TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 321, Number 2, October 1990

ZETA FUNCTIONS OF FORMAL LANGUAGES

JEAN BERSTEL AND CHRISTOPHE REUTENAUER

ABSTRACT. Motivated by symbolic dynamics and algebraic geometry over finite fields, we define cyclic languages and the zeta function of a language. The main result is that the zeta function of a cyclic language which is recognizable by a finite automation is rational.

1. INTRODUCTION

Motivated by algebraic geometry over finite fields and symbolic dynamics, we call a *zeta function* of a formal language L the function

$$\zeta(L) = \exp\left(\sum a_n \frac{t^n}{n}\right)$$

where a_n is the number of words of length n in L. Moreover, we say that a language is *cyclic* if it is conjugation-closed ($uv \in L \Leftrightarrow vu \in L$) and if for any two words having a power in common, if one of them is in L, then so is the other. Such languages are rather special, but occur in two very different theories: to each algebraic variety over a finite field, one may associate a cyclic language over this field (conjugation of words corresponds here to conjugation over the field, and the power condition to the compatibility between the various extensions); on the other hand, for any sofic system (in symbolic dynamics) the set of words w, such that $\cdots www\cdots w\cdots$ is in the system, is a cyclic language, even recognizable.

Our main result states that if L is a cyclic language which is recognizable by a finite automaton (i.e., regular), then its zeta function is rational (Theorem 1), and effectively computable, as the proof shows.

One consequence is that the zeta function of a sofic system in symbolic dynamics is rational, a fact which was claimed in [29 and 9]. Moreover, it is effectively computable, if the sofic system is given by a semigroup or a graph.

There is of course a striking analogy with one of the Weil ex-conjectures, stating that the zeta function of an algebraic variety over a finite field is rational (Dwork's theorem [10], see also [14]). In fact, several constructions allow us to associate to each such variety a cyclic language (see §3); however, these

Received by the editors September 25, 1987.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 68Q45; Secondary 34C35, 14G10, 20M35, 68Q70, 05A15.

constructions do not produce recognizable languages, so Theorem 1 does not give a new proof of Dwork's theorem.

We prove, in fact, a structure theorem on cyclic recognizable languages: such a language is (informally speaking) a linear combination over $\mathbb{Z}$ of traces of finite deterministic automata (Theorem 2). This result is actually the difficult point; it has Theorem 1 as a simple consequence, using a variant (Proposition 2) of a theorem of Bowen and Lanford [5], which rests essentially on Jacobi's identity $\det(m) = \exp \circ \operatorname{tr} \circ \log(m)$, for any matrix m (when defined). The proof of Theorem 2 is made in §4 and uses the theory of minimal ideals in finite semigroups.

A by-product of Theorem 2, which should be explored elsewhere, is that cyclic recognizable languages constitute a new class of languages which, as biprefix codes [25], have a semisimple syntactic algebra.

We want to thank Mike Boyle, who clarified for us the history of the rationality of the zeta function of a sofic system, and for his careful reading of the manuscript and suggestions. The referee helped us with his comments, too.

A preliminary version of the present paper has been published in the Proceedings of the International Congress of Automata, Languages and Programming, Turku (1988).

2. Definitions and main result

We assume the reader is familiar with the elementary notions of finite automata theory (see [19; 11, Vol. A]). Recall that when L is a language contained in some free monoid A^*, then L is regular if and only if L is recognizable (by a finite automaton).

Let a_n be the number of words of length n in the language L. Then the usual *generating function* of L is $\sum_{n\geq 0} a_n t^n$. It is a well-known result, which goes back to Chomsky and Schützenberger [8], that when L is recognizable by a finite automaton, then its generating function is a rational function.

Call *zeta function* of L the function

$$\zeta(L) = \exp\left(\sum_{n\geq 1} a_n \frac{t^n}{n}\right).$$

This definition and the following ones will be motivated in the next section. This function is in general neither rational nor has integer coefficients, even if L is recognizable: for instance, for $L = \{a\}$ and $L = \{(ab)^n | n \in \mathbb{N}\}$, the zeta functions are respectively $\exp(t)$ and $1/\sqrt{1-t^2}$.

We say that a language is *cyclic* if for any words u, v, w and integer $n \geq 1$, the two following conditions hold:

$$uv \in L \Leftrightarrow vu \in L, \tag{1}$$

$$w \in L \Leftrightarrow w^n \in L. \tag{2}$$

Recall that two words x and y are said to be *conjugate* if for some words u and v, one has $x = uv$, $y = vu$. Hence, equation (1) means that L is conjugation-closed. Moreover, each word x in A^* is the power y^n of a unique *primitive* word y, which means that y is not a nontrivial power of another word (see e.g., [3 or 21]): y is called the *primitive root* of x. Then, equation (2) means that L is closed for the equivalence relation described by: x and y are equivalent iff x and y have the same primitive root iff x and y have a nontrivial power in common. This easily implies that the set of cyclic languages is closed for arbitrary union, intersection and complementation.

A first fact, rather classical (compare to [17, Proposition 11.1.3]), implies that the zeta function of a cyclic language has integer coefficients.

Proposition 1. *Let L be a cyclic language. Then its zeta function has the infinite product expansion*

$$\zeta(L) = \prod_{n\geq 1} \frac{1}{(1-t^n)^{\alpha_n}} \tag{3}$$

where α_n is the number of conjugation classes of primitive words contained in L. In particular, $\zeta(L)$ has integer coefficients.

Note that if two words are conjugate, they are simultaneously primitive or not.

Equivalently, α_n may be defined as the number of *Lyndon words* of length n in L (see e.g., [21]). For instance, when L is simply the whole free monoid A^*, then the α_n's are the *Witt numbers*, which count the Lyndon words, the homogeneous dimensions of free Lie algebras, the ranks of the quotients of the lower central series of a free group, the primitive necklaces and the irreducible polynomials over a finite field (see e.g., [21, 27]).

Proof. We have to show that

$$\exp\left(\sum_{n\geq 1} a^n \frac{t^n}{n}\right) = \prod_{k\geq 1} \frac{1}{(1-t^k)^{\alpha^k}}.$$

Take the logarithmic derivative of both members and multiply by t, obtaining

$$\sum_{n\geq 1} a_n t^n = \sum_{k\geq 1} \alpha_k \frac{kt^k}{1-t^k} = \sum_{k\geq 1}\sum_{p\geq 1} \alpha_k k t^{kp}.$$

This is equivalent to

$$a_n = \sum_{k|n} k\alpha_k.$$

But this expresses the fact that each word x of length n is the power of a unique primitive word of length k dividing n and has k conjugates. □

Our main result is

Theorem 1. *If L is a cyclic language which is recognizable by a finite automaton, then its zeta function is rational.*

Example 1. Let L be the set of words on the alphabet $\{a, b, c\}$ of the form

$$a^{n_0}bca^{n_1}bc\cdots bca^{n_k}$$

for some $k \geq 1$ and $n_i \geq 0$, or of the form

$$ca^{n_0}bca^{n_1}bc\cdots bca^{n_k}b$$

for some $k \geq 0$ and $n_i \geq 0$. Then L is cyclic and recognizable. The number a_n of words of length n in L is $F_n - 1 + F_{n-2}$, where the F_n is the nth Fibonacci number. Hence, $a_n = \theta^n + \overline{\theta}^n - 1$ where

$$\theta = \frac{1+\sqrt{5}}{2}, \qquad \overline{\theta} = \frac{1-\sqrt{5}}{2}.$$

Thus

$$\begin{aligned}\zeta(L) &= \exp\left(\sum_{n\geq 1}(\theta^n + \overline{\theta}^n - 1)\frac{t^n}{n}\right)\\ &= \exp\left(\sum \theta^n \frac{t^n}{n}\right)\exp\left(\sum \overline{\theta}^n \frac{t^n}{n}\right)\exp\left(\sum \frac{-t^n}{n}\right)\\ &= \frac{1-t}{(1-\theta t)(1-\overline{\theta}t)} = \frac{1-t}{1-t-t^2}.\end{aligned}$$

Hence $\zeta(L)$ is rational.

It is known in general (see e.g., [17, Proposition 11.1.1]) that $\exp(\sum a_n t^n/n)$ is rational if and only if one has $a_n = \alpha_1\lambda_1^n + \cdots + \alpha_k\lambda_k^n$ for some *integers* α_i and some complex numbers λ_i. This arithmetic approach is, however, impossible in our case.

Remarks. 1. As the proof of Theorem 1 will show, the zeta function may be effectively computed. It should be noted that it is *decidable* if a given recognizable language L is cyclic. Indeed, condition (1) and (2) may be tested in the *syntactic monoid* of L, and this monoid is finite (see [19; 11, Vol. A]). We do not know, however, how to construct all cyclic recognizable languages (except of course the trivial construction of enumerating all automata and checking if the language is cyclic.) Note that the set of cyclic recognizable language is a boolean algebra. However, it is not a variety in the sense of [11, Vol. B].

2. It is a well-known fact that the conjugation-closure of a recognizable language L (that is, the smallest conjugation-closed language containing L) is still recognizable. However, it is not true that the cyclic closure of a recognizable language is always recognizable; take for instance the language $a^*b^* = \{a^i b^j | i, j \geq 0\}$ and use the pumping lemma for recognizable languages (see e.g., [11, Vol. A, Proposition 2.5.1]).

3. It has been proved recently [15] that it is decidable if the zeta function of a recognizable language is rational; note, however, that this condition is far from implying that the language is cyclic. Indeed, changing a cyclic language in a finite number of words without changing a_n will give a language with the same zeta function, but the cyclic property is easily destroyed. See also [16] for related results.

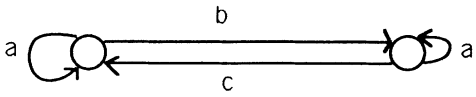
In order to prove Theorem 1, we will prove a more general result, which gives some insight in the structure of cyclic recognizable languages.

Denote by $\mathbb{Z}\langle\langle A\rangle\rangle$ the set of noncommutative formal power series over $\mathbb{Z}$ on the alphabet A. Each language L defines a series, its *characteristic series* defined by $\underline{L} = \sum_{w\in L} w$. Now, let $\mathscr{A}$ be a finite automaton over A, and define a formal power series, called the *trace* of $\mathscr{A}$ and denoted by $\mathrm{tr}(\mathscr{A})$, by

$$\mathrm{tr}(\mathscr{A}) = \sum_{w\in A^*} \alpha_w w$$

where the coefficient α_w of the word w is equal to the number of couples (q, c) where q is a state in $\mathscr{A}$ and c a path $q \to q$ in $\mathscr{A}$ labelled w.

Example 2. The trace of the automaton



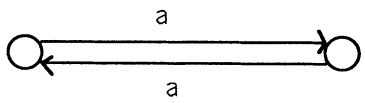
is the series having as coefficient of w

2, if w is a power of a;

1, if w is a shuffle of a's and a word of the form $(bc)^i$ or $(cb)^i$, $i \geq 1$.

0, otherwise.

The trace of the automaton

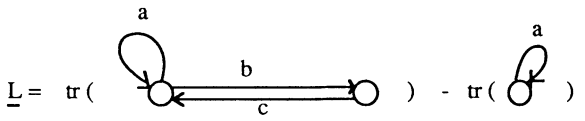


is $\sum_{n\geq 0} 2a^{2n}$.

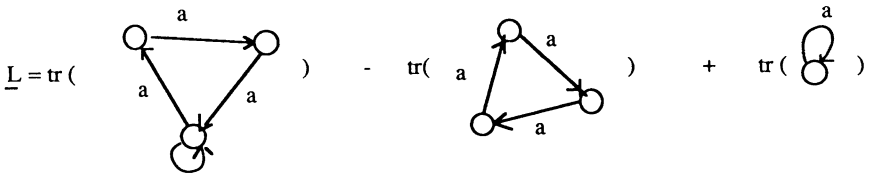
In what follows, a *deterministic* automaton will always be a not necessarily complete deterministic automaton (see [11, Vol. A] for definitions).

Theorem 2. *The characteristic series of each cyclic regular language is a linear combination over* $\mathbb{Z}$ *of traces of finite deterministic automata.*

Example 3. For $L =$ the language of Example 1, one has



Now, let L be the set of words on the alphabet $\{a, b\}$ such that between any two b's, the number of a's is a multiple of 3, even cyclically. Then



Theorem 2 will be proved in §4. In the sequel of this section, we show how one may deduce Theorem 1 from Theorem 2. In fact, we shall prove a little bit more.

Let $\pi : \mathbb{Z}\langle\langle A\rangle\rangle \to \mathbb{Z}[[A]]$ be the natural homomorphism, where $\mathbb{Z}[[A]]$ is the usual commutative algebra of formal power series in the variables $a \in A$. Let $S \in \mathbb{Z}\langle\langle A\rangle\rangle$ be a noncommutative series. Then one has $S = \sum_{n\geq 0} S_n$ where each S_n is the homogeneous part of S of degree n. Call *generalized zeta function* of S the commutative series

$$Z(S) = \exp\left(\sum_{n\geq 1} \frac{\pi(S_n)}{n}\right) \in \mathbb{Z}[[A]].$$

Note that if L is a language, then

$$\zeta(L) = \theta(Z(\underline{L}))$$

where θ: $\mathbb{Z}[[A]] \to \mathbb{Z}[[t]]$ is the homomorphism $\theta(a) = t$, for any letter a in A. Hence it suffices to show that $Z(\underline{L})$ is rational, under the hypothesis of Theorem 1. Call *matrix* of an automaton $\mathscr{A}$ the matrix E in $\mathbb{Z}[A]^{Q\times Q}$ (where Q is the set of states of $\mathscr{A}$) defined by

$$E_{p,q} = \sum_{p \xrightarrow{a} q} a$$

where $p \xrightarrow{a} q$ means that there is an edge labelled a from p to q. Call *determinant* (cf. [28; 3, VIII.2]) of $\mathscr{A}$ the polynomial in $\mathbb{Z}[[A]]$

$$\det(\mathscr{A}) = \det(I - E)$$

where I is the $Q \times Q$ identity matrix.

Proposition 2. *The generalized zeta function of the trace of a finite automaton is equal to the inverse of the determinant of this automaton.*

Proof. Let $\mathscr{A}$ be a finite automaton. Then it is an easy consequence of a well-known fact in automata theory (see e.g., [10, Proposition VI.6.1]) that

$$\pi(\mathrm{tr}(\mathscr{A})) = \mathrm{tr}\left(\sum_{n\geq 0} E^n\right) = \mathrm{tr}((I-E)^{-1}).$$

Actually, this equality justifies the terminology "trace of an automaton". More precisely, let

$$\mathrm{tr}(\mathscr{A}) = \sum_{n\geq 0} S_n$$

be the decomposition into homogeneous parts. Then $\pi(S_n) = \mathrm{tr}(E^n)$. Hence the generalized zeta function of $\mathrm{tr}(\mathscr{A})$ is

$$Z = \exp\left(\sum_{n\geq 1} \frac{\pi(S_n)}{n}\right) = \exp\left(\sum_{n\geq 1} \frac{1}{n}\mathrm{tr}(E^n)\right)$$

$$= \exp\left(\mathrm{tr}\sum_{n\geq 1} \frac{E^n}{n}\right) = \exp(\mathrm{tr}(\log(I-E)^{-1})).$$

Now, the Jacobi's identity tells us that $\det(M) = \exp(\mathrm{tr}(\log(M)))$ for any matrix M where it is defined (instead of the Jacobi's identity, one may use e.g., [14, Appendix, Lemma 4.1]). Hence $Z = \det(I-E)^{-1}$ which was to be shown. □

In order to deduce Theorem 1, note that if $S = \sum \alpha_i S_i$ for some series S, S_i and integers α_i, then $Z(S) = \prod_i Z(S_i)^{\alpha_i}$. Thus Theorem 1 may be deduced from Theorem 2 and Proposition 2. Note that the condition $\alpha_i \in \mathbb{Z}$ is crucial to rationality.

Example 4. For $L =$ the first language of Example 3, we have

$$Z(L) = \begin{vmatrix} 1-a, & -b \\ -c, & 1 \end{vmatrix}^{-1} \cdot |1-a| = \frac{1-a}{1-a-bc}.$$

Its ordinary zeta function is

$$\zeta(L) = \frac{1-t}{1-t-t^2}$$

For the second one, we have

$$Z(L) = \begin{vmatrix} 1-b, & -a, & 0 \\ 0, & 1, & -a \\ -a, & 0, & 1 \end{vmatrix}^{-1} \cdot \begin{vmatrix} 1, & -a, & 0 \\ 0, & 1, & -a \\ -a, & 0, & 1 \end{vmatrix} \cdot |1-a|^{-1}$$

$$= \frac{1-a^3}{(1-b-a^3)(1-a)} = \frac{1+a+a^2}{1-b-a^3}.$$

Its ordinary zeta function is

$$\zeta(L) = \frac{1 + t + t^2}{1 - t - t^3}$$

Another consequence of Theorem 2 is that the syntactic algebra of each cyclic recognizable language is semisimple (and finite dimensional). Indeed, it suffices to apply Proposition II.2.1(i) of [24]. Thus, cyclicity of a language is a combinatorial property which, as biprefixity, implies the semisimplicity of the syntactic algebra [25].

3. Motivations and applications

(a) Let $\mathbb{F}_q$ be the finite field with q elements, $\mathbb{F}_{q^\infty}$ its algebraic closure and $f \in \mathbb{F}_q[x_1, \ldots, x_k]$. Let V be the set of solutions in $\mathbb{F}_{q^\infty}$ of the algebraic equation

$$f(x_1, \ldots, x_k) = 0 \tag{4}$$

and let a_n be the number of those solutions which lie in the field $\mathbb{F}_{q^n}$. Then the *zeta function* of f is the series

$$\zeta(f) = \exp\left(\sum_{n \geq 1} a_n \frac{t^n}{n}\right).$$

It was one of the Weil conjectures, proved by Dwork [10], that this function is rational (more generally, the same holds for any algebraic variety V defined over $\mathbb{F}_q$).

Now, let A be the alphabet $A = (\mathbb{F}_q)^k$. Then there exists a mapping $\varphi: A^* \to \mathbb{F}_{q^\infty}$ with the following properties:

(i) For any n, $\varphi|A^n$ is a bijection from A^n onto $\mathbb{F}_{q^n}$.

(ii) For any words u and v, $\varphi(u, v)$ and $\varphi(vu)$ are conjugate points over $\mathbb{F}_q$.

(iii) For any word w and integer $n \geq 1$, $\varphi(w) = \varphi(w^n)$.

Such a mapping may be constructed using a family of primitive elements, one for each $\mathbb{F}_{q^n}$, following Golomb [13]; or using a family of normal bases [20] of $\mathbb{F}_{q^n}$ (see e.g., [27]).

Note that an algebraic variety V defined over $\mathbb{F}_q$ (such as the set of solutions of equation (4)) is $\mathbb{F}_q$-conjugation-closed. Hence $L = \varphi^{-1}(V)$ will be a cyclic language, which encodes V, and the zeta function of L is equal to the zeta function of the algebraic variety V.

Unfortunately, no known mapping φ as above allows us to obtain a recognizable language L. This would give a new proof of the rationality of the zeta function of V, which was one of the motivations of this paper. The construction of a mapping φ such that algebraic varieties correspond to recognizable languages is an open problem, certainly difficult, related to the construction of

a natural bijection between irreducible polynomials over $\mathbb{F}_q$ of degree n and primitive necklaces over $\mathbb{F}_q$ of length n (see e.g., [27]).

(b) Let A be a finite alphabet and $\sigma : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be the *shift mapping*, that is

$$\sigma : (a_n)_{n\in\mathbb{Z}} \to (a_{n+1})_{n\in\mathbb{Z}}.$$

If $S \subseteq A^{\mathbb{Z}}$ is closed under σ, then its zeta function is $\exp(\sum_{n\geq 1} u_n \frac{t^n}{n})$ where u_n is the number of points x in S such that $\sigma^n(x) = x$ (in other words, x is periodic and has n as a period). Call *pattern* of a periodic word $x = (a_n)_{n\in\mathbb{Z}}$ a word $w \in A^*$ such that $p = \text{length}(w)$ is a period of x and that for some $n \in \mathbb{Z}$, one has $w = a_{n+1} \cdots a_{n+p}$. In other words

$$x = \cdots www \cdots w \cdots$$

with the origin 0 somewhere. Then associate to each σ-closed subset S of $A^{\mathbb{Z}}$ the language L of its patterns. Evidently, L is a cyclic language, whose zeta function is equal to that of S.

We consider now the case where S is a *sofic* system [29]. Recall that such a system is obtained in the following way: let M be a finite monoid with a zero 0, and let $\mu: A^* \to M$ be a monoid homomorphism from the free monoid A^* into M. Then S is defined to be the set of sequences $(a_n)_{n\in\mathbb{Z}} \in A^{\mathbb{Z}}$ such that for any $i < j$ in $\mathbb{Z}$, one has $\mu(a_i a_{i+1} \cdots a_j) \neq 0$. Equivalently, S is the set of sequences (a_n) such that $a_i \cdots a_j$ is the label of some path in a fixed finite automaton (depending on S). If S is a sofic system, it is clear that the set of factors of the sequences in S is a recognizable language. Hence, by the following result, its set of patterns is recognizable, too.

Proposition 3. *Let L be a recognizable language such that for any word w and integer $n \geq 1$, one has: $w \in L \Rightarrow w^n \in L$. Then the cyclic closure of L is recognizable. The set of patterns of the periodic words of a sofic system is recognizable.*

All the constructions are effective, of course. See [2] for the study of languages associated to sofic systems.

Proof. (i) Let $L = \mu^{-1}(P)$, where $\mu: A^* \to M$ is the natural monoid homomorphism from A^* onto the (finite) syntactic monoid M of L and P is a subset of M (see [17, 10]).

Let $P' = \{m \in M | \exists p,\ q \in M,\ \exists n \geq 1,\ m = pq,\ (qp)^n \in P\}$.

Then $L' = \varphi^{-1}(P')$ is a recognizable language, which is the cyclic closure $\overline{L}$ of L. indeed, if w is in $\overline{L}$, then for some u, v and n, one has $w = uv$ and $(vu)^n \in L$; this implies that $\varphi(w) = \varphi(u)\varphi(v)$, $(\varphi(v)\varphi(u))^n \in P$, hence $\varphi(w) \in P'$ and $w \in L'$; conversely, if $w \in L'$, then a power of w is conjugate to some word in L, thus w is in $\overline{L}$.

(ii) Let S be a sofic system. Then S is equal to the set of labels of bi-infinite paths of a finite automaton $\mathscr{A}$. Let L be the language consisting of all words w such that for some state q in $\mathscr{A}$, there is a path $q \xrightarrow{w} q$. Then L is

recognizable and satisfies the condition of the proposition. Hence, its cyclic closure $\overline{L}$ is recognizable. But $\overline{L}$ is equal to the set of patterns of S, as may be easily verified. □

This proposition, together with Theorem 1, shows that the *zeta function of a sofic system is rational*, and gives an effective procedure for computing it. Actually, the rationality of the zeta function of a sofic system was quoted without proof by Coven and Paul [9], who claimed that Manning's argument [22] could be adapted. The latter was confirmed to us by Mike Boyle, especially in the light of a recent work of D. Fried [12]; moreover, Manning's argument is constructive, and so is another procedure given without proof by R. Bowen [6] and a recent one of M. Boyle [7]. Finally, there is another recent effective proof, due to M. P. Béal [1], which uses an exterior-power construction for finite automata.

Actually, we show a little bit more: the *generalized zeta function* of a sofic system is rational; the latter function is a series in several variables which gives some information on the commutative composition of the patterns of the periodic words. Note also that when S is an irreducible sofic system, then the cyclic language L associated to it as above allows us to recover S. Indeed, the set of periodic points is then dense in S. Observe that Proposition 2 is a variant of Bowen and Lanford's result [5], and that in the case of an irreducible subshift of finite type (i.e., the set of bi-infinite paths of a transitive graph), the inverse of the generalized zeta function is an irreducible polynomial, as shown in [26, Theorem 3] (see also [23, Lemma 4]).

4. Proof of theorem 2

A noncommutative formal power series

$$S = \sum_{w \in A^*} (S, w)w$$

will be called *cyclic* (in this section only) if the three following properties are satisfied:

(i) There exists a finite monoid M, a surjective monoid homomorphism $\mu : A^* \to M$ and a function $\varphi : M \to \mathbb{Z}$ such that for any word w, $(S, w) = \varphi \circ \mu(w)$. Moreover, for any group G contained in M, the restriction of φ to G is a $\mathbb{Z}$-linear combination of permutation characters of G (a permutation character is a function χ obtained in the following way: Let G act on a set E, and let $\chi(g) =$ number of points of E fixed by g).

(ii) S is conjugation-closed, that is, for any words u and v, $(S, uv) = (S, vu)$.

(iii) For any word w, the sequence $u_n = (S, w^{n+1})$ satisfies a proper linear recurrence (that is, for some $\alpha_1, \ldots, \alpha_k$, $\alpha_k \neq 0$, one has: $u_{n+k} = \alpha_1 u_{n+k-1} + \cdots + \alpha_k u_n$, for any $n \geq 0$).

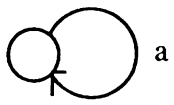
We shall prove

Theorem 2. *Each cyclic series is a $\mathbb{Z}$-linear combination of traces of finite deterministic automata.*

Remark. The first part of condition (i) expresses the fact that S is a rational power series whose set of coefficients is finite. Equivalently, S is a linear combination of characteristic series of recognizable languages [4, Theorem 2.7]. The extension of Theorem $2'$ to rational power series in general (including the good extension of the property "cyclic") is an open problem.

Theorem $2'$ implies Theorem 2. Indeed, for each cyclic recognizable language $L \subseteq A^*$, there exists by Kleene's theorem a finite monoid M, a surjective monoid homomorphism $\mu : A^* \to M$ and a subset P of M such that $\mu^{-1}(P) = L$. Define $\varphi : M \to \mathbb{Z}$ by $\varphi(m) = 1$ if $m \in P$, $\varphi(m) = 0$ otherwise. Then clearly $(\underline{L}, w) = \varphi \circ \mu(w)$. Moreover, if G is a group in M, φ is constant on G, because any two elements of G have a power in common (G being finite) and L is cyclic; so $\varphi|G$ is a $\mathbb{Z}$-multiple of the trivial character and (i) is satisfied for $S = \underline{L}$. Condition (ii) is also satisfied, because L is cyclic, and condition (iii) is true, because for any word w, the sequence $(\underline{L}, w^{n+1})_{n \geq 0}$ is constant, L being cyclic.

Now, we prove Theorem $2'$ by induction on the cardinality of the monoid M of condition (i). If M has a zero, we may assume that $\varphi(0) = 0$, replacing if necessary φ by $\varphi - \varphi(0)$ and S by $S - \varphi(0)T$, where T is the trace of the automaton



(an edge labelled a for each letter a). Let J be a 0-minimal ideal of M if M has a zero, and the minimal ideal of M if M has no zero. (See [19, Chapter 2] for the semigroup theory which is needed here.) If no element of J is idempotent, then each element x of J is of square 0, hence the sequence $(\varphi(x^{n+1}))_{n \geq 0}$ is $\varphi(x), 0, 0, \ldots, 0, \ldots$. Because of condition (iii), we must have $\varphi(x) = 0$. In this case, we may replace M by the Rees quotient M/J and conclude by induction, because J has at least 2 elements, hence $|M/J| < |M|$.

Hence, we may suppose that J contains an idempotent, hence a maximal group (or H-class) G. There exist a monoid representation

$$\theta : M \to G_0^{\lambda \times \lambda}$$

where G_0 is G with a zero adjoined, where each matrix $\theta(m)$ has at most one nonzero entry in each row, where the restriction of θ to G satisfies

$$\forall g \in G, \qquad \theta(g) = \begin{pmatrix} g & 0 & \ldots & 0 \\ * & 0 & \ldots & 0 \\ \vdots & \vdots & & \vdots \\ * & 0 & \ldots & 0 \end{pmatrix}, \tag{5}$$

and such that $\theta(0) = 0$ (see [19, II.5]).

We know by (i) that the restriction of φ to G is a $\mathbb{Z}$-linear combination of permutation characters:

$$\varphi|G = \sum_i \alpha_i \chi_i \qquad (\alpha_i \in \mathbb{Z}). \tag{6}$$

For each i there exists, by definition of a permutation character, a representation β_i of G of order b_i by 0-1 invertible permutation matrices such that

$$\chi_i(g) = \operatorname{tr}(\beta_i(g)). \tag{7}$$

Define a representation θ_i of M of order $b_i\lambda$ by 0-1 matrices having one nonzero entry at most in each row, by replacing in each matrix $\theta(m)$ each nonzero entry g by $\beta_i(g)$ and each zero entry by the zero matrix of order b_i.

Now, we obtain a representation $\theta_i \circ \mu$ of the free monoid, which is associated to a deterministic finite automata $\mathscr{A}_i$, because of the row-form of the matrices. Define

$$T = S - \sum \alpha_i \operatorname{tr}(\mathscr{A}_i).$$

Let $\Psi : M \to \mathbb{Z}$ be the function defined by

$$\Psi(m) = \varphi(m) - \sum_i \alpha_i \operatorname{tr}(\theta_i(m)). \tag{8}$$

Then, by construction, we have for any word w

$$(T, w) = \Psi \circ \mu(w). \tag{9}$$

Let g be in G. Then by (6) and (7), $\varphi(g) = \sum \alpha_i \chi_i(g) = \sum \alpha_i \operatorname{tr}(\beta_i(g))$. This is equal, by the special form (5) and by definition of θ_i, to $\sum \alpha_i \operatorname{tr}(\theta_i(g))$. Hence, $\Psi|G = 0$.

We show that T is a cyclic series. Condition (iii) is satisfied. Indeed, for any matrix P, the sequence $(\operatorname{tr}(P^{n+1}))_{n \geq 0}$ satisfies to a proper linear recurrence, associated to the polynomial having as roots the nonzero characteristic roots of P. Moreover, any linear combination of proper sequences is still proper [4]. Condition (ii) is clearly satisfied, because $\operatorname{tr}(PQ) = \operatorname{tr}(QP)$. Moreover, condition (i) is satisfied. Indeed, this comes from (9) on one hand; on the other hand, if H is a group in M, then $\Psi|H$ is a $\mathbb{Z}$-linear combination of permutation-characters by (8) and the following easy lemma.

Lemma 1. *Let H be a group and $\theta : H \to \mathbb{Z}^{d \times d}$ be a representation of H by* 0-1 *matrices having at most one nonzero entry by row. Then the function $h \to \operatorname{tr}(\theta(h))$ is a permutation character.*

Proof. Each h induces a partial function on the set $\{1, \ldots, d\}$, by $i \cdot h = j$ if $\theta(h)_{i,j} = 1$, undefined if the ith row of $\theta(h)$ is zero. These functions have all the same image E, because H is a group. The restriction of each h to E is a bijection $E \to E$, and the number of fixpoints of this bijection is precisely $\operatorname{tr}(\theta(h))$. □

Now, we show that Ψ vanishes on J, which will allow to replace M by the Rees quotient M/J and conclude the proof by induction. We have

$\Psi(0) = 0$, because $\theta(0) = 0$. If x in J is of square 0, then $\Psi(x) = 0$, because $\Psi(x^n) = 0$ for $n \geq 2$ and the sequence $(\Psi(x^{n+1}))_{n\geq 0}$ satisfies a proper linear recurrence. If x in J is not of square 0, then there exist elements u, v in J such that $x = uv$ and $vu \in G$. Let us admit this for the moment; then, as $\Psi|G = 0$, we have $\Psi(x) = \Psi(uv) = \Psi(vu) = 0$.

Hence, it remains to prove the above claim, which is a consequence of the following lemma, J being a 0-simple semigroup.

Lemma 2. *Let J be a 0-simple finite semigroup and G a maximal subgroup of J. Then any element of J of square $\neq 0$ is conjugate to some element in G.*

Proof. We use the Rees matrix representation of J: for some finite sets I and Λ, the semigroup J is isomorphic to the set consisting of 0 and of the triples (i, g, λ) with $i \in I$, $\lambda \in \Lambda$, $g \in G$ and multiplication $(i, g, \lambda)(j, h, \mu) = (i, gp_{\lambda j}h, \mu)$ if $p_{\lambda j} \neq 0$, and $= 0$ if $p_{\lambda j} = 0$, where $P = (p_{\lambda j}) \in G_0^{\Lambda \times J}$ is a fixed matrix (see [19, Chapter 3]).

One may suppose that G corresponds, in the above isomorphism, to the set $G' = \{(i, g, \lambda) | g \in G\}$ and that $x = (j, h, \mu)$. As $x^2 \neq 0$, one has $p_{\mu j} \neq 0$. Similarly, $p_{\lambda i} \neq 0$. Now, define $u = (j, h, \lambda)$ and $v = (i, p_{\lambda i}^{-1}, \mu)$. Then $uv = (j, hp_{\lambda i}p_{\lambda i}^{-1}, \mu) = x$ and $vu = (i, p_{\lambda i}^{-1}p_{\mu j}h, \lambda) \in G'$, which concludes the proof. □

References

1. M.-P. Béal, *Puissance extérieure d'un automate déterministe: application au calcul de la fonction zeta d'un système sofique* (to appear).
2. D. Beauquier, *Minimal automaton for a factorial, transitive, rational language*, Theoret. Comput. Sci. **67** (1989), 65–73.
3. J. Berstel and D. Perrin, *The theory of codes*, Academic Press, 1986.
4. J. Berstel and C. Reutenauer, *Rational series and their languages*, EATCS Monogr. in Theoret. Compu. Sci., 1988.
5. R. Bowen and O. Lanford, *Zeta functions of restrictions of the shift transformation*, Proc. Sympos. Pure Math., vol. 14, Amer. Math. Soc., Providence, R. I., 1970, pp. 43–50.
6. R. Bowen, *On axiom A diffeomorphisms*, CBMS Regional Conf. Ser. Math., no. 35, Amer. Math. Soc., Providence, R. I., 1978.
7. M. Boyle, Personal communication (1988).
8. N. Chomsky and M. P. Schützenberger, *The algebraic theory of context-free languages*, Computer Programming and Formal Systems, (P. Braffort and D. Hirschberg, eds.), North-Holland, 1963.
9. E. M. Coven and M. E. Paul, *Sofic systems*, Israel J. Math. **20** (1975), 165–177.
10. B. Dwork, *On the rationality of the zeta function of an algebraic variety*, Amer. J. Math. **82** (1960), 631–648.
11. S. Eilenberg, *Automata, languages and machines*, Vols. A, B, Academic Press, 1974.
12. D. Fried, *Finitely presented dynamical systems*, Ergodic Theory Dynamical Systems **7** (1987), 489–507.
13. S. W. Golomb, *Irreducible polynomials, synchronization codes, primitive necklaces and the cyclotomic algebra*, Combinatorial Mathematics and its Applications, Monograph Series in Prob. and Stat. 4, Univ. of North Carolina Press, Chapel Hill, 1969, pp. 358–370.

14. R. Hartshorne, *Algebraic geometry*, Springer-Verlag, 1977.
15. J. Honkala, *A necessary condition for the rationality of the zeta function of a regular language*, Theoret. Comput. Sci. **66** (1989), 341–347.
16. ____, *On generalized zeta functions of formal languages and series*, Discrete Appl. Math. (to appear).
17. K. Ireland and M. Rosen, *A classical introduction to modern number theory*, Springer-Verlag, 1982.
18. N. Koblitz, *P-adic numbers, p-adic analysis and zeta functions*, Springer-Verlag, 1984.
19. G. Lallement, *Semigroups and combinatorial applications*, Wiley, 1979.
20. R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia of Mathematics, Addison-Wesley, 1983.
21. M. Lothaire, *Combinatorics on words*, Encyclopedia of Mathematics, Addison-Wesley, 1983.
22. A. Manning, *Axiom* A *diffeomorphisms have rational zeta functions*, Bull. London Math. Soc. **3** (1971), 215–220.
23. M. Nasu, *Uniformly finite-to-one and onto extensions of homomorphisms between strongly connected graphs*, Discrete Math. **39** (1982), 171–197.
24. C. Reutenauer, *Séries formelles et algèbres syntaxiques*, J. Algebra **66** (1980), 448–483.
25. ____, *Semisimplicity of the algebra associated to a biprefix code*, Semigroup Forum **23** (1981), 327–342.
26. ____, *Ensembles libres de chemins dans un graphe*, Bull. Soc. Math. France **114** (1986), 135–152.
27. ____, *Mots circulaires et polynômes irréductibles*, Ann. Sci. Math. Québec **12** (1988), 275–285.
28. M. P. Schützenberger, *Sur certains sous-monoïdes libres*, Bull. Soc. Math. France **93** (1965), 209–223.
39. B. Weiss, *Subshifts of finite type and sofic systems*, Monatsh. Math. **77** (1973), 462–474.

LITP, Université Pierre et Marie Curie, 4 Place Jussieu, 75252 Paris, France

Département de Matématiques & Informatique Université du Québec À Montréal, C.P. 8888, Succ.A, Montréal, Québec, Canada H3C 3P8