Definition 4.4.1. *The* derivative *of the series* $\sum_{n\geq 0} u_n X^{-n}$, *where* u_n *belongs to* $\mathbb{F}_q$, *is the series* $(\sum_{n\geq 0} u_n X^{-n})' = -\sum_{n\geq 0} n u_n X^{-n-1}$.

Proposition 4.4.2. *The derivative of an algebraic series is algebraic.*

Remark. The converse is generally not true. For instance, if $\sum u_n X^{-n}$ is transcendental then $(\sum u_n X^{-n})^q = \sum u_n X^{-qn}$ is also transcendental but its derivative is equal to 0 (in $\mathbb{F}_q((1/X))$).

Let us prove that the transcendence of the bracket series implies the transcendence of Π. We have

$$\Pi = \prod_{j=1}^{+\infty}(1 - \frac{[j]}{[j+1]}),$$

i.e.,

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

The derivative of $\frac{X^{q^{j+1}} - X^{q^j}}{X^{q^{j+1}} - X}$ is equal to $\frac{X^{q^{j+1}} - X^{q^j}}{(X^{q^{j+1}} - X)^2}$. The logarithmic derivative of Π, $\frac{\Pi'}{\Pi}$, is thus equal to

$$\frac{\Pi'}{\Pi} = \sum_{j\geq 1} \frac{1}{(X^{q^{j+1}} - X)},$$

i.e.,

$$\frac{\Pi'}{\Pi} = \sum_{j\geq 2} \frac{1}{[j]}.$$

The series Π is hence transcendental. Otherwise the series $\frac{\Pi'}{\Pi}$ would be algebraic and so would be the bracket series. ∎

4.5 Conclusion

How can one recognize that a sequence is not k-automatic, or in other words, that a formal power series with coefficients in a finite field is transcendental? Let us review some more techniques to disprove the automaticity of a sequence.

- Let us recall that an automatic sequence has a low complexity function, due to its strong underlying structure: the complexity of a fixed point of a substitution of constant length satisfies (see [101] and Chap. 3)

  $$\exists C,\ \forall n,\ p(n) \leq Cn.$$

  This disproves the automaticity of a high complexity sequence. Note more generally that the complexity of a fixed point of a substitution satisfies (see [133, 269])

  $$\exists C',\ \forall n,\ p(n) \leq C'n^2,$$

  but if the substitution is primitive, then we get (see Proposition 3.3.3)

  $$\exists C'',\ \forall n,\ p(n) \leq C''n.$$

- If the frequencies of the factors of an automatic sequence exist, they are rational (for more precise results on frequencies of automatic sequences, see [101]). Let us recall that if the corresponding substitution is primitive, then the frequencies exist.
- Shallit introduces in [325] a *measure of automaticity* of a sequence $u = (u(n))_{n\in\mathbb{N}}$ over a finite alphabet: the k-automaticity of a sequence is defined as the smallest possible number of states in any deterministic finite automaton which generates the prefix of size n of this sequence. This measure tells quantitatively how “close” a sequence is to being k-automatic. Note that the automaton is fed with the digits i, starting from the *least significant digit*: there are languages of low automaticity whose mirror image has high automaticity (see [159]).
- Yao gives in [382] non-automaticity criteria motivated by a transcendence criterion due to de Mathan (see [112]). Originally the work of de Mathan used Diophantine approximation but Koskas gave a proof using automata of this criterion in [213]. In particular, Yao gives a simple proof of a result due to Mkaouar: the sequence of partial quotients in the continued fraction expansion of the Baum-Sweet series (see Chap. 2) is not p-automatic, for any integer $k \geq 2$.
- Durand has generalized in [130, 129] Christol, Kamae, Mendès France and Rauzy theorem to uniformly recurrent substitutive sequences. This characterization is based on the notion of *return words* and *derived sequence.* A return word over the factor W is a word separating two successive occurrences of W; a derived sequence of a given minimal sequence u, is a sequence obtained by coding u by return words over a non-empty prefix of

the sequence u. The characterization is the following: a uniformly recurrent sequence is substitutive if and only if the set of its return words is finite. This result was proved independently by Holton and Zamboni [175]. It has been extended to substitutive tilings by Priebe [282]. Note that the notion of return words has many applications in arithmetics with generalizations of Cobham's theorem [131], or in dynamics with a description of minimal stationary Bratelli-Verskik diagrams [132]. See also Chap. 12.

Acknowledgements. I am greatly indebted to J.-P. Allouche, M. Mendès France, M. Koskas and A. Siegel for their many comments.