Rational approximations to algebraic Laurent series with coefficients in a finite field

by

ALINA FIRICEL (St Martin d'Hères)

1. Introduction. One of the basic question in Diophantine approximation is how well real numbers can be approximated by rationals. The theory of rational approximation of real numbers was transposed to function fields after the pioneering works of Maillet [15] in 1906 and Gill [10] in 1930. In the present work, we are interested in the way algebraic Laurent series with coefficients in a finite field can be approximated by rational functions.

Given a field \mathbb{K} , we let $\mathbb{K}(T)$, $\mathbb{K}[[T^{-1}]]$ and $\mathbb{K}((T^{-1}))$ denote, respectively, the field of rational functions, the ring of formal series and the field of Laurent series over the field \mathbb{K} . We also consider the absolute value defined on $\mathbb{K}(T)$ by

$$|P/Q| = |T|^{\deg P - \deg Q}$$

for $(P,Q) \in \mathbb{K}[T]^2$, where |T| is a fixed real number larger than 1. The field of Laurent series in 1/T, usually denoted by $\mathbb{K}((T^{-1}))$, should be seen as a completion of the field $\mathbb{K}(T)$ for this absolute value. Thus, if f is a nonzero element of $\mathbb{K}((T^{-1}))$ defined by

$$f(T) = a_{i_0}T^{-i_0} + a_{i_0+1}T^{-i_0-1} + \cdots,$$

where $i_0 \in \mathbb{Z}$, $a_i \in \mathbb{K}$, $a_{i_0} \neq 0$, we have $|f| = |T|^{-i_0}$. We also say that a Laurent series is *algebraic* if it is algebraic over the field $\mathbb{K}(T)$ of rational functions. The *degree* of an algebraic Laurent series f in $\mathbb{K}((1/T))$ is defined as $[\mathbb{K}(T)(f) : \mathbb{K}(T)]$, the degree of the field extension generated by f.

We recall that the *irrationality exponent* of a given Laurent series f, denoted by $\mu(f)$, is the supremum of the real numbers τ for which the inequality

$$\left|f - \frac{P}{Q}\right| < \frac{1}{|Q|^{\tau}}$$

²⁰¹⁰ Mathematics Subject Classification: 11J61, 11J82, 11T99, 68R15.

Key words and phrases: automatic sequences, finite fields, irrationality measures, Laurent series, uniform morphisms.

A. Firicel

has infinitely many solutions $(P,Q) \in \mathbb{K}[T]^2$, $Q \neq 0$. Thus, $\mu(f)$ measures the quality of the best rational approximations to f.

Throughout this paper, p denotes a prime number and q is a power of p. Our aim is to study the irrationality exponent of algebraic Laurent series in the field $\mathbb{F}_q((1/T))$.

In 1949, Mahler [14] observed that the analogue of Liouville's fundamental inequality holds true for algebraic Laurent series over a field of positive characteristic.

THEOREM 1.1 (Mahler, 1949). Let \mathbb{K} be a field of positive characteristic and $f \in \mathbb{K}((T^{-1}))$ be an algebraic Laurent series over $\mathbb{K}(T)$ of degree d > 1. Then there exists a positive real number C such that

$$\left|f - \frac{P}{Q}\right| \ge \frac{C}{|Q|^d}$$

for all $(P,Q) \in \mathbb{K}[T]^2$ with $Q \neq 0$.

In other words, Mahler's theorem tells us that the irrationality exponent of an algebraic irrational Laurent series is at most equal to its degree.

In the case of real numbers, Liouville's theorem was superseded by the works of Thue [24], Siegel [21], Dyson [8] and others, leading to the famous Roth theorem [19], which states that the irrationality exponent of an irrational algebraic real number is equal to 2. In 1960, Uchiyama obtained an analogue of Roth's theorem [25] for the case of Laurent series with coefficients in a field of characteristic 0.

When the base field has positive characteristic, it is well-known that there is no direct analogue of Roth's theorem. In fact, the Liouville–Mahler theorem turns out to be optimal. In order to see this, it is sufficient to consider the element $f_q \in \mathbb{F}_q((T^{-1}))$ defined by $f_q(T) = \sum_{i \ge 0} T^{-q^i}$. It is not difficult to see that f_q is an algebraic Laurent series of degree q (since it satisfies the equation $f^{\dot{q}} - f + T^{-1} = 0$ while the irrationality exponent of f is equal to q. Note that these examples are sometimes referred to as Mahler's algebraic Laurent series. In the same direction, Osgood [16] and Baum and Sweet [5] gave examples of algebraic Laurent series of various degrees for which Liouville's bound is the best possible. For a special class of algebraic Laurent series, the bound given by Liouville for the irrational exponent was improved by Osgood [16, 17]. In 1976, he proved an analog of Thue's theorem for algebraic Laurent series which are not solutions of a rational Riccati differential equation. In 1996, de Mathan and Lasjaunias [13] proved that the analogue of Thue's theorem actually holds for every algebraic Laurent series in $\mathbb{K}((T^{-1}))$, \mathbb{K} being an arbitrary field of characteristic p, which satisfies no equation of the form $f = (Af^{p^s} + B)/(Cf^{p^s} + D)$, where $A, B, C, D \in \mathbb{K}[T]$, not all zero, and $s \in \mathbb{N}^*$. Laurent series satisfying such an equation are called *hyperquadratic* and were studied by many authors [12, 20, 22, 26]. Note that every hyperquadratic Laurent series also satisfies a Riccati differential equation.

Apart from the results obtained by Mahler, Lasjaunias–de Mathan or Osgood, we do not know other general methods of bounding from above the irrationality exponent of algebraic Laurent series over $\mathbb{F}_q(T)$. It is worth mentioning that the situation for function fields totally differs from the one of real numbers. For instance Schmidt [20] and Thakur [22] independently proved that the set of irrationality exponents of algebraic Laurent series contains all rational real numbers greater than or equal to 2.

The aim of this paper is to introduce a new approach in order to bound from above the irrationality exponent of an algebraic Laurent series, which is based on the use of the Laurent series expansion. As a starting point, we use a theorem of Christol [6] which characterizes in terms of automata the algebraic Laurent series with coefficients in a finite field. More precisely, we recall that $f(T) = \sum_{i\geq 0} a_i T^{-i} \in \mathbb{F}_q[[T^{-1}]]$ is algebraic if and only if the sequence $(a_i)_{i\geq 0}$ is generated by a *p*-automaton. Furthermore, we recall that by a classical result of Eilenberg [9] the so-called *p*-kernel of a *p*-automatic sequence is always finite (see Section 3.1).

Our main result is the following explicit general upper bound for the irrationality exponent of algebraic Laurent series in $\mathbb{F}_p((1/T))$.

THEOREM 1.2. Let $f(T) = \sum_{i \geq -k} a_i T^{-i}$ be an algebraic Laurent series with coefficients in a finite field of characteristic p. Let s be the cardinality of the p-kernel of $\mathbf{a} = (a_i)_{i\geq 0}$ and e be the number of states of the minimal automaton generating \mathbf{a} (in direct reading). Then the irrationality exponent $\mu(f)$ satisfies

(1)
$$\mu(f) \le p^{s+1}e.$$

The approach we use to prove Theorem 1.2 already appears in a different framework in [1, 2, 3]. It is essentially based on repetitive patterns occurring in automatic sequences. More precisely, each algebraic formal series $f(T) = \sum_{i\geq 0} a_i T^{-i}$ is identified with a *p*-automatic sequence $\mathbf{a} := (a_i)_{i\geq 0}$ over \mathbb{F}_q . Then we use a theorem of Cobham which characterizes *p*-automatic sequences in terms of *p*-uniform morphisms of free monoids (see Section 2.2). As a consequence of this result and of the pigeonhole principle, we are able to find infinitely many pairs of finite words (U_n, V_n) and a number $\omega > 1$ such that $U_n V_n^{\omega}$ is a prefix of \mathbf{a} for every positive integer *n*. Hence, there exists an infinite sequence of pairs (P_n, Q_n) of polynomials such that the Laurent series expansion of the rational function P_n/Q_n is the (ultimately periodic) sequence $\mathbf{c}_n := U_n V_n^{\infty}$. The sequence of rational functions P_n/Q_n provides good rational approximations to *f* since the words \mathbf{a} and \mathbf{c}_n have the common prefix $U_n V_n^{\omega}$. Furthermore, the lengths of U_n and V_n are respectively of the form kp^n and ℓp^n . Using such approximations we are able to prove the following result (see Theorem 3.7):

$$\frac{k+\omega\ell}{k+\ell} \le \mu(f) \le \frac{p^{s+1}(k+\ell)}{(\omega-1)\ell}.$$

In practice, it may happen that we can choose U_n and V_n such that **a** and \mathbf{c}_n have the same first $(k + \omega \ell)p^n$ digits, while the $((k + \omega \ell)p^n + 1)$ th digits are different. In this case, the upper bound we obtain for the irrationality exponent may be much better and in particular does not depend anymore on the cardinality of the *p*-kernel. Furthermore, in the case where we can prove that $(P_n, Q_n) = 1$ for all *n* large enough, we obtain a significant improvement on the upper bound

$$\frac{k+\omega\ell}{k+\ell} \le \mu(f_{\mathbf{a}}) \le \max\left(\frac{k+\omega\ell}{k+\ell}, 1+\frac{p(k+\ell)}{(\omega-1)\ell}\right);$$

as will also be explained in Remark 3.8, that sometimes leads to the exact value $\mu(f)$. Note that when working with similar constructions involving real numbers, it is well-known that this coprimality assumption is usually difficult to check (see [3]).

In the second part of this paper, we introduce a new approach in order to overcome this difficulty. We provide an algorithm that allows us to check, in finite time, whether the polynomials P_n and Q_n , associated with an algebraic Laurent series f, are relatively prime for all n large enough. In order to do this, we observe that the rational approximations we obtain have a very specific form: the roots of Q_n can only be 0 or ℓ th roots of unity (see Section 3.4). Then we have to develop a calculus allowing one to compute the polynomials $P_n(T)$. In order to do this, we introduce some matrices associated with p-morphisms. These matrices generalize the so-called incidence matrix of the underlying morphism (see Section 4) and their study could also be of independent interest.

In the last part of this paper, we illustrate the relevance of our approach with a few examples. We give several algebraic Laurent series for which we are able to compute the exact value of the irrationality exponent. In particular, we prove the following result.

THEOREM 1.3. Let f be a root of the following equation over $\mathbb{F}_2(T)$:

$$X^4 + X + \frac{T}{T^4 + 1} = 0.$$

Then $\mu(f) = 3$ *.*

2. Terminology and basic notions. A *word* is a finite or infinite sequence of symbols (or letters) belonging to a nonempty set \mathcal{A} , called the *alphabet*. We usually denote words by juxtaposition of their symbols.

Given an alphabet \mathcal{A} , we let $\mathcal{A}^* := \bigcup_{m=0}^{\infty} \mathcal{A}^m$ denote the set of finite words over \mathcal{A} . Let $V := a_0 a_1 \cdots a_{m-1} \in \mathcal{A}^*$; then the integer m is the *length* of V and is denoted by |V|. A word of length 0 is an empty word, usually denoted by ε . We also let \mathcal{A}^m denote the set of all finite words of length mand by $\mathcal{A}^{\mathbb{N}}$ the set of all infinite words over \mathcal{A} . We typically use the uppercase italic letters U, V, W to represent elements of \mathcal{A}^* , and bold lowercase letters **a**, **b**, **c** to represent infinite words.

For any nonnegative integer n, we write $U^n := UU \cdots U$ (*n*-fold concatenation of the word U). More generally, for any positive real number ω we let U^{ω} denote the word $U^{\lfloor \omega \rfloor}U'$, where U' is the prefix of U of length $\lceil (\omega - \lfloor \omega \rfloor) |U| \rceil$. Here, $\lfloor \zeta \rfloor$ and $\lceil \zeta \rceil$ denote, respectively, the integer part and the upper integer part of the real number ζ . We also write $U^{\infty} := UU \cdots$, that is, U concatenated (with itself) infinitely many times.

An infinite word **a** is *periodic* if there exists a finite word V such that $\mathbf{a} = V^{\infty}$. An infinite word is *ultimately periodic* if there exist two finite words U and V such that $\mathbf{a} = UV^{\infty}$.

Throughout this paper, we set $\mathcal{A}_m := \{0, 1, \dots, m-1\}$ for $m \ge 1$, which will serve as a generic alphabet.

2.1. Automatic sequences and Christol's theorem. Let $k \ge 2$ be an integer. An infinite sequence $\mathbf{a} = (a_i)_{i\ge 0}$ is k-automatic if, roughly speaking, there exists a finite automaton which produces the term a_i as output, when the input is the k-ary expansion of i.

For a formal definition of an automatic sequence, let us define a kdeterministic finite automaton with output or, briefly, k-DFAO. This is a 5-tuple

$$M = (Q, \delta, q_0, \Delta, \varphi)$$

where Q is a finite set of states, $\delta: Q \times \mathcal{A}_k \to Q$ is the transition function, q_0 is the initial state, Δ is the output alphabet and $\varphi: Q \to \Delta$ is the output function. For a finite word $W = w_r w_{r-1} \cdots w_0 \in \mathcal{A}_k^r$, we let $[W]_k$ denote the number $\sum_{i=0}^r w_i k^i$.

We now say that a sequence $\mathbf{a} = (a_i)_{i\geq 0}$ is *k*-automatic if there exists a *k*-DFAO such that $a_i = \varphi(\delta(q_0, w))$ for all $i \geq 0$ and all words W with $[W]_k = i$.

A classical example of automatic sequence is the so-called Thue–Morse sequence: $\mathbf{t} = (t_i)_{i\geq 0} = 01101001100\cdots$, which counts the number of 1's (mod 2) in the base-2 representation of *i*. It is generated by the automaton depicted in Fig. 1. More references on automatic sequences can be found in the monograph [4].

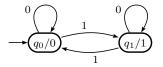


Fig. 1. Automaton generating the Thue–Morse sequence

If we now consider the Laurent series $f_{\mathbf{t}}(T) = \sum_{i \ge 0} t_i T^{-i}$ as an element of $\mathbb{F}_2((T^{-1}))$, one can check that $f_{\mathbf{t}}$ satisfies the algebraic equation

 $(T+1)^3 f_{\mathbf{t}}^2(T) + T(T+1) f_{\mathbf{t}}(T) + 1 = 0.$

Hence, f_t is an algebraic Laurent series over $\mathbb{F}_2(T)$ whose sequence of coefficients is a 2-automatic sequence. Actually, this is not an isolated case. Indeed, the famous theorem of Christol [6] precisely describes the algebraic Laurent series over $\mathbb{F}_q(T)$:

THEOREM 2.1 (Christol, 1979). Let $f_{\mathbf{a}}(T) = \sum_{i \geq -i_0} a_i T^{-i}$ be a Laurent series with coefficients in a finite field of characteristic p. Then $f_{\mathbf{a}}$ is algebraic over $\mathbb{F}_q(T)$ if and only if the sequence $\mathbf{a} = (a_i)_{i\geq 0}$ is p-automatic.

We also mention that a well-known result of Eilenberg states that a sequence is p-automatic if and only if it is q-automatic for any power q of p.

2.2. Morphisms and Cobham's theorem. Let \mathcal{A} (respectively \mathcal{B}) be a finite alphabet and let \mathcal{A}^* (respectively \mathcal{B}^*) be the corresponding free monoid. A *morphism* is a map σ from \mathcal{A}^* to \mathcal{B}^* such that $\sigma(UV) = \sigma(U)\sigma(V)$ for all $U, V \in \mathcal{A}^*$. Since concatenation is preserved, it is then possible to define a morphism defined on \mathcal{A} .

Let k be a positive integer. A morphism σ is said to be k-uniform if $|\sigma(a)| = k$ for any $a \in \mathcal{A}$. A k-uniform morphism will also be called a k-morphism. If k = 1, then σ is simply called a *coding*.

If $\mathcal{A} = \mathcal{B}$ we can iterate the application of σ . Hence, if $a \in \mathcal{A}$, then $\sigma^0(a) = a$ and $\sigma^i(a) = \sigma(\sigma^{i-1}(a))$ for every $i \geq 1$. Let $\sigma : \mathcal{A} \to \mathcal{A}^*$ be a morphism. The set $\mathcal{A}^* \cup \mathcal{A}^{\mathbb{N}}$ is endowed with its natural topology.

Roughly, two words are close if they have a long common prefix. We can thus extend the action of a morphism by continuity to $\mathcal{A}^* \cup \mathcal{A}^{\mathbb{N}}$. Then a word $\mathbf{a} \in \mathcal{A}^{\mathbb{N}}$ is a fixed point of a morphism σ if $\sigma(\mathbf{a}) = \mathbf{a}$.

A morphism σ is *prolongable* on $a \in \mathcal{A}$ if $\sigma(a) = aX$ for some $X \in \mathcal{A}^+ := \mathcal{A}^* \setminus \{\varepsilon\}$ such that $\sigma^k(X) \neq \varepsilon$ for any $k \in \mathbb{N}$. If σ is prolongable then the sequence $(\sigma^i(a))_{i>0}$ converges to the infinite word

$$\sigma^{\infty}(a) = \lim_{i \to \infty} \sigma^i(a) = aX\sigma(X)\sigma^2(X)\sigma^3(X)\dots$$

With this notation, we can now cite an important theorem of Cobham, which gives a characterization of k-automatic sequences in terms of k-uniform morphisms. THEOREM 2.2 (Cobham, 1972). Let $k \ge 2$. Then a sequence $\mathbf{a} = (a_i)_{i\ge 0}$ is k-automatic if and only if it is the image, under a coding, of a fixed point of a k-uniform morphism.

3. Proof of Theorem 1.2. Theorem 1.2 is an easy consequence of the more precise result established in Theorem 3.7. In order to prove Theorem 3.7, we first establish an approximation lemma, which is the analog of a classical result in Diophantine approximation (Lemma 3.2). Then we show how to construct, starting with an arbitrary algebraic Laurent series f with coefficients in a finite field, an infinite sequence of rational approximations of f satisfying the assumptions of our approximation lemma. We thus deduce the expected upper bound for the irrationality exponent of f.

All along this section, we provide comments and remarks allowing one to improve in most cases this general upper bound (see in particular Remark 3.8 and Section 3.4).

3.1. Maximal repetitions in automatic sequences. Before stating our approximation lemma, we first recall a useful result, which will allow us later to control repetitive patterns occurring as prefixes of automatic sequences. The proof of the following lemma can be found in [2, Lemma 5.1, p. 1356]. Before stating it, we recall that the *kernel* $K_k(\mathbf{a})$ of a k-automatic sequence $\mathbf{a} = (a_i)_{i\geq 0}$ is defined as the set of all subsequences of the form $(a_{k^n i+l})_{i\geq 0}$, where $n \geq 0$ and $0 \leq l < k^n$. Furthermore, we recall that by a result of Eilenberg a sequence \mathbf{a} is k-automatic if and only if $K_k(\mathbf{a})$ is finite.

LEMMA 3.1. Let **a** be a non-ultimately periodic k-automatic sequence defined on an alphabet \mathcal{A} . Let $U \in \mathcal{A}^*$, $V \in \mathcal{A}^* \setminus \{\varepsilon\}$ and $\omega \in \mathbb{Q}$ be such that UV^{ω} is a prefix of **a**. Let s be the cardinality of the k-kernel of **a**. Then

$$\frac{|UV^{\omega}|}{|UV|} < k^s.$$

3.2. An approximation lemma. We start with the following result which is, in fact, an analog of Lemma 4.1 in [3] for Laurent series with coefficients in a finite field. We also recall the proof, since it is not very long and it may be of independent interest.

LEMMA 3.2. Let f(T) be a Laurent series with coefficients in \mathbb{F}_q . Let δ , ρ and θ be real numbers such that $0 < \delta \leq \rho$ and $\theta \geq 1$. Assume that there exists a sequence $(P_n/Q_n)_{n\geq 1}$ of rational fractions with coefficients in \mathbb{F}_q and some positive constants c_0 , c_1 and c_2 such that

(i) $|Q_n| < |Q_{n+1}| \le c_0 |Q_n|^{\theta}$,

(ii)
$$c_1/|Q_n|^{1+\rho} \le |f - P_n/Q_n| \le c_2/|Q_n|^{1+\delta}.$$

Then the irrationality exponent $\mu(f)$ satisfies

(2)
$$1 + \delta \le \mu(f) \le \theta(1+\rho)/\delta$$

Furthermore, if there is $N \in \mathbb{N}^*$ such that $(P_n, Q_n) = 1$ for any $n \ge N$, then

$$1 + \delta \le \mu(f) \le \max(1 + \rho, 1 + \theta/\delta)$$

In this case, if $\rho = \delta$ and $\theta \leq \delta^2$, then $\mu(f) = 1 + \delta$.

Proof. The left-hand inequality of (2) is clear. We therefore turn to the other inequality. Let $P/Q \in \mathbb{F}_q(T)$ be such that |Q| is large enough. Then there exists a unique integer $n = n(Q) \ge 2$ such that

(3)
$$|Q_{n-1}| < (2c_2|Q|)^{1/\delta} \le |Q_n|.$$

If $P/Q \neq P_n/Q_n$ then

$$\left|\frac{P}{Q} - \frac{P_n}{Q_n}\right| \ge \frac{1}{|QQ_n|},$$

and using (3) and (ii) we get

$$\left| f - \frac{P_n}{Q_n} \right| \le \frac{c_2}{|Q_n|^{1+\delta}} = \frac{c_2}{|Q_n| |Q_n|^{\delta}} \le \frac{1}{2|Q| |Q_n|}.$$

By the triangle inequality, we have

$$\left|f - \frac{P}{Q}\right| \ge \left|\frac{P}{Q} - \frac{P_n}{Q_n}\right| - \left|f - \frac{P_n}{Q_n}\right|$$

Now (i) together with (3) implies that $|Q_n| \leq c_0 |Q_{n-1}|^{\theta} < c_0 (2c_2 |Q|)^{\theta/\delta}$. Thus,

$$\left| f - \frac{P}{Q} \right| \ge \frac{1}{2|Q| |Q_n|} \ge \frac{1}{2|Q| c_0 (2c_2|Q|)^{\theta/\delta}} \ge \frac{c_3}{|Q|^{\theta(1+\rho)/\delta}}$$

since $1 + \theta/\rho \leq \theta + \theta/\rho$ (because $\theta \geq 1$), with $c_3 := 1/(2c_0(2c_2)^{\theta/\delta})$. On the other hand, if $P/Q = P_n/Q_n$, then

$$\left| f - \frac{P}{Q} \right| = \left| f - \frac{P_n}{Q_n} \right| \ge \frac{c_1}{|Q_n|^{1+\rho}} \ge \frac{c_1}{(c_0(2c_2|Q|)^{\theta/\rho})^{1+\rho}} = \frac{c_4}{|Q|^{\theta(1+\rho)/\delta}},$$

where $c_4 = c_1/(c_0^{1+\rho}(2c_2)^{\theta(1+\rho)/\delta})$.

The case where $(P_n, Q_n) = 1$ is treated in a similar way and we refer the reader to [3, Lemma 4, p. 10]. The proof consists, as previously, of two cases, but when $P_n/Q_n = P/Q$ and P/Q is reduced, then $Q_n = Q$; this permits one to obtain an improved upper bound.

Note that the second part of Lemma 3.2 is also known as Voloch's Lemma; for more details, we refer the reader to the original paper of [26], and to Thakur's monograph [23, p. 314].

3.3. Construction of rational approximations via Christol's theorem. Let

$$f(T) := \sum_{i \ge 0} a_i T^{-i} \in \mathbb{F}_q[[T^{-1}]]$$

be an irrational algebraic Laurent series over $\mathbb{F}_q(T)$.

We recall that, by Christol's theorem, the sequence $\mathbf{a} := (a_i)_{i\geq 0}$ is *p*-automatic. (In all that follows, we will only work with *p*- or p^r -automatic sequences, $r \geq 1$. The letter k will denote the length of some finite words.) According to Cobham's theorem, there exist $m \geq 1$, a *p*-morphism

$$\sigma:\mathcal{A}_m\to\mathcal{A}_m^*$$

and a coding

$$\varphi: \mathcal{A}_m \to \mathbb{F}_q$$

such that $\mathbf{a} = \varphi(\sigma^{\infty}(a))$ where $a \in \mathcal{A}_m$.

In all that follows, we let $f_{\mathbf{a}}(T) = \sum_{i\geq 0} a_i T^{-i}$ denote the Laurent series associated with the infinite word $\mathbf{a} = (a_i)_{i\geq 0}$.

We also give the following definition for a polynomial associated with a finite word.

DEFINITION 3.3. Let $U = a_0 a_1 \cdots a_{k-1}$ be a finite word over a finite field. We associate with U the polynomial $P_U(T) := \sum_{j=0}^{k-1} a_{k-1-j} T^j$. If $U = \varepsilon$, we set $P_U(T) = 0$.

For example, if we consider the word $U = 1020310 \in \mathcal{A}_5$ then

$$P_U(T) = T^6 + 2T^4 + 3T^2 + T$$

is a polynomial with coefficients in \mathbb{F}_5 .

Using this notation, we have the following two lemmas.

LEMMA 3.4. Let U, V be two finite words such that $|U| = k \in \mathbb{N}$ and $|V| = \ell \in \mathbb{N}$ and let $\mathbf{a} := UV^{\infty}$. Then

$$f_{\mathbf{a}}(T) = \frac{P_U(T)(T^{\ell} - 1) + P_V(T)}{T^{k-1}(T^{\ell} - 1)}.$$

If k = 0, we have

$$f_{\mathbf{a}}(T) = \frac{TP_V(T)}{T^\ell - 1}.$$

Proof. Let $U := a_0 a_1 \cdots a_{k-1}$ and $V := b_0 b_1 \cdots b_{\ell-1}$. Writing the associated Laurent series with $\mathbf{a} := UV^{\infty}$, we have

$$f_{\mathbf{a}}(T) = (a_0 + a_1 T^{-1} + \dots + a_{k-1} T^{-(k-1)}) + (b_0 T^{-k} + \dots + b_{\ell-1} T^{-(k+\ell-1)}) + \dots$$

and then factorizing $T^{-(k-1)}, T^{-k}, T^{-(k+\ell)}, T^{-(k+2\ell)}, \ldots$ and using the definition of $P_U(T)$ and $P_V(T)$ (see Def. 3.3), we obtain

$$f_{\mathbf{a}}(T) = T^{-(k-1)}P_U(T) + T^{-k}(b_0 + b_1T^{-1} + \dots + b_{\ell-1}T^{-(\ell-1)}) + T^{-(k+\ell)}(b_0 + \dots + b_{\ell-1}T^{-(\ell-1)}) + \dots = T^{-(k-1)}P_U(T) + T^{-(k+\ell-1)}P_V(T)(1 + T^{-\ell} + T^{-2\ell} + T^{-3\ell} + \dots) = \frac{P_U(T)(T^{\ell} - 1) + P_V(T)}{T^{k-1}(T^{\ell} - 1)}.$$

The second identity of the lemma immediately follows by replacing k = 0 in the identity given above.

LEMMA 3.5. Let $\mathbf{a} = (a_i)_{i\geq 0}$ and $\mathbf{b} = (b_i)_{i\geq 0}$ be infinite sequences over a finite alphabet, satisfying $a_i = b_i$ for $0 \leq i \leq L - 1$, where $L \in \mathbb{N}^*$. Then

$$|f_{\mathbf{a}} - f_{\mathbf{b}}| \le 1/|T|^L$$

with equality when $a_L \neq b_L$.

Proof. This follows immediately from the definition of an ultrametric norm. \blacksquare

We now construct a sequence $(P_n/Q_n)_{n\geq 0}$ of rational fractions satisfying the assumptions of Lemma 3.2. The approach we use appears in [2] and is essentially based on the repetitive patterns occurring in automatic sequences.

The sequence **a** being *p*-automatic, the *p*-kernel is finite. We let *e* denote the number of states of the minimal automaton generating **a** (in *direct reading*) and *s* the cardinality of the *p*-kernel. Consider a prefix *P* of $\sigma^{\infty}(a)$ of length e+1. Observe that *e* is greater than or equal to the cardinality of the internal alphabet of **a**, that is, \mathcal{A}_m . It follows, from the pigeonhole principle that there exists a letter $b \in \mathcal{A}_m$ occurring at least twice in *P*. This means that there exist two (possibly empty) words U' and V' and a letter *b* (both defined over \mathcal{A}_m) such that

$$P := U'bV'b.$$

Now, if we set U := U', V := bV', |U| := k, $|V| := \ell$, $\omega := 1 + 1/\ell$, then UV^{ω} is a prefix of $\sigma^{\infty}(a)$.

Let $n \in \mathbb{N}$, $U_n := \varphi(\sigma^n(U))$ and $V_n = \varphi(\sigma^n(V))$. Since $\mathbf{a} = \varphi(\sigma^{\infty}(a))$

it follows that, for any $n \in \mathbb{N}$, $U_n V_n^{\omega}$ is a prefix of **a**. Notice also that $|U_n| = |U|p^n$ and $|V_n| = |V|p^n$ and the sequence $(|V_n|)_{n\geq 1}$ is increasing.

If k > 0, then, for any $n \ge 1$, we set

(4)
$$Q_n(T) = T^{kp^n - 1}(T^{\ell p^n} - 1).$$

(If k = 0, then we set $Q_n(T) = T^{\ell p^n} - 1$ for any $n \ge 1$.)

Let \mathbf{c}_n denote the infinite word $U_n V_n^{\infty}$. There exists $P_n(T) \in \mathbb{F}_q[T]$ such that

$$f_{\mathbf{c}_n}(T) = \frac{P_n(T)}{Q_n(T)}.$$

More precisely, by Lemma 3.4, the polynomial $P_n(T)$ may be defined by

(5)
$$P_n(T) = P_{U_n}(T)(T^{\ell p^n} - 1) + P_{V_n}(T) \quad \text{for } k > 0$$

(and $P_n(T) = TP_{V_n}(T)$ for k = 0).

Since **a** and \mathbf{c}_n have the common prefix $U_n V_n^{\omega}$, Lemma 3.5 yields

(6)
$$\left| f_{\mathbf{a}} - \frac{P_n}{Q_n} \right| \le \frac{c_2}{\left| Q_n \right|^{\frac{k+\omega\ell}{k+\ell}}}$$

where $c_2 = |T|^{\frac{k+\ell}{k+\omega\ell}}$.

Furthermore, if **a** and \mathbf{c}_n have the common prefix $U_n V_n^{\omega}$ and their $((k + \omega \ell)p^n + 1)$ th letters are different, then, by Lemma 3.5, inequality (6) becomes an equality. On the other hand, we also have the following result, which is an easy consequence of Lemma 3.1.

LEMMA 3.6. Let s be the cardinality of the p-kernel of the sequence $\mathbf{a} := (a_i)_{i>0}$. Then

$$\left| f_{\mathbf{a}} - \frac{P_n}{Q_n} \right| \ge \frac{1}{|Q_n|^{p^s}}.$$

Proof. Using Lemma 3.1 we obtain

$$|U_n V_n^{\omega}| < p^s |U_n V_n|.$$

This implies that **a** and **c**_n cannot have the same first $p^{s}|U_{n}V_{n}|$ digits. Hence

$$\left| f_{\mathbf{a}} - \frac{P_n}{Q_n} \right| \ge \frac{1}{|T|^{(|U_n| + |V_n|)p^s}} = \frac{1}{(|T| |Q_n|)^{p^s}} \ge \frac{c_1}{|Q_n|^{p^s}},$$

where $c_1 := 1/|T|^{p^s}$.

This shows that $(P_n/Q_n)_{n\geq 1}$ satisfies the assumptions of Lemma 3.2 with $\theta = p, \ \rho = p^s - 1$ and $\delta = (\omega - 1)\ell/(k + \ell)$. With this notation, we obtain the following theorem.

THEOREM 3.7. Let $f_{\mathbf{a}}(T) = \sum_{i\geq 0} a_i T^{-i} \in \mathbb{F}_q[[T^{-1}]]$ be an irrational algebraic Laurent series over $\mathbb{F}_q(T)$. Let k, l, ω, s be the parameters of $f_{\mathbf{a}}$ defined above. Then the irrationality exponent $\mu(f_{\mathbf{a}})$ satisfies

(7)
$$\frac{k+\omega\ell}{k+\ell} \le \mu(f_{\mathbf{a}}) \le \frac{p^{s+1}(k+\ell)}{(\omega-1)\ell}.$$

REMARK 3.8. If, for every n, **a** and \mathbf{c}_n have the same first $(k + \omega \ell)p^n$ digits, while their $((k + \omega \ell)p^n + 1)$ th digits are different, then

$$\left| f_{\mathbf{a}} - \frac{P_n}{Q_n} \right| = \frac{c_2}{|Q_n|^{1+\delta}}$$

Thus, inequality (7) does not depend on s (the cardinality of the p-kernel) anymore. More precisely, in this case, P_n and Q_n satisfy Lemma 3.2 with $\theta = p, \rho = \delta = (\omega - 1)\ell/(k + \ell)$ and we have

$$\frac{k+\omega\ell}{k+\ell} \le \mu(f_{\mathbf{a}}) \le \frac{p(k+\omega\ell)}{(\omega-1)\ell}.$$

Moreover, if there exists N such that $(P_n, Q_n) = 1$ for any $n \ge N$, then

$$\frac{k+\omega\ell}{k+\ell} \le \mu(f_{\mathbf{a}}) \le \max\left(\frac{k+\omega\ell}{k+\ell}, 1+\frac{p(k+\ell)}{(\omega-1)\ell}\right).$$

If $U = \varepsilon$, that is, k = 0, then

$$\omega \le \mu(f_{\mathbf{a}}) \le p \frac{\omega}{\omega - 1}.$$

(Notice that this inequality makes sense because $\omega ; otherwise, the infinite sequence$ **a** $would be periodic and <math>f_{\mathbf{a}}$ rational.) Furthermore, if $\omega - 1 \ge \sqrt{p}$ and $(P_n, Q_n) = 1$, then $\mu(f_{\mathbf{a}}) = \omega$. All this explains why, in many cases, the general upper bound we obtained in Theorem 1.2 can be significantly improved.

Proof of Theorem 1.2. By construction, $\omega = 1 + 1/\ell$ and $k + \ell \leq e$. By Theorem 3.7, it follows immediately that $\mu(f_{\mathbf{a}}) \leq p^{s+1}e$.

3.4. An equivalent condition for coprimality of P_n and Q_n . We have seen in Remark 3.8 that, in the case where the numerator P_n and the denominator Q_n of our rational approximations are relatively prime, the bound for the irrationality exponent obtained in Theorem 1.2 can be significantly improved. This serves as a motivation for this section, which is devoted to the coprimality of P_n and Q_n .

First, let us recall the following result, which is an easy consequence of the fact that the greatest common divisor of two polynomials, defined over a field \mathbb{K} , also belongs to \mathbb{K} .

LEMMA 3.9. Let $P, Q \in \mathbb{F}_q[T]$. Then (P, Q) = 1 over $\mathbb{F}_q[T]$ if and only if (P, Q) = 1 over $\overline{\mathbb{F}}_p[T]$.

We recall that $\overline{\mathbb{F}}_p$ is the classical notation for an algebraic closure of \mathbb{F}_p .

Let $k > 0, n \in \mathbb{N}^*$ and $Q_n(T) = T^{kp^n-1}(T^{\ell p^n}-1) \in \mathbb{F}_q[T]$. Since we work in characteristic p, we have

$$Q_n(T) = T^{kp^n - 1} (T^{\ell} - 1)^{p^n}.$$

Now, let P be an arbitrary polynomial with coefficients in \mathbb{F}_q . Then $(P, Q_n) = 1$ if and only if (P(T), T) = 1 and $(P(T), T^{\ell} - 1) = 1$. In other words, $(P, Q_n) = 1$ if and only if $P(0) \neq 0$ and $P(a) \neq 0$ for all $a \in \overline{\mathbb{F}}_p$ such that $a^{\ell} = 1$.

Therefore, we easily obtain the following lemma, which will simplify the study of the coprimality of polynomials P_n and Q_n , by using some properties of P_{U_n} and P_{V_n} . (We recall that $U_n = \varphi(\sigma^n(U))$ and $V_n = \varphi(\sigma^n(V))$, where U and V are introduced in Section 3.3.)

LEMMA 3.10. Let $n \in \mathbb{N}^*$ and P_n , Q_n defined in (5) and (4). Then $(P_n, Q_n) = 1$ over $\mathbb{F}_q(T)$ if and only if

- (i) $P_{U_n}(0) \neq P_{V_n}(0)$,
- (ii) for any $a \in \overline{\mathbb{F}}_p^n$ such that $a^{\ell} = 1$, $P_{V_n}(a) \neq 0$.

REMARK 3.11. If k = 0, then $Q_n = T^{\ell p^n} - 1 = (T^{\ell} - 1)^{p^n}$. In this case, $(P_n, Q_n) = 1$ over $\mathbb{F}_q(T)$ if and only if for any $a \in \overline{\mathbb{F}}_p$ such that $a^{\ell} = 1$, $P_{V_n}(a) \neq 0$.

4. Matrices associated with morphisms. The purpose of this section is to give an approach which will allow one to compute the polynomials $P_{U_n}(T)$ and $P_{V_n}(T)$, described in the previous section. In particular, we show that, if $\alpha \in \overline{\mathbb{F}}_p$, the sequences $(P_{U_n}(\alpha))_{n\geq 1}$ and $(P_{V_n}(\alpha))_{n\geq 1}$ are ultimately periodic. Lemma 3.10 implies that we have to test the coprimality of P_n and Q_n only for a finite number of indices n.

Let $U = a_0 a_1 \cdots a_{k-1}$ be a finite word on \mathcal{A}_m and let $i \in \mathcal{A}_m$. We let $\mathcal{P}_U(i)$ denote the set of positions of i in the word \overline{U} ; we write simply \mathcal{P}_i if there is no doubt about U.

DEFINITION 4.1. We associate with U the row vector $v_U(T) = (\beta_{U,j}(T))_{0 \le j \le m-1}$ with coefficients in $\mathbb{F}_p[T]$ where, for any $j \in \mathcal{A}_m$, $\beta_{U,j}$ is defined by

(8)
$$\beta_{U,j}(T) = \begin{cases} \sum_{l \in \mathcal{P}_j} T^l & \text{if } j \text{ occurs in } U, \\ 0 & \text{otherwise.} \end{cases}$$

EXAMPLE 4.2. Consider $U = 1020310 \in \mathcal{A}_5^*$. Then $\mathcal{P}_0 = \{0, 3, 5\}, \mathcal{P}_1 = \{1, 6\}, \mathcal{P}_2 = \{4\}, \mathcal{P}_3 = \{2\}$ and $\mathcal{P}_4 = \emptyset$. The vector associated with U is

$$v_U(T) = (1 + T^3 + T^5, T + T^6, T^4, T^2, 0).$$

We also recall that $P_U(T) = T^6 + 2T^4 + 3T^2 + T$ (see Definition 3.3) and we observe that

$$P_U(T) = v_U(T) \begin{pmatrix} 0\\1\\2\\3\\4 \end{pmatrix}.$$

DEFINITION 4.3. Let $\sigma : \mathcal{A}_m \to \mathcal{A}_m^*$ be a morphism. We associate with σ the $m \times m$ matrix $M_{\sigma}(T)$ with coefficients in $\mathbb{F}_p[T]$ defined by

$$M_{\sigma}(T) = (\beta_{\sigma(i),j}(T))_{0 \le i,j \le m-1}$$

EXAMPLE 4.4. Let $\sigma : \mathcal{A}_3 \to \mathcal{A}_3^*$, $\sigma(0) = 010$, $\sigma(1) = 2101$ and $\sigma(2) = 00211$. Then

$$M_{\sigma}(T) = \begin{pmatrix} T^2 + 1 & T & 0 \\ T & T^2 + 1 & T^3 \\ T^4 + T^3 & T + 1 & T^2 \end{pmatrix}.$$

It is not difficult to see that such matrices have some interesting general properties as claimed in the following remarks.

REMARK 4.5. The matrix $M_{\sigma}(1)$ is the reduction modulo p of the socalled incidence matrix associated with the morphism σ . This matrix has some nice properties and has been the subject of extensive studies (see for instance [18]).

REMARK 4.6. If σ_1 and σ_2 are two *p*-morphisms over \mathcal{A}_m then

$$M_{\sigma_1 \circ \sigma_2}(T) = M_{\sigma_2}(T^p) M_{\sigma_1}(T).$$

Now, our main goal is to prove that, if $\alpha \in \overline{\mathbb{F}}_p$, the sequences $(P_{U_n}(\alpha))_{n\geq 1}$ and $(P_{V_n}(\alpha))_{n\geq 1}$ are ultimately periodic. This will be the subject of Proposition 4.14. In order to prove it, we will need the following auxiliary results.

LEMMA 4.7. Let $\sigma : \mathcal{A}_m \to \mathcal{A}_m^*$ be a p-morphism and $U = a_0 \cdots a_{k-1} \in \mathcal{A}_m^*$. For any $n \in \mathbb{N}$ we denote $U_n = \sigma^n(U) = \sigma^n(a_0) \cdots \sigma^n(a_{k-1})$. Then

$$P_{U_n}(T) = v_U(T^{p^n})R_n(T),$$

where, for any $n \in \mathbb{N}$,

$$R_n(T) = \begin{pmatrix} P_{\sigma^n(0)}(T) \\ P_{\sigma^n(1)}(T) \\ \vdots \\ P_{\sigma^n(m-1)}(T) \end{pmatrix}.$$

310

Proof. Since $U_n = \sigma^n(a_0) \cdots \sigma^n(a_{k-1})$ and σ is a *p*-morphism, we infer that

$$P_{\sigma^n(U)}(T) = P_{\sigma^n(a_0)}(T)T^{(k-1)p^n} + P_{\sigma^n(a_1)}(T)T^{(k-2)p^n} + \dots + P_{\sigma^n(a_{k-1})}(T).$$

Hence there exists a vector $S_n(T) = (s_0(T^{p^n}), s_1(T^{p^n}), \ldots, s_{m-1}(T^{p^n}))$, where $s_i(T), 0 \le i \le m-1$, are some polynomials with coefficients 0 or 1, such that

$$P_{\sigma^n(U)}(T) = S_n(T) \begin{pmatrix} P_{\sigma^n(0)}(T) \\ P_{\sigma^n(1)}(T) \\ \vdots \\ P_{\sigma^n(m-1)}(T) \end{pmatrix}$$

and $S_n(T) = S_0(T^{p^n})$. For n = 0, the equality above becomes

$$P_U(T) = S_0(T) \begin{pmatrix} 0 \\ 1 \\ \vdots \\ m-1 \end{pmatrix}.$$

By Definitions 4.1 and 3.3, we deduce that $S_0(T) = v_U(T)$. This ends the proof.

LEMMA 4.8. Let $n \in \mathbb{N}$ and let σ be a p-morphism over \mathcal{A}_m . Then

$$R_{n+1}(T) = M_{\sigma}(T^{p^n})R_n(T),$$

where $M_{\sigma}(T)$ is the matrix associated with σ as in Definition 4.3.

Proof. Let σ be defined as follows:

$$\begin{cases} \sigma(0) = a_0^{(0)} a_1^{(0)} \cdots a_{p-1}^{(0)}, \\ \sigma(1) = a_0^{(1)} a_1^{(1)} \cdots a_{p-1}^{(1)}, \\ \vdots \\ \sigma(m-1) = a_0^{(m-1)} a_1^{(m-1)} \cdots a_{p-1}^{(m-1)}, \end{cases}$$

where $a_i^{(j)} \in \mathcal{A}_m$ for any $i \in \{0, 1, \dots, p-1\}$ and $j \in \{0, 1, \dots, m-1\}$. Then, for any $j \in \{0, 1, \dots, m-1\}$ and $n \in \mathbb{N}^*$, we have

$$\sigma^{n+1}(j) = \sigma^n(\sigma(j)) = \sigma^n(a_0^{(j)}a_1^{(j)}\cdots a_{p-1}^{(j)}) = \sigma^n(a_0^{(j)})\sigma^n(a_1^{(j)})\cdots \sigma^n(a_{p-1}^{(j)}).$$

Hence

$$P_{\sigma^{n+1}(j)}(T) = P_{\sigma^n(a_0^{(j)})}(T)T^{(p-1)p^n} + \dots + P_{\sigma^n(a_{p-1}^j)}(T).$$

It follows by Lemma 4.7 that

$$\begin{pmatrix} P_{\sigma^{n+1}(0)}(T) \\ P_{\sigma^{n+1}(1)}(T) \\ \vdots \\ P_{\sigma^{n+1}(m-1)}(T) \end{pmatrix} = (\beta_{\sigma(i),j}(T^{p^n}))_{0 \le i,j \le m-1} \begin{pmatrix} P_{\sigma^n(0)}(T) \\ P_{\sigma^n(1)}(T) \\ \vdots \\ P_{\sigma^n(m-1)}(T) \end{pmatrix},$$

that is, $R_{n+1}(T) = M_{\sigma}(T^{p^n})R_n(T)$.

REMARK 4.9. In particular, if n = 0 in the previous lemma, we obtain

$$\begin{pmatrix} P_{\sigma(0)}(T) \\ P_{\sigma(1)}(T) \\ \vdots \\ P_{\sigma(m-1)}(T) \end{pmatrix} = (\beta_{\sigma(i),j}(T))_{0 \le i,j \le m-1} \begin{pmatrix} 0 \\ 1 \\ \vdots \\ m-1 \end{pmatrix} = M_{\sigma}(T)R_0(T)$$

for any *p*-morphism σ defined over \mathcal{A}_m .

Notice also that, if φ is a coding defined over \mathcal{A}_m , we have a similar identity

$$\begin{pmatrix} P_{\varphi(\sigma(0))}(T) \\ P_{\varphi(\sigma(1))}(T) \\ \vdots \\ P_{\varphi(\sigma(m-1))}(T) \end{pmatrix} = (\beta_{\varphi(\sigma(i)),j}(T))_{0 \le i,j \le m-1} \begin{pmatrix} \varphi(0) \\ \varphi(1) \\ \vdots \\ \varphi(m-1) \end{pmatrix}$$

The following corollaries are immediate.

COROLLARY 4.10. Let $n \in \mathbb{N}^*$ and let σ be a p-morphism defined on \mathcal{A}_m . Then

$$R_n(T) = M_{\sigma}(T^{p^{n-1}})M_{\sigma}(T^{p^{n-2}})\cdots M_{\sigma}(T) \begin{pmatrix} 0\\ 1\\ \vdots\\ m-1 \end{pmatrix},$$

where $M_{\sigma}(T)$ is the matrix associated with σ as in Definition 4.3.

COROLLARY 4.11. Let σ be a p-morphism defined on \mathcal{A}_m . Then for any $n \in \mathbb{N}^*$,

$$M_{\sigma^n}(T) = M_{\sigma}(T^{p^{n-1}})M_{\sigma}(T^{p^{n-2}})\cdots M_{\sigma}(T)$$

where $M_{\sigma}(T)$ is the matrix associated with σ as in Definition 4.3.

COROLLARY 4.12. Let $a \in \mathbb{F}_p$. Then $M_{\sigma^n}(a) = M_{\sigma}^n(a)$ for any $n \in \mathbb{N}$.

PROPOSITION 4.13. Let p be a prime, q a power of p, and $\sigma : \mathcal{A}_m \to \mathcal{A}_m^*$ a p-morphism. Let $\alpha \in \mathbb{F}_r$, where $r = p^t$, $t \in \mathbb{N}^*$. Then for any positive integer k we have

(9)
$$M_{\sigma^{kt}}(\alpha) = (M_{\sigma^t}(\alpha))^k.$$

Proof. We argue by induction on k. Obviously, this is true for k = 1. We suppose that (9) is satisfied for k and we prove it for k + 1. Using Corollary 4.11 and the fact that $\alpha^r = \alpha$ we obtain

$$M_{\sigma^{(k+1)t}}(\alpha) = \underbrace{M_{\sigma}(\alpha^{p^{kt+t-1}})\cdots M_{\sigma}(\alpha^{p^{t}})}_{= M_{\sigma}(\alpha^{p^{kt-1}})\cdots M_{\sigma}(\alpha)} \underbrace{M_{\sigma}(\alpha^{p^{t-1}})\cdots M_{\sigma}(\alpha)}_{= M_{\sigma^{kt}}(\alpha)M_{\sigma^{t}}(\alpha) = (M_{\sigma^{t}}(\alpha))^{k+1}. \bullet$$

PROPOSITION 4.14. Let p be a prime, q a power of p and $U = a_{k-1} \cdots a_0 \in \mathcal{A}_m^*$. Let $\sigma : \mathcal{A}_m \to \mathcal{A}_m^*$ be a p-morphism and $\varphi : \mathcal{A}_m \to \mathbb{F}_q$ a coding. Let $\alpha \in \mathbb{F}_r$, where $r = p^t$, $r \in \mathbb{N}^*$. Then the sequence $(P_{\varphi(\sigma^n(U))}(\alpha))_{n\geq 0}$ is ultimately periodic.

Proof. First, notice that, as in Lemma 4.7, we have

$$P_{\varphi(\sigma^{n}(U))}(T) = v_{U}(T^{p^{n}}) \begin{pmatrix} P_{\varphi(\sigma^{n}(0))}(T) \\ P_{\varphi(\sigma^{n}(1))}(T) \\ \vdots \\ P_{\varphi(\sigma^{n}(m-1))}(T) \end{pmatrix}$$

By Remark 4.9, we have

$$\begin{pmatrix} P_{\varphi(\sigma^{n}(0))}(T) \\ P_{\varphi(\sigma^{n}(1))}(T) \\ \vdots \\ P_{\varphi(\sigma^{n}(m-1))}(T) \end{pmatrix} = M_{\sigma^{n}}(T) \begin{pmatrix} \varphi(0) \\ \varphi(1) \\ \vdots \\ \varphi(m-1) \end{pmatrix}$$

Hence

$$P_{\varphi(\sigma^{n}(U)}(\alpha) = v_{U}(\alpha^{p^{n}})M_{\sigma^{n}}(\alpha) \begin{pmatrix} \varphi(0) \\ \varphi(1) \\ \vdots \\ \varphi(m-1) \end{pmatrix}$$

Clearly, the sequence $(v_U(\alpha^{p^n}))_{n\geq 0}$ is periodic with period less than or equal to t since $v_U(\alpha^{p^{n+t}}) = v_U(\alpha^{p^n})$ for any $n \in \mathbb{N}^*$. We now prove that the sequence $(M_{\sigma^n}(\alpha))_{n\geq 0}$ is ultimately periodic.

Since $\alpha \in \mathbb{F}_{p^t}$, we have $\alpha^{p^t} = \alpha$ and thus, by Corollary 4.11, for any k and $n \in \mathbb{N}$,

$$M_{\sigma^{n+kt}}(\alpha) = M_{\sigma^n}(\alpha)M_{\sigma^{kt}}(\alpha)$$

Therefore, by Proposition 4.13 we have, for any $k \in \mathbb{N}$,

$$M_{\sigma^{n+kt}}(\alpha) = M_{\sigma^n}(\alpha)M_{\sigma^{kt}}(\alpha) = M_{\sigma^n}(\alpha)(M_{\sigma^t}(\alpha))^k.$$

Since $M_{\sigma^t}(\alpha)$ is an $m \times m$ matrix with coefficients in a finite field, there exist distinct positive integers m_0 and n_0 (suppose that $m_0 < n_0$) such that $M_{\sigma^t}(\alpha)^{m_0} = M_{\sigma^t}(\alpha)^{n_0}$. This implies that

$$M_{\sigma^{n+m_0t}}(\alpha) = M_{\sigma^n}(\alpha)(M_{\sigma^t}(\alpha))^{m_0} = M_{\sigma^n}(\alpha)(M_{\sigma^t}(\alpha))^{n_0} = M_{\sigma^{n+n_0t}}(\alpha),$$

and thus the sequence $(M_{\sigma^n}(\alpha))_{n\geq 0}$ is ultimately periodic, with pre-period at most $m_0 t$ and period at most $(n_0 - m_0)t$. Since $(v_U(\alpha^{p^n}))_{n\geq 0}$ is periodic with period at most t, it follows that $(P_{\varphi(\sigma^n(U))}(\alpha))_{n\geq 0}$ is ultimately periodic (with pre-period at most $m_0 t$ and period at most $(n_0 - m_0)t^2$). This ends the proof. \blacksquare

REMARK 4.15. All the properties (we have proved here) of the matrices associated with morphisms are still true on replacing *p*-morphisms by p^r morphisms for any $r \in \mathbb{N}^*$, because, in general, the key point is that the map $x \mapsto x^{p^r}$ is a morphism (the *r*th power of the Frobenius morphism). Thus, it only suffices to replace T^p by T^{p^r} in our results proved before.

5. Examples. In Theorem 1.2 we give a general upper bound for the irrationality exponent of algebraic Laurent series with coefficients in a finite field. In many cases, the sequence of rational approximations $(P_n/Q_n)_{n\geq 0}$ we construct turns out to satisfy the conditions (i) and (ii) of Lemma 3.10. This naturally gives rise to a much better estimate, as hinted in Remark 3.8. In this section, we illustrate this claim with a few examples of algebraic Laurent series for which the irrationality exponent is exactly computed or at least well estimated.

EXAMPLE 5.1. Let us consider the following equation over $\mathbb{F}_2(T)$:

(10)
$$X^4 + X + \frac{T}{T^4 + 1} = 0.$$

This equation is related to the Mahler algebraic Laurent series, previously mentioned. Let $E_1 = \{ \alpha \in \mathbb{F}_2((T^{-1})) : |\alpha| < 1 \}$. We first notice that (10) has a unique solution f in E_1 . This can be obtained by showing that the map

$$h: E_1 \to E_1, \quad X \mapsto X^4 + \frac{T}{T^4 + 1},$$

is well defined and is a contracting map from E_1 to E_1 . Then the fixed point theorem in a complete metric space implies that the equation h(X) = X,

314

which is equivalent to (10), has a unique solution in E_1 . Let $f(T) := \sum_{i\geq 0} a_i T^{-i}$ denote this solution (with $a_i = 0$, since f belongs to E_1).

The second step is to find the morphisms that generate the sequence of coefficients of f, as in Cobham's theorem. Notice that there is a general method that allows one to obtain these morphisms when we know the algebraic equation. In this example, we try to describe the important steps of this method; we will give further details later.

By inserting f in (10) and using the fact that $f^4(T) = \sum_{i\geq 0} a_i T^{-4i}$ we easily obtain the following relations between the coefficients of f:

- (11) $a_{i+1} + a_i + a_{4i+4} + a_{4i} = 0,$
- (12) $a_1 = 0, \quad a_2 = 0, \quad a_3 = 1,$
- (13) $a_{i+4} + a_i = 0 \quad \text{if } i \neq 0 \quad [4].$

From (12) and (13), we get $a_{4i+1} = 0$, $a_{4i+2} = 0$ and $a_{4i+3} = 1$, for any $i \ge 0$. From (11) we deduce that

$$a_{16i+4} = a_{16i+8} = a_{16i} + a_{4i},$$

$$a_{16i+12} = a_{16i+8} + 1 = a_{16i} + a_{4i} + 1.$$

This implies that the 4-kernel of $\mathbf{a} := (a_i)_{i \ge 0}$ is

$$K_4(\mathbf{a}) = \{(a_i)_{i \ge 0}, (a_{4i})_{i \ge 0}, (a_{16i})_{i \ge 0}, (0), (1)\}.$$

Consequently, the 4-automaton generating **a** is as in Fig. 2.

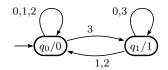


Fig. 2. A 4-automaton recognizing a

Once we have the automaton, there is a general approach to obtain the morphisms that generate an automatic sequence. More precisely, the proof of Cobham's theorem precisely describes this process. The reader may consult the original article of Cobham [7] or the monograph [4, Theorem 6.3.2, p. 175]. Following this approach, we find that $\mathbf{a} = \sigma^{\infty}(0)$, where σ is defined by

$$\sigma(0) = 0001, \quad \sigma(1) = 1001.$$

It is now possible to apply our approach described in the first part of the paper. We will prove the following result, stated as Theorem 1.3 in the Introduction:

$$\mu(f) = 3.$$

Notice that Mahler's theorem implies only that $\mu(f) \leq 4$, and Osgood's Theorem or Lasjaunias and de Mathan's Theorem cannot be applied since this Laurent series is clearly hyperquadratic.

Proof. We are going to introduce an infinite sequence $(P_n/Q_n)_{n\geq 1}$ of rational fractions converging to f. Since **a** begins with 0001, we denote V = 0 and $V_n = \sigma^n(V)$ for any $n \geq 1$. Hence **a** begins with $V_n V_n V_n$ for any non-negative integer n.

Since $|V_n| = 4^n$, we set $Q_n(T) = T^{4^n} - 1$. In Section 3.3, we showed that there exists a polynomial $P_n(T) \in \mathbb{F}_2[T]$ such that

$$P_n(T)/Q_n(T) = f_{V_n^{\infty}}(T).$$

The Laurent series expansion of P_n/Q_n begins with

 $\sigma^n(0001)\sigma^n(0001)\sigma^n(0001)\sigma^n(0),$

and we deduce that it begins with

 $\sigma^n(0001)\sigma^n(0001)\sigma^n(0001)0,$

while the sequence \mathbf{a} begins with

 $\sigma^n(0001)\sigma^n(0001)\sigma^n(0001)1.$

Hence, the first $3 \cdot 4^n$ digits of the Laurent series expansions of P_n/Q_n and of f are the same, while the following coefficients are different. Using the notations from Theorem 3.7 and Remark 3.8, we have k = 0, $\ell = 4$, $\omega = 3$ and p = 4.

According to Remark 3.8, we deduce that

$$3 \le \mu(f) \le 6,$$

and if $(P_n, Q_n) = 1$ for any $n \ge 1$, then

$$\mu(f) = 3.$$

It thus remains to prove that $(P_n, Q_n) = 1$ for every positive integer n. Let $n \ge 1$. By Lemma 3.10 we have to prove that $P_n(1) \ne 0$, i.e., $P_{\sigma^n(0)}(1) \ne 0$. Remark 4.9 implies that

$$\binom{P_{\sigma^n(0)}(T)}{P_{\sigma^n(1)}(T)} = M_{\sigma^n}(T) \binom{0}{1}.$$

Hence, $P_{\sigma^n(0)}(1) \neq 0$ if and only if

$$(1 \ 0)M_{\sigma^n}(1) \begin{pmatrix} 0\\1 \end{pmatrix} \neq 0,$$

that is, if and only if

$$(1 \ 0)M_{\sigma}^{n}(1) \begin{pmatrix} 0\\ 1 \end{pmatrix} \neq 0.$$

Indeed, by Corollary 4.12, we have $M_{\sigma^n}(1) = M_{\sigma}^n(1)$. Since

$$M_{\sigma}(1) = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix},$$

we deduce that $M_{\sigma^n}(1) = M_{\sigma}(1)$ and so

$$(1 \ 0) \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \neq 0.$$

Consequently, $(P_n, Q_n) = 1$. This ends the proof.

REMARK 5.2. Let $f(T) = \sum_{i>0} a_i T^{-i}$ be a Laurent series with coefficients in a finite field \mathbb{F}_q , where \overline{q} is a power of p, and suppose that there is $P(T) \in \mathbb{F}_q[T]$ such that P(f) = 0. As mentioned before, there is a general approach that allows one to find the automaton that generates the infinite sequence $\mathbf{a} := (a_i)_{i \geq 0}$. This consists of the following steps. First, there exists a polynomial Q with coefficients in \mathbb{F}_q , of the form $Q(X) = \sum_{i>0} B_i(T) X^{p^i}$ with $B_0(T) \neq 0$ such that Q(f) = 0. This is known as Ore's polynomial and its existence is due to Ore's theorem (for a proof see, for example, [4, Lemma 12.2.3, p. 355]. Hence, the first step is to find such an Ore polynomial vanishing at f (this is possible by raising P to the power of p as many times as we need). The second step is to find some recurrent relations between the terms a_i in order to find the kernel of **a**. This is possible thanks to the Frobenius morphism. The third step is the construction of the automaton generating **a**. Notice that a sequence is *p*-automatic if and only if its *p*-kernel is finite. The proof of this well-known result is explicit and we refer the reader to [4, Theorem 6.6.2, p. 18]. The last step is to find the morphisms generating \mathbf{a} , as described in Cobham's theorem. In order to do this, the reader may refer to the proof of Cobham's theorem, which is explicit as well.

The following examples present different computations of irrationality exponents of Laurent power series over finite fields. We do not give the relevant algebraic equations because the computation is quite long, but, as in the previous example (where we find the morphisms if we know the equation), there is a general approach that allows one to compute the equation of a Laurent series when we know the automaton generating the sequence of its coefficients. Indeed, by knowing the morphisms we can find the automaton (see the proof of Cobham's theorem), and knowing the automaton allows finding the kernel (see [4, Theorem 6.6.2, p. 185]) and the relations between the coefficients. These relations allow one to find a polynomial that vanishes at the given Laurent series (the reader may consult the proof of Christol's theorem in [6] or [4, p. 356], and also [11] where a generalisation of Christol's theorem is given). More precisely the polynomial that we compute from these A. Firicel

relations is also an Ore polynomial. Finally, we have to factor this polynomial and to check which irreducible factor vanishes at our algebraic Laurent series.

EXAMPLE 5.3. We now consider the Laurent series

$$f_{\mathbf{a}}(T) = \sum_{i \ge 0} a_i T^{-i} \in \mathbb{F}_2[[T^{-1}]],$$

where the sequence $\mathbf{a} := (a_i)_{i \ge 0}$ is the image under the coding φ of the fixed point of the 8-uniform morphism σ , φ and σ being defined as follows:

$$\begin{split} \varphi(0) &= 1, \quad \sigma(0) = 00000122, \\ \varphi(1) &= 0, \quad \sigma(1) = 10120011, \\ \varphi(2) &= 1, \quad \sigma(2) = 12120021. \end{split}$$

Thus $\mathbf{a} = 11111011111...$

PROPOSITION 5.4. One has $\mu(f_{\mathbf{a}}) = 5$.

Proof. Using the notations from Theorem 3.7 and Remark 3.8, we have $k = 0, \ell = 1, \omega = 5$ and p = 8 (since σ is an 8-uniform morphism). By applying the same method as for the previous example, we can easily prove the proposition.

EXAMPLE 5.5. We now consider the Laurent series

$$f_{\mathbf{a}}(T) = \sum_{i \ge 0} a_i T^{-i} \in \mathbb{F}_3[[T^{-1}]],$$

where the sequence $\mathbf{a} := (a_i)_{i \ge 0}$ is the fixed point beginning with zero of the following 3-uniform morphism:

$$\sigma(0) = 010, \quad \sigma(1) = 102, \quad \sigma(2) = 122.$$

Thus $\mathbf{a} = 010102010...$

PROPOSITION 5.6. The irrationality exponent of $f_{\mathbf{a}}$ satisfies

$$8/3 \le \mu(f_{\mathbf{a}}) \le 14/5.$$

In this case, we are not able to compute the exact value of the irrationality exponent but the lower bound we found shows that the degree of $f_{\mathbf{a}}$ is greater than or equal to 3. Hence our upper bound obviously improves on the one that could be deduced from Liouville–Mahler's theorem.

Proof of Proposition 5.6. We are going to introduce an infinite sequence $(P_n/Q_n)_{n\geq 0}$ of rational fractions converging to $f_{\mathbf{a}}$. Since **a** begins with 010102, we denote V := 010102 and for any $n \geq 1$, $V_n := \sigma^n(V)$. Hence **a** begins with

$$\sigma^n(010102)\sigma^n(010102)\sigma^n(0101)$$

for any $n \ge 1$. Now, we set $Q_n(T) = T^{2 \cdot 3^n} - 1$. There exists a polynomial $P_n(T) \in \mathbb{F}_3[T]$ such that

$$P_n(T)/Q_n(T) = f_{V_n^{\infty}}(T).$$

The Laurent series expansion of P_n/Q_n begins with

$$\sigma^n(010102)\sigma^n(010102)\sigma^n(0101)\sigma^n(0)$$

and so with

$$\sigma^n(010102)\sigma^n(010102)\sigma^n(0101)0$$

while the sequence \mathbf{a} begins with

 $\sigma^n(010102)\sigma^n(010102)\sigma^n(0101)1.$

Hence, the first $16 \cdot 3^n$ digits of the Laurent series expansions of P_n/Q_n and $f_{\mathbf{a}}$ are the same, while the following coefficients are different. Using the notations from Theorem 3.7 and Remark 3.8, we have k = 0, $\ell = 6$, $\omega = 8/2$ and p = 3.

By Remark 3.8, we deduce that

$$8/3 \le \mu(f_{\mathbf{a}}) \le 24/5.$$

Furthermore, if $(P_n, Q_n) = 1$ for every $n \ge 1$, then

 $8/3 \le \mu(f_{\mathbf{a}}) \le 14/5.$

Let $n \ge 1$. We now prove that $(P_n, Q_n) = 1$. By Lemma 3.10, since

$$Q_n(T) = (T-1)^{3^n} (T+1)^{3^n},$$

we have to prove that, for all $n \ge 1$, $P_n(1) \ne 0$ and $P_n(-1) \ne 0$.

By definition of $(P_n(T))_{n>0}$ (see (5)) we have

$$P_n(1) = P_{V_n}(1)$$
 and $P_n(-1) = P_{V_n}(-1).$

Since $V_n = \sigma^n(010102) = \sigma^{n+1}(01)$, we have

$$P_{V_n}(T) = P_{\sigma^{n+1}(0)}(T)T^{3^{n+1}} + P_{\sigma^{n+1}(1)}(T).$$

Hence,

$$P_{V_n}(1) = P_{\sigma^{n+1}(0)}(1) + P_{\sigma^{n+1}(1)}(1),$$

$$P_{V_n}(-1) = -P_{\sigma^{n+1}(0)}(-1) + P_{\sigma^{n+1}(1)}(-1).$$

Remark 4.9 implies that

$$\begin{pmatrix} P_{\sigma^n(0)}(T) \\ P_{\sigma^n(1)}(T) \\ P_{\sigma^n(2)}(T) \end{pmatrix} = M_{\sigma^n}(T) \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix}.$$

If we now set T = 1 (respectively T = -1), we find that $P_n(1) \neq 0$ (respectively $P_n(-1) \neq 0$) if and only if

$$(1 \quad 1 \quad 0)M_{\sigma}^{n}(1) \begin{pmatrix} 0\\1\\2 \end{pmatrix} \neq 0,$$

respectively,

$$(-1 \ 1 \ 0)M_{\sigma}^{n}(-1) \begin{pmatrix} 0\\ 1\\ 2 \end{pmatrix} \neq 0.$$

The matrix associated with σ is

$$M_{\sigma}(T) = \begin{pmatrix} T^2 + 1 & T & 0 \\ T & T^2 & 1 \\ 0 & T^2 & T + 1 \end{pmatrix}.$$

Hence,

$$M_{\sigma}(1) = \begin{pmatrix} 2 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 2 \end{pmatrix} \quad \text{and} \quad M_{\sigma}(-1) = \begin{pmatrix} 2 & -1 & 0 \\ -1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Notice that $M_{\sigma}^2(\pm 1) = M_{\sigma}^4(\pm 1)$, and an easy computation shows that $(P_{V_n}(1))_{n\geq 0}$ is 2-periodic and $(P_{V_n}(-1))_{n\geq 0}$ is 1-periodic; more precisely, $(P_{V_n}(1))_{n\geq 0} = (12)^{\infty}$ and $(P_{V_n}(-1))_{n\geq 0} = (1)^{\infty}$. This proves that $P_{V_n}(1)$ and $P_{V_n}(-1)$ never vanish, which ends the proof.

EXAMPLE 5.7. We now consider the Laurent series

$$f_{\mathbf{a}}(T) = \sum_{i \ge 0} a_i T^{-i} \in \mathbb{F}_5[[T^{-1}]],$$

where the sequence $\mathbf{a} := (a_i)_{i \ge 0}$ is the fixed point beginning with zero of the following 5-uniform morphism:

$$\sigma(0) = 00043, \quad \sigma(1) = 13042, \quad \sigma(2) = 14201,$$

 $\sigma(3) = 32411, \quad \sigma(4) = 00144.$

Thus $\mathbf{a} = 0004300043...$

PROPOSITION 5.8. One has

$$\mu(f_{\mathbf{a}}) = 17/5.$$

Notice that, by Mahler's theorem, the degree of algebraicity of $f_{\mathbf{a}}$ is greater than or equal than 4.

320

Proof. Using the notations from Theorem 3.7 and Remark 3.8, we have $k = 0, \ell = 5, \omega = 17/5$ and p = 5. By applying the same method as for the previous examples, we can easily prove the proposition.

References

- B. Adamczewski et Y. Bugeaud, Nombres réels de complexité sous-linéaire : mesures d'irrationalité et de transcendance, J. Reine Angew. Math. 658 (2011), 65–98.
- [2] B. Adamczewski and J. Cassaigne, Diophantine properties of real numbers generated by finite automata, Compos. Math. 142 (2006), 1351–1372.
- [3] B. Adamczewski and T. Rivoal, Irrationality measures for some automatic reals numbers, Math. Proc. Cambridge Philos. Soc. 147 (2009), 659–678.
- [4] J.-P. Allouche and J. Shallit, Automatic Sequences: Theory, Applications, Generalizations, Cambridge Univ. Press, Cambridge, 2003.
- [5] L. Baum and M. Sweet, Continued fractions of algebraic power series in characteristic 2, Ann. of Math. 103 (1976), 593–610.
- [6] G. Christol, Ensembles presque périodiques k-reconnaissables, Theoret. Comput. Sci. 9 (1979), 141–145.
- [7] A. Cobham, Uniform tag sequences, Math. Systems Theory 6 (1972), 164–192.
- [8] F. J. Dyson, The approximation to algebraic numbers by rationals, Acta Math. 79 (1947), 225–240.
- [9] S. Eilenberg, Automata, Languages and Machines, Vol. A, Academic Press, New York, 1974.
- [10] B. P. Gill, An analogue for algebraic functions of the Thue-Siegel theorem, Ann. of Math. 31 (1930), 207–218.
- K. Kedlaya, The algebraic closure of the power series field in positive characteristic, Proc. Amer. Math. Soc. 129 (2001), 3461–3470.
- [12] A. Lasjaunias, A survey of Diophantine approximation in fields of power series, Monatsh. Math. 130 (2000), 211–229.
- [13] A. Lasjaunias and B. de Mathan, *Thue's theorem in positive characteristic*, J. Reine Angew. Math. 473 (1996), 195–206.
- K. Mahler, On a theorem of Liouville in fields of positive characteristic, Canad. J. Math. 1 (1949), 397–400.
- [15] E. Maillet, Introduction à la théorie des nombres transcendants et des propriétés arithmétiques des fonctions, Gauthier-Villars, Paris, 1906.
- [16] C. Osgood, An effective lower bound on the "Diophantine approximation" of algebraic functions by rational functions, Mathematika 20 (1973), 4–15.
- [17] C. Osgood, Effective bounds on the "Diophantine approximation" of algebraic functions over fields of arbitrary characteristic and applications to differential equations, Nederl. Akad. Wetensch. Proc. Ser. A 78 (1975), 105–119.
- M. Queffélec, Substitution Dynamical Systems—Spectral Analysis, Lecture Notes in Math. 1294, Springer, Berlin, 1987.
- K. F. Roth, Rational approximations to algebraic numbers, Mathematika 2 (1955), 1-20; corrigendum, 169.
- [20] W. Schmidt, On continued fractions and Diophantine approximation in power series fields, Acta Arith. 95 (2000), 139–166.
- [21] C. Siegel, Approximation algebraischer Zahlen, Math. Z. 10 (1921), 173–213.

A. Firicel

- [22] D. Thakur, Diophantine approximation exponents and continued fractions for algebraic power series, J. Number Theory 79 (1999), 284–291.
- [23] D. Thakur, Function Field Arithmetic, World Sci., Singapore, 2004.
- [24] A. Thue, Über Annäherungswerte algebraischer Zahlen, J. Reine Angew. Math. 135 (1909), 284–305.
- [25] S. Uchiyama, Rational approximations to algebraic functions, J. Fac. Sci. Hokkaido Univ. Ser. I 15 (1961), 173–192.
- [26] J. F. Voloch, Diophantine approximation in positive characteristic, Period. Math. Hungar. 19 (1988), 217–225.

Alina Firicel Institut Joseph Fourier Université de Grenoble 100 rue des maths, BP 74 38402 St Martin d'Hères Cedex, France E-mail: Alina.Firicel@ujf-grenoble.fr

> Received on 29.9.2011 and in revised form on 20.6.2012 (6831)

322