ADVANCES IN APPLIED MATHEMATICS **18,** 1–17 (1997)
ARTICLE NO. AM960492

N-Rationality of Zeta Functions

Christophe Reutenauer*

Université du Québec à Montréal, CP 8888 succ. Centre-Ville, Montréal, Canada H3C 3P8

Received February 10, 1996

DEDICATED TO THE MEMORY OF MARCEL PAUL SCHÜTZENBERGER

1. INTRODUCTION

The main result of the present paper is the sharpening of rationality theorems of Manning [23], Fried [18], and Gromov [19], with an application to hyperbolic groups. The basic concept we shall use is that of **N**-rationality.

A series is called **N**-rational if it is obtained from polynomials over **N** in the variable t by applying the following operations: sum, product, *star* (by definition the star of a series S is $S^* = \sum_{n \geq 0} S^n$, defined if S has no constant term: it is the inverse of $1 - S$). The important condition is that one never performs subtraction; this may be interpreted by the existence of an algorithm which generates the objects whose generating function is the given series. Equivalently, a series is **N**-rational if and only it is the generating series of some rational (regular) language. Thus **N**-rationality is a kind of combinatorial rationality.

An **N**-rational series is a rational series and has necessarily coefficients in **N**, but a rational series with coefficients in **N** need not be **N**-rational (see the book of Eilenberg [12, Example VIII.6.1] for a counterexample and more on this subject). As a consequence of theorems of Berstel [3], Soittola [27], and Katayama et al. [20], a complete characterization of **N**-rational series is known (see Section 4.5): roughly speaking, **N**-rational series are rational series with coefficients in **N** which have a unique pole of minimal modulus.

Many rational series appearing in the mathematical literature are actually **N**-rational. This is the case for the Hilbert series of finitely generated

* Supported by a NSERC grant (Canada) and LABRI (Bordeaux).

0196-8858/97 $25.00

commutative graded algebras, by the Hilbert−Serre theorem. More generally, this is also the case for the Hilbert series of the so-called automaton algebras; see the book [28] by Ufnarovskij, where many results on Hilbert and Poincaré series are discussed (there is also a huge bibliography); it is likely that most of these series, when they are rational, are actually **N**-rational. Next, the generating series by length of the geodesic words in an hyperbolic group is **N**-rational, since this set of words is a rational language; a similar property holds more generally for automatic groups, see [14]. Note that the Hilbert series of the plactic monoid, or equivalently that of the enveloping algebra of the free nilpotent Lie algebra of class 2, is also **N**-rational, by Littlewood's formula giving the sum of all Schur functions. Finally, note that the zeta function of a smooth algebraic variety over a finite field is **N**-rational: indeed, by Dwork's theorem, it is rational, has coefficients in **N**, and, by Deligne's theorem, it has a unique pole of minimal modulus (equal to q^{-n}, with n = dimension of the variety and q = number of elements in the ground field).

We study here the **N**-rationality of certain *cyclic sets*, in the sense of Rota: these are sets with an action of the infinite cyclic group. Their good enumerating series are zeta functions: see the work of Dress and Siebeneicher [10, 11]. The cyclic sets we investigate are finitely presented dynamical systems, in the sense of Gromov [19] and Fried [18]. We prove that their zeta functions are **N**-rational: this result (Theorem 4.1) extends the rationality theorems of Manning [23] for systems satisfying Smale's Axiom A, Coven and Paul [9] for sofic systems (see also [5] and [1]) and Fried [18] for finitely presented systems. It is obtained as a consequence of similar theorems on languages: first we extend the rationality theorem of Berstel and the author [5] concerning rational cyclic languages (that is, languages which are recognizable by a finite automaton and which are conjugation-, power-, and radical-closed), and show that they are **N**-rational (Theorem 2.1); then we extend this result to a class of rational equivalence relations, whose definition was motivated by the definition of finitely presented systems (Theorem 3.1). In Section 4, we derive several consequences, including the **N**-rationality for finitely presented dynamical systems, an extension to sub-Markov systems, which generalizes a result of Gromov and has a consequence for the enumeration of stable conjugation classes in hyperbolic groups, and give several remarks and conjectures.

2. LANGUAGES

Let A be a finite *alphabet* and let A^* denote the free monoid generated by A. If L is a subset of A^*, we call it a *language*. A language is *rational* if it is obtained from finite languages by a finite number of *rational opera-*

tions: these are finite union and product and the operation $L \mapsto L^* = \bigcup_{n \geq 0} L^n$ = submonoid generated by L (this operation is called the *Kleene star operation*). Rational languages are also called *regular* languages. By Kleene's theorem, a language is rational if and only if it is *recognizable*. One of the many possible equivalent definitions of the latter notion is the following: $L \subseteq A^*$ is recognizable if for some finite monoid M, some monoid homomorphism μ: $A^* \to M$, and some subset P of M,

$$L = \mu^{-1}(P). \tag{1}$$

Observe that μ may be chosen to be surjective; then one has $L = \mu^{-1}\mu(L)$.

It is well known that if L is a rational language, then its (ordinary) *generating function* $\sum_{n \geq 0} |L \cap A^n| t^n \in \mathbf{Z}[[x]]$ is rational. Following [5], we call *zeta function* of L the series

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

It has been shown in [5] that if L is rational and *cyclic*, then $\zeta(L)$ is a rational series in $\mathbf{Z}[[t]]$. Recall that L is called cyclic if for any words u, v, w in A^* and any $n \geq 1$, one has: (i) $uv \in L \Leftrightarrow vu \in L$ and (ii) $w \in L \Leftrightarrow w^n \in L$. In a monoid, the transitive closure of the relation $uv \sim vu$ is called *conjugation*, since it specializes to usual conjugation in groups; in a free monoid, this relation is simply $uv \sim vu$ and a conjugation class is also called a *circular word*. Thus a language L is cyclic if and only if it is conjugation-closed (by (i)) and power- and radical-closed (by (ii)).

A series $S = \sum_{n \geq 0} a_n t^n \in \mathbf{Z}[[t]]$ is **N**-*rational* if the two following equivalent conditions hold:

(i) S is the (ordinary) generating function of a rational language;

(ii) S is obtained from polynomials with coefficients in **N** by a finite number of the following operations: sum, product, and the *star* operation $T \mapsto T^* = \sum_{n \geq 0} T^n = (1 - T)^{-1}$.

The concept of **N**-rational series is well known in language theory since the work of Schützenberger [25]: he has related the work of Kleene on finite automata to the concept of (noncommutative) rationality.

THEOREM 2.1. *The zeta function of a cyclic rational language is* **N**-*rational.*

Remarks. 1. The zeta function of a rational language is in general not rational; see [5].

2. In view of (i) above, the theorem means equivalently that for each rational cyclic language L, there exists a rational language L' such that the zeta function of L is equal to the generating function of L'.

We shall deduce Theorem 2.1 from a characterization of cyclic rational languages. Following Schützenberger [26], we call (finite) *factorization* of the free monoid A^* a totally ordered *finite* family $(F_i)_{i \in I}$ of free submonoids of A^* such that each word $w \in A^*$ has a unique factorization $w = \prod_{i \in I} w_i$, with $w_i \in F_i$, where the product is taken in decreasing order. Such a factorization is called *rational* if each F_i is a rational language.

THEOREM 2.2. *Let L be a language containing the empty word. Then L is a rational cyclic language if and only if there exists a rational factorization $A^* = \prod_{i \in I} F_i$ and a subset J of I such that L is the closure under conjugation of $\bigcup_{j \in J} F_j$.*

Proof of Theorem 2.1. Suppose that L is of the form given in Theorem 2.2. By [5, Prop. 1], $\zeta(L) = \prod_{C \subset L} (1 - t^{l(C)})^{-1}$, where the product is taken over all primitive conjugation classes C contained in L and $l(C)$ is the common length of the words in C (recall that a word is *primitive* if it is not a power of another word, and a class is primitive if all its elements are). By Schützenberger's factorization theorem [26], each conjugation class C in A^* intersects exactly one submonoid F_i. Since L is a union of classes, one has $\zeta(L) = \prod_{j \in J} \prod_{C \cap F_j \neq \emptyset} (1 - t^{l(C)})^{-1}$, where the second product is over the primitive conjugation classes C in A^*. By the factorization theorem again, the mapping $C \mapsto C \cap F_j$ is a bijection from the set of primitive conjugation classes C in A^* intersecting F_j into the set of primitive conjugation classes of the free monoid F_j (the latter is a *very pure* submonoid of A^*, that is, for any words u and v, uv, $vu \in F_j$ implies u, $v \in F_j$). Hence the second product above is equal to $\Pi_C (1 - t^{l(C)})^{-1}$, where the product is over all primitive conjugation classes C in the free monoid F_j and the length is with respect to A. Now, in a free monoid, the elements are in bijection with the multisets of primitive conjugation classes: indeed, this is a consequence of the theorem of Poincaré–Birkhoff–Witt and the fact that Hall bases are in bijection with primitive conjugation classes; or use Lyndon's theorem, Theorem 5.1.5 in [22]. Hence the last product is equal to $\sum_{w \in F_j} t^{l(w)}$, that is, the generating function of F_j, which is **N**-rational, F_j being rational. Finally, $\zeta(L)$ is the product of the generating functions of the F_j, $j \in J$, hence is **N**-rational. This proves Theorem 2.1.

The proof shows that the *multivariate zeta function* (in the sense of [5] where it is called generalized zeta function) of a cyclic rational language is **N**-rational.

Proof of Theorem 2.2. If L is the closure under conjugation of $\bigcup_{j \in J} F_j$, with the F_i as in the statement, then L is rational, since J is finite, each F_j is rational, and closure under conjugation preserves rationality. Moreover,

by the factorization theorem, each F_j is a *pure* submonoid, that is, $w \in F_j \Leftrightarrow w^n \in F_j$. Hence, the closure under conjugation of F_j is a cyclic language, and so is also L.

Conversely, let L be a rational cyclic language and μ: $A^* \to M$ be a surjective monoid homomorphism with M finite and $L = \mu^{-1}(P)$, $P \subset M$. Note that we have $w \in L \Leftrightarrow \mu(w) \in \mu(L)$.

Recall the lemma of Krohn and Rhodes (see [21, Lemma 7.2.7]): if a set X generates a finite monoid, then one of the four following cases occurs: (1) M is a cyclic monoid (that is, M may be generated by one element); (2) M is a group; (3) $S = M \setminus 1$ is a left simple semigroup (meaning that $Ss = S$ for any s in S); (4) there exists a partition $X = X_1 \cup X_2$ such that X_1^* and $(X_1^* X_2)^*$ are proper submonoids of M; recall that the notation Y^* means the submonoid generated by Y.

Furthermore, if C^* is the free monoid on C and $C = C_1 \cup C_2$ is a partition, then $C^* = (C_1^* C_2)^* C_1^*$ is a factorization of the free monoid (reminiscent of the Lazard elimination process, see [22, Example 5.3.12]). We shall construct the family $(F_i)_{i \in I}$ by iterating the latter factorization.

Suppose that we have already constructed a rational factorization $(F_i)_{i \in I}$. If for some $j \in I$ the submonoid $\mu(F_j)$ of M does not satisfy condition 1, 2, or 3 above (with M replaced by $\mu(F_j)$), let C be the unique basis of the free submonoid F_j of A^*; C is rational since F_j is. Then $X = \mu(C)$ generates $\mu(F_j)$ and we are in case 4. With the notation of that case, let $C_k = \mu^{-1}(X_k) \cap C$, $k = 1, 2$. Then C_k is rational and we have the factorization of the free monoid $F_j = C^* = (C_1^* C_2)^* C_1^*$; moreover, X has the partition $X_1 \cup X_2$, C has the partition $C_1 \cup C_2$, $X = \mu(C)$, and $\mu(C_k) \subset X_k$. This implies that $X = \mu(C) = \mu(C_1 \cup C_2) = \mu(C_1) \cup \mu(C_2) \subset X_1 \cup X_2 = X$. Thus we must have $\mu(C_i) = X_i$, hence $\mu((C_1^* C_2)^*) = (X_1^* X_2)^*$ and $\mu(C_1^*) = X_1^*$ are proper submonoids of $\mu(F_j)$. Then we replace F_j in the factorization $\prod F_i$ by $(C_1^* C_2)^* C_1^*$.

Thus an induction on the cardinality of the monoids $\mu(F_i)$, starting with the trivial factorization, shows that we may suppose that each submonoid $\mu(F_i)$ of M satisfies condition 1, 2, or 3. We show that, at the cost of factorizing once more each F_i, we may suppose that either $F_i \subset L$ or $F_i \cap L = \{1\}$.

Suppose that condition 1 holds, that is, $\mu(F_i)$ is a cyclic monoid; we may even suppose that it is not a group, otherwise we are in the next case. Then $\mu(F_i) = m^*$, $m \in M$, and $m^k \neq 1$ for $k \geq 1$. If $m^k \in \mu(L)$ for some $k \geq 1$, then, L being cyclic, $m \in \mu(L)$, and $m^k \in \mu(L)$ for any $k \geq 0$, since $1 \in L$. Hence $\mu(F_i) = m^* \subset \mu(L)$ and consequently $F_i \subset L$. If on the contrary $m^k \notin \mu(L)$ for any $k \geq 1$, then let C be the basis of F_i, $C_1 = \{w \in C \mid \mu(w) = 1\}$, $C_2 = C \setminus C_1 = \{w \in C \mid \mu(w) = m^k, \ k \geq 1\}$; then we have the factorization of the free monoid $F_i = (C_1^* C_2)^* C_1^*$,

$C_1^* \subset L$, $(C_1^* C_2)^* \cap L = \{1\}$ and we are done. Indeed, $\mu(C_1^*) = \{1\} \subset \mu(L)$, hence $C_1^* \subset L$ and $\mu((C_1^* C_2)^+) \subset \{m^k \mid k \geq 1\}$, hence $L \cap (C_1^* C_2)^* = \{1\}$.

Suppose now that condition 2 holds for $\mu(F_i)$, that is, it is a group. We know that $1 \in L$, hence the neutral element $\mu(1)$ of this group is in $\mu(L)$. If w is any word in F_i, then some power $\mu(w)^k$ is equal to $\mu(1)$. Hence, $w^k \in L$, and $w \in L$, since L is cyclic. We deduce that $F_i \subset L$.

Finally, suppose that condition 3 holds, that is $S = \mu(F_i) \setminus 1$ is a left simple semigroup. Using Lemma 2 in [4], we see that any two elements S have some powers which are conjugate. Hence, by cyclicity of L, either $S \subset \mu(L)$ or $S \cap \mu(L) = \emptyset$. In the first case $\mu(F_i) \subset \mu(L)$, thus $F_i \subset L$, and in the second case, we define C_1 and C_2 as in case 1, and we are done.

Finally, we find a subset J of I such that $F_j \subset L$ if $j \in J$ and $F_i \cap L = \{1\}$ if $i \in I \setminus J$. Since by the factorization theorem, each conjugation class in A^* intersects some F_i, we have that L is the closure under conjugation of $\bigcup_{j \in J} F_j$. This ends the proof of Theorem 2.2.

Note that Theorem 2.2 extends the characterization of *sofic* languages in [2] and the proof of Theorem 2.1 extends their formula for the zeta function of the sofic system associated to a finite circular code.

3. RELATIONS

We call *rational relation* on A^* a binary relation on A^* whose graph is a rational subset of the product monoid $A^* \times A^*$; rational subsets of a monoid are defined similarly to rational languages. If R is an equivalence relation on a subset of A^* (the *domain* of R), we say that it is *cyclic* if:

(i) equivalent words mod. R have the same length;

(ii) viewing R as a subset of the free monoid $(A \times A)^*$, it is cyclic.

Call *pattern* of a periodic element $x \in A^{\mathbf{Z}}$ a word in A^+ of the form $x_{i+1} \cdots x_{i+p}$, for some period $p \geq 1$ of x and some integer i (we denote by A^+ the set $A^* \setminus 1$, which is the free semigroup on A). If L is a cyclic language, let $S(L)$ denote the set of periodic elements in $A^{\mathbf{Z}}$ whose patterns lie in L. Then $|L \cap A^n|$ = number of elements in $S(L)$ having n as a period = number of elements in $S(L)$ which are fixpoints of σ^n, where σ is the *shift* mapping, $\sigma(x) = y$, with $y_i = x_{i+1}$.

Thus the zeta function of a cyclic language is the zeta function of the (abstract) dynamical system $(S(L), \sigma)$, that is, the series

$$\exp\left(\sum_{n \geq 1} (\textit{number of fixpoints of } \sigma^n) \frac{t^n}{n} \right).$$

We define the *zeta function* of a cyclic relation R in a similar way; note that the domain of R is a cyclic language L. Define an equivalence relation $S(R)$ on $S(L)$ by: $x \equiv y \bmod S(R)$ if each pattern of the periodic element (x, y), viewed as an element of $(A \times A)^{\mathbf{Z}}$, is in R.

Let us describe more precisely this equivalence relation. For a nonempty word w, take the notation $w^\infty = \cdots www \cdots www \cdots \in A^{\mathbf{Z}}$, with the first letter of w in position 0. Then for $u, v \in L$, we have $u^\infty \equiv v^\infty \bmod S(R)$ if and only if for all words u', v' of equal length with $u^\infty = u'^\infty$ and $v^\infty = v'^\infty$, one has $u' \equiv v' \bmod R$. Note that by cyclicity of R, this is also equivalent to $u^i \equiv v^j \bmod R$ for some $i, j \geq 1$ (or equivalently for all i, j with $il(u) = jl(v)$).

The relation $S(R)$ is an equivalence relation, compatible with σ, so that $S(L)/S(R)$ inherits the mapping σ. The zeta function of the dynamical system $(S(L)/S(R), \sigma)$ is $\exp(\sum_{n \geq 1} a_n t^n/n)$, where a_n is the number of fixed points of σ^n in $S(L)/S(R)$. This series is by definition the *zeta function* $\zeta(R)$ of the cyclic relation R. Note that this extends the definition of Section 2, since when $R =$ identity relation on a cyclic language L, then $\zeta(L) = \zeta(R)$.

We describe the fixed points of σ^n in $S(L)/S(R)$. A class $w^\infty \bmod S(R)$, where w is a word of length $\geq n$ (this does not restrict generality, since one may replace w by some power), is a fixpoint of σ^n if and only if $w = uv$, $l(u) = n$, and $uv \equiv vu \bmod R$.

THEOREM 3.1. *The zeta function of a cyclic rational relation on A* with equivalence classes of bounded cardinality is* **N***-rational.*

The proof will be done in several steps. First, we prove it for special relations, defined by the action of a finite group, then we show that in the general case, the zeta function is a product of zeta functions of this special case.

As the proof will show, the ordinary generating function $\sum_{n \geq 1} a_n t^n$ is also **N**-rational.

THEOREM 3.2. *Let a finite group G act on a finite set A and extend this action to automorphisms of A*. Let L be a rational cyclic language closed under this group action and let R be the cyclic equivalence relation on L defined by this group action. Then the zeta function of R is* **N***-rational.*

Observe that the set $S(L)/S(R)$ is the set of orbits of $S(L)$ under the natural action of G on $A^{\mathbf{Z}}$. We denote it also by $S(L)/G$ and consider more generally $S(A^*)/G$ and $A^{\mathbf{Z}}/G$.

We need a result describing periodic elements in $A^{\mathbf{Z}}/G$; it uses itself an elementary lemma on permutation groups which will be proved in the Appendix.

LEMMA 3.3. *An element x in $A^{\mathbf{Z}}/G$ has n as a period if and only if it is of the form*

$$\cdots (g^{-2}w)(g^{-2}w)\cdot w(gw)(g^2w)\cdots$$

(*where position* 0 *is at the right of the dot*) *for some $g \in G$ and some $w \in A^n$. There are $|G|$ such couples (g,w) representing x.*

Proof. Let $x \in A^{\mathbf{Z}}$ be a fixpoint of $\sigma^n \bmod G$. Then we may write $x = \cdots w_{-2}w_{-1}\cdot w_0 w_1 \cdots$, with each word w_i of length n. Then

$$\sigma^n(x) = \cdots w_{-2}w_{-1}w_0 \cdot w_1 \cdots,$$

so that there exists $g \in G$ sending the first element onto the second, that is, $w_{i+1} = gw_i$ for any integer i. By putting $w = w_0$, we find that x is of the required form. The converse is similar.

Let G act on A^n; observe that the element of $A^{\mathbf{Z}}/G$ defined by (g,w) depends only on the cycle defined by the mapping u of Lemma 5.1, with A^n in place of A. Hence, the latter implies the lemma.

Proof of Theorem 3.2. Let $B = G \times A$. Define the function $f\colon B^* \to A^*$ by

$$f((g_1,a_1)\cdots(g_n,a_n)) = (g_1a_1)(g_1g_2a_2)\cdots(g_1\cdots g_na_n).$$

Define also the function $\theta\colon B^+ \to S(A^*)/G$ by

$$\theta(w) = \left(f(w)gf(w)\cdots g^{k-1}f(w)\right)^{\infty} \bmod G$$

where $w = (g_1,a_1)\cdots(g_n,a_n)$, $g = g_1\cdots g_n$, and k is the order of g in G. Note that each element in $S(A^*)/G$ of period n has exactly $|G|^n$ preimages of length n under θ: this is because we have by Lemma 3.3 $|G|$ choices for the couple $(g, f(w))$, then $|G|^{n-1}$ choices for w, the product $g = g_1\cdots g_n$ being already chosen.

Let $L' = \{w \in A^* \mid \theta(w) \in S(L)/G\}$. We show that L' is a rational cyclic language. This will imply by Theorem 2.1 that

$$\exp\left(\sum_{n\geq 1} |G|^n \times \textit{number of points in } S(L)/G \textit{ of period } n \times t^n/n\right)$$

is $\mathbf{N}$-rational. Hence the zeta function of R, obtained from the previous one by replacing t by $t/|G|$, is $\mathbf{Q}_+$-rational. Thus by a theorem of Fliess [15], it is $\mathbf{N}$-rational.

Let w be as above, $w' = (g_2,a_2)\cdots(g_n,a_n)(g_1,a_1)$, $g' = g_2\cdots g_ng_1$, and note that k is also the order of g'. Then

$$\sigma(\theta(w)) = g_1\theta(w'),$$

which shows that L' is cyclic, $S(L)$ being closed under σ and the action of G. Furthermore,

$$\theta(w^p) = \theta(w).$$

Hence L' is cyclic.

Define the *sign* of w to be $\mathrm{sgn}(w) = g$ and let

$$L_g = \{x \in A^* \mid x(gx) \cdots (g^{k-1}x) \in L\}.$$

With the notations of Eq. (1), we have

$$L_g = \bigcup_{m_1, \ldots, m_k} \mu^{-1}(m_1) \cap (\mu \circ g)^{-1}(m_2) \cap \cdots \cap (\mu \circ g^{k-1})^{-1}(m_k),$$

where the m_i in M are subject to $m_1 \cdots m_k \in P$, and where g is considered as an element of $\mathrm{Aut}(A^*)$. This shows that L_g is a rational language. Now, we have

$$L' = \bigcup_{g \in G} \{w \in B^* \mid \mathrm{sgn}(w) = g \text{ and } f(w) \in L_g\}.$$

The function f is *rational*, that is, its graph is a rational subset of the monoid $B^* \times A^*$; actually it is even sequential. Hence f^{-1} preserves rationality of languages (see [4, Cor. III.4.2]). Since $\{w \mid \mathrm{sgn}(w) = g\}$ is clearly rational, we obtain that L' is rational. This ends the proof of Theorem 3.2.

Proof of Theorem 3.1. By assumption, each class mod.R has at most r elements.

1. Suppose first that the following property holds: each nonempty word in $L = \mathrm{dom}(R)$ has a power whose class has r elements. Let $B = A^r$ and consider the following language on B^* (we view a word in B^* as an r-tuple of words of equal length in A^*):

$$L' = \{(u_1, \ldots, u_r) \in B^* \mid \{u_1, \ldots, u_r\} \textit{ is the class } \mathrm{mod}.R \textit{ of } x \in L\}.$$

Then L' is a rational cyclic language. Furthermore, the symmetric group S_r acts naturally on B^*, and L' is closed under this action; define the equivalence relation R' on L' by $u \equiv v \bmod R'$ if $gu = v$ for some $g \in S_r$. By Theorem 3.2, the zeta function of R' is **N**-rational.

We show that it is equal to the zeta function of R. Indeed, define a mapping f: $S(L)/S(R) \to S(L')/S(R')$ by letting $s = x^\infty \in S(L)$, with $x \in L$; we may suppose that the class mod.R of x has r elements and we define $f(s) =$ image of $(u_1, \ldots, u_r)^\infty$ in $S(L')/S(R')$, where the class of

x mod.R is $\{u_1, \ldots, u_r\}$, the order of the u_i being immaterial by definition of $S(R')$. This is well defined, since if $t = y^\infty$ ($y \in L$) and $s \equiv t$ mod.$S(R)$, then $x^i \equiv y^j$ mod.R for some $i, j \geq 1$ with $il(x) = jl(y)$. By cyclicity of R, the class of x^i is $\{u_1^i, \ldots, u_r^i\}$, which is therefore that of y^j. Hence, the class of y is $\{v_1, \ldots, v_r\}$, with $v_k^j = u_k^i$, hence $f(s) = (u_1, \ldots, u_r)^\infty \equiv (v_1, \ldots, v_r)^\infty = f(t)$mod.$S(R')$.

Suppose now that $f(x^\infty) = f(y^\infty)$; then, the classes of x and y being as above, we have $(u_1, \ldots, u_r)^\infty \equiv (v_1, \ldots, v_r)^\infty$ mod.$S(R')$. Then $(u_1, \ldots, u_r)^i = (v_{g1}, \ldots, v_{gr})^j$, for some $i, j \geq 1$, hence $\{u_1^i, \ldots, u_r^i\} = \{v_1^j, \ldots, v_r^j\}$. In particular, $x^i \equiv y^j$ mod.R. Thus $x^\infty = y^\infty$ mod.$S(R)$ and f is injective.

Now, let $(u_1, \ldots, u_r) \in L'$. Then $\{u_1, \ldots, u_r\}$ is the class mod.R of some x in L. Hence f is surjective.

Finally, f commutes with the shift, which implies that R and R' have the same zeta function.

2. In the general case, let L_i be the set of words whose class mod.R has i elements. By assumption, $L_i = \varnothing$ for $i > r$. By [12, Prop. IX.8.3], each L_i is a rational language. Moreover, L_r is conjugation-closed and contains w^n for each w in L_r and $n \geq 1$; hence, by [5, Prop. 3], the cyclic closure K of L_r is a cyclic rational language, which is closed also for R. The zeta function of R is the product of the zeta function of $R \mid K$ and of $R \mid (L \setminus K)$ (L is the domain of R), since $S(L)/S(R)$ has the corresponding partition, whose two blocks are closed under the shift. Now, the restriction of R to a cyclic rational language is a cyclic rational relation, by [12, Theorem IX.4.1]. Therefore, the first zeta function above is $\mathbf{N}$-rational by Part 1, and the second by induction on r (the case $r = 1$ being the case of cyclic languages).

4. APPLICATIONS

4.1. *Finitely Presented Dynamical Systems*

A *dynamical system* is a double (Ω, f), where Ω is a compact topological space and f is a homeomorphism $\Omega \to \Omega$. It is a *subshift of finite type* if f is the restriction to Ω of the shift in $A^{\mathbf{Z}}$, with A finite and discrete and $A^{\mathbf{Z}}$ equipped with the product topology, and if Ω is of the following form: there exists an integer N and a set F of words of length N in A^* such that an element $x \in A^{\mathbf{Z}}$ is in Ω if and only if all its factors of length N (that is, all the words $x_{i+1} \cdots x_{i+N}$) are in F (see [8, Chap. 2] for definitions and results concerning this section).

More generally, following Gromov [19, 8.4.B] and Fried [18], a dynamical system (Ω, f) is called *finitely presented* if it is the quotient of a system of finite type by an equivalence relation which, when viewed as a subset of

$(A \times A)^{\mathbf{Z}}$, is itself a system of finite type. By theorem of Fried [18], (Ω, f) has always a finite presentation which is *finite-to-one*, that is, the fibers of the quotient map have bounded cardinality.

It is the notion of finitely presented system which motivated our definition of cyclic rational relations. Indeed, since the set of words in A^* whose factors of length N are in F is a rational language, Theorem 3.1 implies the following result.

THEOREM 4.1. *The zeta function of a finitely presented dynamical system is* **N***-rational.*

As for Theorem 3.1, the ordinary generating function, that is, $\sum_{n \geq 1} a_n t^n$ (with a_n = number of points of period n), is also **N**-rational.

Proof. Let (Ω, f) be a dynamical system of finite type. Then there exists a finite set A, an integer N, sets F and G of words of length N in A^*, and $(A \times A)^*$ respectively, and a continuous mapping h from S onto Ω such that $h \circ \sigma = f \circ h$, with S = set of elements in $A^{\mathbf{Z}}$ whose factors of length N are in F, and $T = \{(x, y) \in A^{\mathbf{Z}} \times A^{\mathbf{Z}} \mid h(x) = h(y)\}$ = set of elements in $(A \times A)^{\mathbf{Z}}$ whose factors of length N are in G. Moreover, we may suppose that h is finite-to-one. Then it is well known that the set of periodic elements in Ω is the image under h of the set of periodic elements in S. Let L (resp. R) be the set of patterns of S (resp. T). Then L and R are cyclic languages in A^* and $(A \times A)^*$ respectively. Moreover, they are rational, since L (resp. R) is the set of words in A^* (resp. $(A \times A)^*$) whose factors of length N (even cyclically) are in F (resp. G). Next, $S(L)$ (resp. $S(R)$) is the set of periodic elements in S (resp. T) and $S(L)/S(R)$ is identified with the set of periodic elements in (Ω, f). Hence the zeta function of (Ω, f) is equal to that of R and is **N**-rational by Theorem 3.1 since the classes of R have bounded cardinality.

4.2. *Hyperbolic Groups*

The result of the previous section may be slightly extended, and this has a consequence for hyperbolic groups à la Gromov. Indeed, following [19, p. 250], call the dynamical system (Ω, f) *sub-Markov* if it is the quotient of a subshift of finite type S of $A^{\mathbf{Z}}$ by an equivalence relation T, which is compatible with the shift σ on $A^{\mathbf{Z}}$, and which when viewed as a subset of $(A \times A)^{\mathbf{Z}}$ has the following property: there exists a subshift of finite type T_0 of $(A \times A)^{\mathbf{Z}}$ and an integer i_0 such that $T \subset T_0 \subset \bigcup_{i=0,\ldots,i_0} (\mathrm{id} \times \sigma^i)(T)$, where σ is as usual the shift mapping.

THEOREM 4.2. *The zeta function of a sub-Markov dynamical system, such that the classes of the corresponding equivalence relation have bounded cardinality, is* **N***-rational.*

This extends Theorem 8.5.U of [18].

Proof. Define L and R as in the proof of Theorem 4.1. Moreover, let $R_0 \subset (A \times A)^*$ be the language of patterns of T_0. Then we have $R \subset R_0 \subset \bigcup_{i=0,\dots,i_0} (\mathrm{id} \times \sigma^i)(R)$, where σ acts on finite words by $\sigma(aw) = wa$ if $w \in A^*$ and $a \in A$. Moreover, the classes of R have at most r elements.

We show that R is a rational relation, evidently cyclic. Note that if $u \equiv v \bmod.R$ and if $\sigma^j(v) = v$, then $\sigma^k(u) = u$ for some $k \leq jr$. Indeed, since R is cyclic, it is compatible with σ, hence σ^j induces a bijection of the class $\bmod.R$ of v into itself, hence some power $\leq r$ of σ^j sends u onto itself.

The latter observation implies that if $u \equiv v \bmod.R$ and if v has a small period (which is the smallest $p \geq 1$ such that $\sigma^p(v) = v$), then u also has a small period. Let R' be the set of (u, v) in R such that the period of v is greater than ri_0^2. It is enough to show that R' is rational, since it differs from R by a set which is a finite union of $(u, v)^*$.

We show that

$$R' = \{(u,v) \in R_0 \mid \mathit{period}(v) > ri_0^2 \text{ and } (u, \sigma^{-i}(v)) \notin R_0 \text{ for } i = 1, \dots, i_0\}.$$

Indeed, if (u, v) is in the right-hand side, then $(u, \sigma^{-i}(v))$ is in R, hence in R_0, for some $i = 0, \dots, i_0$; so we must have $i = 0$ and (u, v) is in R, hence in R'. Conversely, if $(u, v) \in R'$, then $(u, v) \in R_0$; if we had $(u, \sigma^{-i}(v)) \in R_0$ for some $i = 1, \dots, i_0$, then $(u, \sigma^{-i-j}(v)) \in R$ for some $j = 0, \dots, i_0$, which implies $v \equiv \sigma^{i+j}(v) \bmod.R$, and finally that v has period $\leq ri_0^2$, which was excluded.

The previous equality shows that R' is rational. Thus R is rational, and we conclude that the zeta function of a sub-Markov system is **N**-rational.

Given a hyperbolic group Γ, call γ_1 and γ_2 *stably conjugate* if for some integer m, γ_1^m is conjugate to γ_2^m [19, 8.5.S]. Denote by $[\gamma]_{\mathrm{st}}$ the stable conjugation class of γ, let the *norm* of this class be $|[\gamma]_{\mathrm{st}}| = \inf_{\gamma' \in [\gamma]_{\mathrm{st}}} |\gamma'|$, where $|\gamma'|$ is the length function in Γ. Moreover, let the *stable norm* of this class be $\|[\gamma]\|_- = \liminf_{n \to \infty} n^{-1} |[\gamma^n]_{st}|$. It is known that $\|[\gamma]\|_- = m_0^{-1} |[\gamma^{m_0}]_{\mathrm{st}}|$ for some m_0 depending only on Γ. Let $p(\gamma)$ be the *exponent* of γ, that is the greatest p such that γ is a pth power and let the *stable exponent* of γ be the number $p[\gamma]_{\mathrm{st}} = \liminf_{i \to \infty} i^{-1} p(\gamma^i)$ (which is an integer). Now define $[N_k]_{\mathrm{st}} = \sum p^{-1}(\gamma) \|[\gamma]\|_-$, where the sum is over all stable conjugation classes of nontorsion elements in Γ whose stable norm is equal to k/m_0 (see [19, 5.2.C and 8.5.S-W]).

COROLLARY 4.3. *The series* $\exp(\sum_k k^{-1} [N_k]_{\mathrm{st}} t^k)$ *is* **N**-*rational.*

Indeed, this is a consequence of the previous theorem and of the last sentence p. 250 in [19]. It seems likely that the same result is true for the series considered in [19, 5.2.D and 8.4.X]. Note that in the case of the free group on n generators, the series of the corollary and of [19, 5.2.D]

coincide, and turn out to be the zeta function of the rational cyclic language of cyclically reduced words in the free group; it is equal to $((1-(2n-1)t)(1+t)^{n-1}(1-t)^n)^{-1}$ (thanks to A. Garsia's and J.-M. Fedou's calculations).

4.3. *Constructible Sets*

As told in the Introduction, the zeta function of a smooth algebraic projective variety over a finite field is **N**-rational. The theorem of Dwork actually tells that the zeta function of each algebraic set is rational, so that the same is true for the difference of two algebraic sets (the zeta function is the corresponding quotient of the zeta functions) and consequently for each constructible set (that is, a boolean combination of algebraic sets), since such a set is a disjoint union of locally closed subsets, and since each locally closed subset is the difference of two algebraic sets. It seems likely that the zeta function of a constructible set is even **N**-rational. This will be certainly true for the complement of a smooth algebraic projective variety.

Similarly, let us call *constructible* each subspace of a dynamical system of finite type, which is a boolean combination (using union and complementation) of closed finitely presented subsystems of the given system. Then it is likely that the zeta function of this subspace (defined by the usual series on the number of fixpoints) is **N**-rational. This conjecture is supported by the following result.

THEOREM 4.4. *Let* Ω *be a boolean combination of sofic subsystems of* $A^{\mathbf{Z}}$. *Let* a_n = *number of points in* Ω *of period* n. *Then* $\exp(\sum_{n\geq 1} a_n t^n/n)$ *is* **N**-*rational*.

Proof. Let Ω be a shift-closed subset of $A^{\mathbf{Z}}$ and $L(\Omega)$ the cyclic language consisting in the set of patterns of Ω. Then the zeta function of Ω is equal to that of $L(\Omega)$, and the mapping $\Omega \mapsto L(\Omega)$ preserves boolean combinations. Since, rational cyclic languages are closed under boolean combinations, and since $L(\Omega)$ is rational cyclic for a sofic system Ω [5, Prop. 3], the theorem follows from Theorem 2.1.

4.4. *Combinatorial Interpretation*

The property of **N**-rationality of a zeta function suggests that there is a combinatorial interpretation of this fact: that is, there is some (canonical) rational language associated to the given mathematical object (dynamical system, algebraic variety, ...) whose generating function is the zeta function of the object, or, more generally, instead of a language, an *unambiguous* rational subset of a graded monoid, whose generating function has this property; recall that an unambiguous rational subset of a monoid is a rational subset such that the rational operations are multiplicity-free (see

[13] or [12, VII.8] for the exact definition), then its generating series is **N**-rational.

We give such an interpretation in the particular case of dynamical system which are subshifts of finite type. Such a system may be viewed as the set of bi-infinite paths of some directed graph, and its zeta function is by the Bowen–Lanford formula [6] equal to $\det(1 - tM)^{-1}$, where M is the incidence matrix of the graph. Furthermore, this series is, according to the Cartier–Foata theory of Möbius functions [7], equal to the generating function of some free partially commutative monoid determined by the graph (more precisely, the generators are the conjugation classes of simple closed paths of the graph, the cycles say, and two cycles commute if they have no vertex in common; the degree of a cycle is the number of vertices on it). Finally, by the Cartier–Foata normal form, this monoid is an unambiguous rational subset of itself (see Prop. 1.3.6 in [15], proof attributed to E. Sontag). See [17] for a direct combinatorial proof for the equality of the zeta function and the generating function of the previous monoid.

For subshifts of finite type, another combinatorial interpretation (and hence proof of **N**-rationality of the zeta function) was indicated to us by Béal, by the use of the formula p. 98 and Prop. 4.5 in [1].

4.5. *N-Rational Functions and Zeta Functions*

According to Berstel's theorem [3], a necessary condition for a rational series to be **N**-rational is that if r is the minimum modulus of its poles, then r is itself a pole, and all other poles of the same modulus are of the form ϵr for some root of unity ϵ. This result, which is related to the Perron–Frobenius theorem on positive matrices, implies among other properties a good asymptotic behaviour of the a_n.

Conversely, a theorem of Soittola [27] and Katayama *et al*. [20] asserts that if a rational series with coefficients in **N** has a unique pole of minimal modulus, then it is **N**-rational.

These results allow us to give a complete characterization of **N**-rational series: a series $\sum_n b_n t^n$ is **N**-rational if and only if for some p, and for each $i = 0, \ldots, p - 1$, the series $\sum_n b_{i+pn} t^n$ is rational, has coefficients in **N**, and has a unique pole of minimal modulus; see [24] for this and related questions.

Two questions arise from the present article, which could perhaps be solved using this characterization: Let $g = \sum_{n \geq 1} a_n t^n$ and $\zeta = \exp(\sum_{n \geq 1} a_n t^n / n)$, where the coefficients a_n are nonnegative integers (series like g and ζ are said to satisfy the *Spitzer identity* in [7, Chap. VII], where also are given two results where this happens, in representation and probability theory).

(i) If g is **N**-rational and ζ is rational, is ζ necessarily **N**-rational? This would give another proof of Theorem 2.1, by using also [5].

(ii) If ζ is **N**-rational, then classically (by logarithmic derivation), g is rational; is g necessarily **N**-rational? A stronger property would be that ζ is then the zeta function of some rational cyclic language.

APPENDIX: A LEMMA ON PERMUTATION GROUPS

Let a finite group G act on a finite set A. Call the *cycle* of this action a *circular word* $(a_1, a_2, \dots, a_k)$, which is a cycle of some permutation of A induced by the action of G; recall that a circular word is an equivalence class of words under conjugation. We call k the *length* of the cycle, and the set $\{a_1, a_2, \dots, a_k\}$ its *orbit*. We say that two cycles $(a_1, a_2, \dots, a_k)$ and $(b_1, b_2, \dots, b_k)$ are *conjugate* if, for some $g \in G$, one has $b_i = ga_i$, for $i = 1, \dots, k$. Note that, when $k \geq 2$, a cycle is a usual cycle in the symmetric group S_A and that we distinguish the cycles of length 1, that is, the fixpoints of the action of G; furthermore, conjugation of cycles is the usual conjugation of permutations in S_A, but under elements of G.

LEMMA A.1. (i) *There are $|A|$ conjugation classes of cycles.*

(ii) *Denote by C the set of cycles and define a mapping u: $G \times A \to C/G$, $(g, a) \mapsto$ conjugation class of the cycle $(a, ga, g^2a, \dots)$. Each fiber of this mapping has $|G|$ elements.*

Proof. For each cycle $c \in C$, let $g_c \in G$ be a fixed element having the cycle c in its cycle decomposition. Also, let G_c be the subgroup of G fixing each point of the orbit $o(c)$ of c.

One has $(a, ga, g^2a, \dots) = c$ if and only if $a \in o(c)$ and $g \in g_c G_c$. Thus we find that there are $l(c)|G_c|$ solutions $(g, a) \in G \times A$ to the previous equality, for fixed c.

Note that if $c' \in C$ and that the previous equation also holds with c', then the orbits of c and c' intersect (they contain a), hence are equal. So the equation above can hold only for one c.

Thus, if we let c vary in its conjugation class under G, we find $|\text{class}(c)|l(c)|G_c|$ solutions to this equality, since $l(c)$ and $|G_c|$ depend only on the class of c. Hence this number is the cardinality of the inverse image under u of class(c) and we must show that it is equal to $|G|$. Equivalently, we show that $|\text{stab}(c)| = |l(c)|G_c|$, where stab$(c)$ is the stabilizer of c in G under conjugation.

Now, recall that in S_A, a cycle c of length k commutes with a permutation g if and only if the restriction of g to the orbit of c is of the form c^i, for some $i = 1, \dots, k$.

Hence, an element g of G fixes the cycle $c \in C$ if and only if g is in the set $\bigcup_{i=1}^{l(c)} g_c^i G_c$. Note that this union is disjoint, so that there are $l(c)|G_c|$ elements in $\mathrm{stab}(c)$, as was to be shown.

This proves (ii), and (i) follows, since u is surjective.

ACKNOWLEDGMENTS

The author is grateful to M.-P. Béal, J. Berstel, M. Coornaert, P. Libbrecht, and S. Poirier for many discussions and correspondence during this work.

REFERENCES

1. M.-P. Béal, Puissance extérieure d'un automate déterministe, application au calcul de la fonction zêta d'un système sofique, *RAIRO Inform. Théorique et Appl.* **29** (1995), 85–103.
2. M.-P. Béal and D. Perrin, Une caractérisation des ensembles sofiques, *Compt. Rend. Acad. Sci. Paris, Sér. A* **303** (1986), 255–257.
3. J. Berstel, Sur les pôles et le quotient d'Hadmard des séries **N**-rationnelles, *Compt. Rend. Acad. Sci. Paris, Sér. A* **272** (1971), 1079–1081.
4. J. Berstel, "Transductions and Context-Free Languages," Teubner, Stuttgart, 1979.
5. J. Berstel and C. Reutenauer, Zeta functions of formal languages, *Trans. Amer. Math. Soc.* **321** (1990), 533–546.
6. R. Bowen and O. Lanford, Zeta functions of restrictions of the shift transformation, *Proc. Symp. Pure Math.* **14** (1970), 907–918.
7. P. Cartier and D. Foata, Problèmes combinatoires de commutations et de réarrangements, Lecture Notes in Math., Vol. **85**, Springer-Verlag, Berlin, 1969.
8. M. Coornaert and A. Papadopoulos, "Symbolic Dynamics and Hyperbolic Groups," Lecture Notes in Math., Vol. **1539**, Springer-Verlag, New York/Berlin, 1993.
9. E. M. Coven and M. E. Paul, Sofic systems, *Israel J. Math.* **20** (1975), 165–177.
10. A. W. M. Dress and C. Siebeneicher, Symmetric powers of cyclic sets and the definition of A. Weil's zeta function, *Proc. Symp. Pure Math* **47** (1987).
11. A. W. M. Dress and C. Siebeneicher, The Burnside ring of the infinite cyclic group and its relations to the necklace algebra, λ-rings, and the universal ring of Witt vectors. *Adv. in Math.* **78** (1989), 1–41.
12. S. Eilenberg, "Automata, Languages, and Machines," Vol. **A**, Academic Press, New York, 1974.
13. S. Eilenberg and M. P. Schützenberger, *Rational sets in commutative monoids, J. Algebra* **13** (1969), 173–191.
14. D. B. A. Epstein, J. W. Cannon, D. F. Holt, S. V. F. Levy, M. S. Paterson, and W. P. Thurston, "Word Processing in Groups," Jones and Bartlett, 1992.
15. M. Fliess, Matrices de Hankel, *J. Maths. Pures Appl.* **53** (1974), 197–224.
16. M. Fliess, Séries rationnelles positives et processus stochastiques, *Ann. Inst. H. Poincaré Sect. B* **11** (1975), 1–21.
17. D. Foata, A combinatorial proof of Jacobi's identity, *Ann. Discrete Math.* **6** (1980), 125–135.
18. D. Fried, Finitely presented dynamical systems, *Ergodic Theory and Dynamical Systems* **7** (1987), 489–507.

19. M. Gromov, Hyperbolic groups, in *"Essays in Group Theory"* (S. M. Gersten, Ed.) MSRI publications, Springer-Verlag, New York/Berlin, 1987.
20. T. Katayama, M. Okamoto, and H. Enomoto, Characterization of the structure-generating functions of regular sets and DOL growth functions, *Inform. and Control* **36** (1978), 85–101.
21. G. Lallement, "Semigroups and Combinatorial Applications," Wiley, New York, 1979.
22. M. Lothaire, "Combinatorics on Words," Addison-Wesley, Reading, MA, 1983.
23. A. Manning, Axiom A diffeomorphisms have rational zeta functions, *Bull. London Math. Soc.* **3** (1971), 215–220.
24. D. Perrin, *On positive matrices, Theoret. Comput. Sci.* **94** (1992), 357–366.
25. M. P. Schützenberger, On the definition of a family of automata, *Inform. and Control* **4** (1961), 245–270.
26. M. P. Schützenberger, On a factorization of free monoids, *Proc. Amer. Math. Soc.* **16** (1965), 21–24.
27. M. Soittola, Positive rational sequences, *Theoret. Comput. Sci.* **2** (1976), 317–322.
28. V. A. Ufnarovskij, Combinatorial and asymptotic methods in algebra, *in* "Algebra VI" (A. I. Kostrikin and I. R. Shafarevitch, Eds.), Encyclopedia of Mathematical Sciences, Vol. **57**, Springer-Verlag, New York/Berlin, 1995.