Discrete Applied Mathematics 32 (1991) 141–153
North-Holland

On generalized zeta functions of formal languages and series

Juha Honkala

Department of Mathematics, University of Turku, 20500 Turku 50, Finland

Received 15 March 1989
Revised 5 October 1989

Abstract

Honkala, J., On generalized zeta functions of formal languages and series, Discrete Applied Mathematics 32 (1991) 141–153.

We study generalized zeta functions of formal languages and series. We give necessary conditions for the rationality of the generalized zeta function. We show that it is decidable whether or not the (generalized) zeta function of a $\mathbb{Q}$-algebraic series is a rational function. The same question is shown to be undecidable for context-free languages.

1. Introduction

The zeta functions and generalized zeta functions of formal languages and power series were defined by Berstel and Reutenauer in [2]. The connections of zeta functions range from abstract to more concrete. Zeta functions can be used to study combinatorial properties of languages. On the other hand, one of the reasons to study zeta functions of formal languages is to try to find a new proof to the celebrated theorem of Dwork, [3], stating that the zeta function of an algebraic variety over a finite field is rational.

The main result of Berstel and Reutenauer is that the (generalized) zeta function of a cyclic regular language is a rational function and can be computed effectively. By definition, a language is cyclic if it is closed under conjugation and if any two words having a nontrivial power in common either both or neither belong to the language. As a consequence of this result Berstel and Reutenauer show that the zeta function of a sofic system is rational.

In this paper we study generalized zeta functions of formal power series in non-

commuting variables having their coefficients in a subring of the field of real numbers. After some preliminary results we show that if the (generalized) zeta function of a series having coefficients in $\mathbb{Z}$ is rational then the power series expansion of the function has integer coefficients. As a consequence we derive necessary conditions for the rationality of the (generalized) zeta function of a language. Indeed, if the generalized zeta function of a language L is rational there exists a series s having a cyclic support such that the generalized zeta function of s equals the generalized zeta function of L. Furthermore, additional assumptions about the coefficients of s can be made. Also, if the generalized zeta function of L is rational, the commutative image of the characteristic series of L is obtained by a letter-to-letter morphism from the difference of the commutative images of the characteristic series of two cyclic languages. If the zeta function of a language L is rational then the generating function of L equals the difference of the generating functions of two cyclic languages. These results show that if the (generalized) zeta function of a language L is rational, then in a way the language L is not very far away from the cyclic languages.

In the last section we show that it is decidable whether or not the (generalized) zeta function of a $\mathbb{Q}$-algebraic series is a rational function. If it is rational it can be computed effectively. In the proof a deep decidability result due to Kuich and Salomaa, [6], is used. As a consequence, if G is a given unambiguous context-free grammar, it is decidable whether or not the (generalized) zeta function of the language generated by G is rational. The same question is shown to be undecidable for context-free grammars.

2. Definitions

We assume that the reader is familiar with the basic notions concerning formal languages and formal power series in noncommuting variables. To fix our terminology, however, we specify the following.

The free monoid generated by a finite alphabet X is denoted by X^*. In the sequel we always assume that $X=\{x_1, \ldots, x_m\}$, where $m \geq 1$. If w belongs to X^*, the length of w is denoted by $\lg(w)$. If A is a semiring, the semiring of formal power series with noncommuting variables in X and coefficients in A is denoted by $A\langle\langle X^*\rangle\rangle$. If r belongs to $A\langle\langle X^*\rangle\rangle$, we use the notations

$$r = \sum_{w \in X^*} (r, w)\, w \quad \text{and} \quad r_n = \sum_{\lg(w)=n} (r, w)\, w$$

where $n \geq 0$. The characteristic series of a language $L \subseteq X^*$ is defined by

$$\operatorname{char}(L) = \sum_{w \in L} w.$$

The subsemiring of $A\langle\langle X^*\rangle\rangle$ consisting of the polynomials is denoted by $A\langle X^*\rangle$.

If A is a ring, $A[X]$ denotes the ring of polynomials in m (commuting) variables. If A is a field, the quotient field of $A[X]$ is denoted by $A(X)$.

The canonical morphism from X^* to the free commutative monoid generated by X is denoted by c. Accordingly, the free commutative monoid generated by X is denoted by $c(X^*)$. The semiring of formal power series with commuting variables in X and coefficients in A is denoted by $A\langle\langle c(X^*)\rangle\rangle$. The morphism c is extended in a natural way to a morphism

$$c: A\langle\langle X^*\rangle\rangle \to A\langle\langle c(X^*)\rangle\rangle.$$

In the sequel we always assume that A is a subsemiring of the field of real numbers. Whenever we consider a formal series $r \in A\langle\langle X^*\rangle\rangle$, we tacitly assume that there exists a constant M such that

$$\left| \sum_{c(w)=u} (r, w) \right| \leq M^{\lg(u)+1} \tag{1}$$

for any $u \in c(X^*)$. This will guarantee that all series under consideration define a real function of real variables.

The following definition is due to Berstel and Reutenauer [2].

Definition 2.1. Suppose $r \in A\langle\langle X^*\rangle\rangle$. The *generalized zeta function* $Z(r)$ of r is defined by

$$Z(r) = \exp\left(\sum_{n \geq 1} \frac{1}{n} c(r_n) \right).$$

The *zeta function* $\zeta(r)$ of r is defined by

$$\zeta(r) = \exp\left(\sum_{n \geq 1} \frac{1}{n} \left(\sum_{\lg(w)=n} (r, w) \right) t^n \right).$$

If $L \subseteq X^*$ is a language, the generalized zeta function of L is defined by

$$Z(L) = Z(\mathrm{char}(L)).$$

Analogously, the zeta function $\zeta(L)$ of L is defined by

$$\zeta(L) = \zeta(\mathrm{char}(L)).$$

Clearly, if a_n is the number of words of length n in L, then

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

If $\theta: A\langle\langle c(X^*)\rangle\rangle \to A\langle\langle t^*\rangle\rangle$ (respectively $\theta: A\langle\langle X^*\rangle\rangle \to A\langle\langle t^*\rangle\rangle$) is the morphism which maps every letter of X to t, then

$$\zeta(r) = \theta(Z(r)) \qquad \text{(respectively } \zeta(r) = Z(\theta(r))\text{)}$$

and

$$\zeta(L) = \theta(Z(L)).$$

If $L \subseteq X^*$ is a language and the number of words of length n in L is a_n, the generating function $G(L)$ of L is defined by

$$G(L) = \sum_{n \geq 0} a_n t^n.$$

A language L is called cyclic if for any words u and v, and integer $n \geq 1$, the following conditions hold:

$$uv \in L \quad \text{if and only if} \quad vu \in L, \tag{2}$$

$$w \in L \quad \text{if and only if} \quad w^n \in L. \tag{3}$$

The main references on formal power series are [6, 1, 10]. For standard algebra we refer to [7].

Example 2.2. If L is a cyclic language, then

$$Z(L) = \prod \frac{1}{1 - c(w)}$$

where w goes over the primitive Lyndon words in L. In particular, $Z(L)$ has integer coefficients.

3. Preliminary results

Theorem 3.1. *Let $A \subseteq \mathbb{R}$ be a ring. Suppose $r \in A\langle\langle X^* \rangle\rangle$. If $Z(r)$ is a rational function, there exist polynomials $R(x_1, \ldots, x_m)$, $S(x_1, \ldots, x_m)$ in $A[X]$ such that*

$$Z(r) = \frac{R(x_1, \ldots, x_m)}{S(x_1, \ldots, x_m)} \text{ and } S(0, \ldots, 0) \neq 0.$$

Furthermore, still assuming the rationality of $Z(r)$, there exist polynomials $P(x_1, \ldots, x_m)$, $Q(x_1, \ldots, x_m)$ in $A[X]$ such that

$$c(r) = \frac{P(x_1, \ldots, x_m)}{Q(x_1, \ldots, x_m)} \text{ and } Q(0, \ldots, 0) \neq 0.$$

Proof. Suppose

$$Z(r) = \frac{R(x_1, \ldots, x_m)}{S(x_1, \ldots, x_m)}, \tag{4}$$

where $R(x_1, \ldots, x_m)$ and $S(x_1, \ldots, x_m)$ belong to $\mathbb{R}[X]$. Choose $\delta > 0$ such that (4) holds when

$$-\delta < x_i < \delta \quad \text{for } 1 \leq i \leq m.$$

Replace in (4) each x_i by $x_i y$, where y is a new variable. We obtain

$$\exp\left(\sum_{n \geq 1} \frac{1}{n} c(r_n) y^n \right) = \frac{R(x_1 y, \ldots, x_m y)}{S(x_1 y, \ldots, x_m y)}. \tag{5}$$

Equation (5) holds if

$$-2 < y < 2,$$

$$-\tfrac{1}{2}\delta < x_i < \tfrac{1}{2}\delta \quad \text{for } 1 \le i \le m.$$

Denote by B the field of fractions of A. Equation (5) implies that

$$\exp\left(\sum_{n\ge 1} \frac{1}{n} c(r_n)\, y^n\right) \in B[X]\langle\langle y^*\rangle\rangle$$

and

$$\exp\left(\sum_{n\ge 1} \frac{1}{n} c(r_n)\, y^n\right) \in \mathbb{R}(X)^{\mathrm{rat}}\langle\langle y^*\rangle\rangle.$$

Because $\mathbb{R}(X)$ is a Fatou extension of $B[X]$, we can without restriction suppose that $R(x_1, \ldots, x_m)$, $S(x_1, \ldots, x_m)$ belong to $A[X]$ and $S(0, \ldots, 0) \neq 0$. This proves the first claim. Equation (5) implies

$$\sum_{n\ge 1} \frac{1}{n} c(r_n)\, y^n = \ln|R(x_1 y, \ldots, x_m y)| - \ln|S(x_1 y, \ldots, x_m y)|$$

and

$$\sum_{n\ge 1} c(r_n)\, y^{n-1} = \frac{1}{R(x_1 y, \ldots, x_m y)} \cdot \frac{\partial R(x_1 y, \ldots, x_m y)}{\partial y} - \frac{1}{S(x_1 y, \ldots, x_m y)} \cdot \frac{\partial S(x_1 y, \ldots, x_m y)}{\partial y}.$$

The validity of the second claim is seen by substituting $y = 1$. □

Lemma 3.2. *Assume $r \in \mathbb{Z}\langle\langle X^*\rangle\rangle$. If $Z(r)$ is a rational function, then $c(r)$ belongs to $\mathbb{Z}^{\mathrm{rat}}\langle\langle c(X^*)\rangle\rangle$.*

Proof. By Theorem 3.1 there exist polynomials $P(x_1, \ldots, x_m)$, $Q(x_1, \ldots, x_m)$ in $\mathbb{Z}[X]$ such that

$$c(r) = \frac{P(x_1, \ldots, x_m)}{Q(x_1, \ldots, x_m)}. \tag{6}$$

Denote

$$G(r) = \sum_{n\ge 0} c(r_n)\, y^n.$$

By (6), $G(r)$ belongs to $\mathbb{Q}(X)^{\mathrm{rat}}\langle\langle y^*\rangle\rangle$. Because $G(r)$ belongs to $\mathbb{Z}[X]\langle\langle y^*\rangle\rangle$ and $\mathbb{Q}(X)$ is a Fatou extension of $\mathbb{Z}[X]$, the series $G(r)$ belongs to $\mathbb{Z}[X]^{\mathrm{rat}}\langle\langle y^*\rangle\rangle$. Therefore there exist polynomials $P_1(x_1, \ldots, x_m, y)$ and $Q_1(x_1, \ldots, x_m, y)$ in $\mathbb{Z}[x_1, \ldots, x_m, y]$ such that

$$G(r) = \frac{P_1(x_1, \ldots, x_m, y)}{1 + Q_1(x_1, \ldots, x_m, y)},$$

where $Q_1(0,\ldots,0)=0$ and the greatest common factor of the numerator and the denominator in $\mathbb{Z}[x_1,\ldots,x_m,y]$ is 1. By (6)

$$\frac{P_1(x_1,\ldots,x_m,y)}{1+Q_1(x_1,\ldots,x_m,y)}=\frac{P(x_1y,\ldots,x_my)}{Q(x_1y,\ldots,x_my)}.$$

Here $1+Q_1(x_1,\ldots,x_m,y)$ divides $Q(x_1y,\ldots,x_my)$ and $Q(0,\ldots,0)\neq 0$. This implies that $Q_1(x_1,\ldots,x_m,y)$ does not have nonzero terms of the form ay^k $(k\geq 0)$. The claim follows by substituting $y=1$. □

Lemma 3.3. *Suppose $A\subseteq\mathbb{R}$ is a unique factorization ring and $r\in A\langle\langle X^*\rangle\rangle$. Suppose*

$$Z(r)=\frac{R(x_1,\ldots,x_m)}{S(x_1,\ldots,x_m)} \tag{7}$$

and

$$c(r)=\frac{P(x_1,\ldots,x_m)}{Q(x_1,\ldots,x_m)}+(r,\varepsilon), \tag{8}$$

where $R(x_1,\ldots,x_m)$, $S(x_1,\ldots,x_m)$, $P(x_1,\ldots,x_m)$, $Q(x_1,\ldots,x_m)$ belong to $A[X]$. Furthermore, suppose that in (7) *and* (8) *the numerator and the denominator do not have a common factor in $A[X]$. Then any nonconstant irreducible factor of $R(x_1,\ldots,x_m)$ or $S(x_1,\ldots,x_m)$ divides $Q(x_1,\ldots,x_m)$ in $A[X]$. Furthermore, $Q(x_1,\ldots,x_m)$ does not have multiple factors.*

Proof. Choose $\delta>0$ such that (7) and (8) hold when $-\delta<x_i<\delta$ for $1\leq i\leq m$. Replace again each x_i by x_iy to obtain

$$\exp\left(\sum_{n\geq 1}\frac{1}{n}c(r_n)\,y^n\right)=\frac{R(x_1y,\ldots,x_my)}{S(x_1y,\ldots,x_my)} \tag{9}$$

and

$$\sum_{n\geq 1}c(r_n)\,y^n=\frac{P(x_1y,\ldots,x_my)}{Q(x_1y,\ldots,x_my)}. \tag{10}$$

These equations hold if

$$-2<y<2,$$

$$-\tfrac{1}{2}\delta<x_i<\tfrac{1}{2}\delta \quad \text{for } 1\leq i\leq m.$$

Equations (9) and (10) imply that

$$\frac{1}{y}\cdot\frac{P(x_1y,\ldots,x_my)}{Q(x_1y,\ldots,x_my)}=\frac{1}{R(x_1y,\ldots,x_my)}\cdot\frac{\partial R(x_1y,\ldots,x_my)}{\partial y}$$
$$-\frac{1}{S(x_1y,\ldots,x_my)}\cdot\frac{\partial S(x_1y,\ldots,x_my)}{\partial y}.$$

Substitute $y=1$ to obtain

$$\frac{P(x_1,\ldots,x_m)}{Q(x_1,\ldots,x_m)}=\frac{R_0(x_1,\ldots,x_m)}{R(x_1,\ldots,x_m)}-\frac{S_0(x_1,\ldots,x_m)}{S(x_1,\ldots,x_m)}, \tag{11}$$

where $R_0(x_1, \ldots, x_m)$ and $S_0(x_1, \ldots, x_m)$ belong to $A[X]$. Furthermore, if $R(x_1, \ldots, x_m)$ (respectively $S(x_1, \ldots, x_m)$) has a nonconstant irreducible factor $R_1(x_1, \ldots, x_m)$ with multiplicity e_1 (respectively $S_1(x_1, \ldots, x_m)$ with multiplicity f_1) then $R_0(x_1, \ldots, x_m)$ (respectively $S_0(x_1, \ldots, x_m)$) has the factor $R_1(x_1, \ldots, x_m)$ with multiplicity $e_1 - 1$ (respectively $S_1(x_1, \ldots, x_m)$ with multiplicity $f_1 - 1$) ($e_1 > 0$, $f_1 > 0$). This follows because neither $R(x_1, \ldots, x_m)$ nor $S(x_1, \ldots, x_m)$ has a factor with constant term equal to zero. (To see this substitute $x_1 = \cdots = x_m = 0$ in (7).) Equation (11) implies

$$\begin{aligned} &P(x_1, \ldots, x_m) R(x_1, \ldots, x_m) S(x_1, \ldots, x_m) \\ &\quad = Q(x_1, \ldots, x_m)[R_0(x_1, \ldots, x_m) S(x_1, \ldots, x_m) \\ &\qquad\qquad - R(x_1, \ldots, x_m) S_0(x_1, \ldots, x_m)]. \end{aligned}$$

This proves the claim. □

4. Necessary conditions for rationality

Theorem 4.1. *Assume $r \in \mathbb{Z}\langle\langle X^* \rangle\rangle$. If $Z(r)$ (respectively $\zeta(r)$) is rational, then $Z(r)$ (respectively $\zeta(r)$) belongs to $\mathbb{Z}^{\mathrm{rat}}\langle\langle c(X^*) \rangle\rangle$ (respectively $\mathbb{Z}^{\mathrm{rat}}\langle\langle t^* \rangle\rangle$) and, consequently, has integer coefficients.*

Proof. The claim concerning $Z(r)$ follows by Theorem 3.1, Lemma 3.2 and Lemma 3.3. This implies the claim concerning $\zeta(r)$ because $\zeta(r) = Z(\theta(r))$, where $\theta : \mathbb{Z}\langle\langle X^* \rangle\rangle \to \mathbb{Z}\langle\langle t^* \rangle\rangle$ maps every letter of X to t. □

Lemma 4.2. *Assume $r \in \mathbb{R}\langle\langle X^* \rangle\rangle$. Then the power series expansion of*

$$Z(r) = \exp\left(\sum_{n \geq 1} \frac{1}{n} c(r_n) \right)$$

has integer coefficients if and only if there exists a sequence (ϱ_n) $(n \geq 1)$ of homogeneous polynomials in $\mathbb{Z}[X]$ with the following properties:

(i) *for any n, $\varrho_n = 0$ or $\deg \varrho_n = n$;*

(ii) *if for every $k \geq 1$, $\varrho_k = \sum_{i=1}^{m_k} \varrho_{ki}$ where the ϱ_{ki} are monomials with disjoint supports, then*

$$c(r_n) = \sum_{k \mid n} \sum_{i=1}^{m_k} k(\varrho_{ki})^{n/k} \tag{12}$$

for each $n \geq 1$;

(iii) *for any n, $\mathrm{supp}(\varrho_n) \subseteq \{c(w) \mid w$ belongs to the cyclic closure of $\mathrm{supp}(r)\}$.*

Proof. The proof of the if-part is not needed in the sequel and is left to the reader.

For the proof of the only if-part suppose that $Z(r)$ has integer coefficients. Define the sequence (ϱ_n) $(n \geq 1)$ of polynomials in $\mathbb{R}[X]$ recursively by

$$\varrho_n = \frac{1}{n} \left(c(r_n) - \sum_{\substack{k \mid n \\ k \neq n}} \sum_{i=1}^{m_k} k(\varrho_{ki})^{n/k} \right).$$

Here, for each $k<n$, we have denoted $\varrho_k=\sum_{i=1}^{m_k}\varrho_{ki}$ where each ϱ_{ki} is a monomial and $\mathrm{supp}(\varrho_{ki_1})\neq\mathrm{supp}(\varrho_{ki_2})$ whenever $i_1\neq i_2$. This also defines recursively the monomials ϱ_{ni}, $1\leq i\leq m_n$, for each $n\geq 1$. By the definition, ϱ_n is a homogeneous polynomial and $\deg\varrho_n=n$ if $\varrho_n\neq 0$. We next show that each ϱ_n belongs to $\mathbb{Z}[X]$.

The polynomial $\varrho_1=c(r_1)$ belongs to $\mathbb{Z}[X]$ because $Z(r)=1+c(r_1)+\cdots$ where the unwritten terms have degree higher than one. Suppose inductively that $\varrho_1,\ldots,\varrho_s$ belong to $\mathbb{Z}[X]$. Then the series

$$Z(r)\cdot\prod_{k=1}^{s}\prod_{i=1}^{m_k}(1-\varrho_{ki})$$

has integer coefficients. On the other hand

$$\begin{aligned}
&Z(r)\cdot\prod_{k=1}^{s}\prod_{i=1}^{m_k}(1-\varrho_{ki})\\
&=\exp\left(\sum_{n\geq 1}\frac{1}{n}c(r_n)+\sum_{k=1}^{s}\sum_{i=1}^{m_k}\ln(1-\varrho_{ki})\right)\\
&=\exp\left(\sum_{n\geq 1}\frac{1}{n}c(r_n)-\sum_{k=1}^{s}\sum_{i=1}^{m_k}\sum_{n\geq 1}\frac{1}{n}(\varrho_{ki})^n\right)\\
&=\exp\left(\sum_{n\geq 1}\frac{1}{n}\left(c(r_n)-\sum_{\substack{k\mid n\\ k\leq s}}\sum_{i=1}^{m_k}k(\varrho_{ki})^{n/k}\right)\right)\\
&=\exp(\varrho_{s+1}+\cdots)=1+\varrho_{s+1}+\cdots.
\end{aligned}$$

(Here the unwritten terms have degree higher than $s+1$.) Therefore ϱ_{s+1} belongs to $\mathbb{Z}[X]$.

Equation (12) follows directly from the definition of the sequence (ϱ_n). Claim (iii) follows by an easy induction. □

Theorem 4.3. *Suppose that $L\subseteq X^*$ is a language and $Z(L)$ is rational. Then there exists a series $s\in\mathbb{Z}\langle\langle X^*\rangle\rangle$ such that the following conditions hold*:

(i) $(s,uv)=(s,vu)$ *and* $(s,u^n)=(s,u)^n$ *for any* $u,v\in X^*$ *and* $n\geq 1$;

(ii) $\mathrm{supp}(s)$ *is a cyclic language*;

(iii) *each word in* $\mathrm{supp}(s)$ *is commutatively equivalent to a word in the cyclic closure of* L;

(iv) $Z(L)=Z(s)$.

Proof. If $Z(L)$ is rational, it has integer coefficients by Theorem 4.1.

Denote $r=\mathrm{char}(L)$. By Lemma 4.2 there exist monomials ϱ_{ni} in $\mathbb{Z}[X]$ with disjoint supports such that

$$c(r_n)=\sum_{k\mid n}\sum_{i=1}^{m_k}k(\varrho_{ki})^{n/k}$$

and $\deg \varrho_{ni} = n$ or $\varrho_{ni} = 0$ ($n \geq 1$, $1 \leq i \leq m_n$). Furthermore, $\mathrm{supp}(\varrho_{ni})$ consists of the commutative image of a word in the cyclic closure of L.

It is easily seen that $(\varrho_{ni}, a^n) = 0$ when $n > 1$, $1 \leq i \leq m_n$ and $a \in X$. Therefore we can regard each ϱ_{ni}, $n > 1$, as a monomial in $\mathbb{Z}\langle X^* \rangle$ such that the support of ϱ_{ni} consists of a word of the form $x_1^{j_1} x_2^{j_2} \ldots x_m^{j_m}$ where at least two j differ from zero. (I.e., ϱ_{ni} is regarded as a monomial in noncommuting variables after it has been written in a canonical way.) This guarantees that

$$\mathrm{supp}(\varrho_{n_1 i_1}^{k_1}) \neq \mathrm{supp}(\varrho_{n_2 i_2}^{k_2}) \quad \text{or} \quad \mathrm{supp}(\varrho_{n_1 i_1}^{k_1}) = \mathrm{supp}(\varrho_{n_2 i_2}^{k_2}) = \emptyset$$

if $n_1 \neq n_2$ or $k_1 \neq k_2$ or if $n_1 = n_2$, and $i_1 \neq i_2$ ($k_1 > 0$, $k_2 > 0$).

Define the series s as follows:

$$(s, w_1 w^t w_2) = (\varrho_{ni}^{t+1}, w^{t+1})$$

if $t \geq 0$, $w_2 w_1 = w$ and w belongs to $\mathrm{supp}(\varrho_{ni})$. The other coefficients of s equal zero. Clearly $\mathrm{supp}(s)$ is closed under conjugation and $(s, uv) = (s, vu)$ for any $u, v \in X^*$. If $u \in \mathrm{supp}(s)$ and $p \geq 1$, we have $u^p \in \mathrm{supp}(s)$ and $(s, u^p) = (s, u)^p$. Suppose $u^j \in \mathrm{supp}(s)$ where $j \geq 1$ and u is primitive. Then there exist words $w, w_1, w_2 \in X^*$ such that $u^j = w_1 w^t w_2$, $w = w_2 w_1$ and $w \in \mathrm{supp}(\varrho_{ni})$ ($t \geq 0$, $n \geq 1$). Because w is primitive, u is a conjugate of w. Therefore u belongs to $\mathrm{supp}(s)$. This proves (i) and (ii). Claim (iii) follows from the definition of s and the assumption concerning the supports of the ϱ_{ni}. By the definition of s

$$c(s_n) = \sum_{k \mid n} \sum_{i=1}^{m_k} k c((\varrho_{ki})^{n/k}) = c(r_n).$$

Hence $Z(s) = Z(L)$. □

With the notation of Theorem 4.3, if $Z(L)$ is rational then

$$Z(L) = \prod \frac{1}{1 - (s, w) c(w)}$$

where w goes over the primitive Lyndon words. (Compare with Example 2.2.)

Theorem 4.4. *Suppose that $L \subseteq X^*$ is a language and $Z(L)$ is rational. Then there exist series $s^{(1)}, s^{(2)} \in \mathbb{N}\langle\langle X^* \rangle\rangle$ such that the conditions* (i), (ii) *and* (iii) *of Theorem* 4.3 *hold for $s^{(1)}$ and $s^{(2)}$, the supports of $s^{(1)}$ and $s^{(2)}$ are disjoint and, furthermore, $Z(L) = Z(s^{(1)} - s^{(2)})$.*

Proof. First prove the following modification of Lemma 4.2. If $r \in \mathbb{Z}\langle\langle X^* \rangle\rangle$ and $Z(r)$ has integer coefficients then there exist two sequences (ϱ_{ni}), (τ_{nj}) ($n \geq 1$, $1 \leq i \leq m_n$, $1 \leq j \leq m_n'$) of monomials in $\mathbb{N}\langle c(X^*) \rangle$ such that the ϱ_{ni} (respectively τ_{nj}) have disjoint supports and the following conditions hold:

(i) for any n and i, $\varrho_{ni} = 0$ or $\deg \varrho_{ni} = n$;

(ii) for any n and j, $\tau_{nj} = 0$ or $\deg \tau_{nj} = n$;

(iii) for any n, i and j, $\mathrm{supp}(\varrho_{ni}) \neq \mathrm{supp}(\tau_{nj})$;

(iv) $$c(r_n) = \sum_{k \mid n} \sum_{i=1}^{m_k} k(\varrho_{ki})^{n/k} - \sum_{k \mid n} \sum_{j=1}^{m'_k} k(\tau_{kj})^{n/k}$$

for any $n \geq 1$;

(v) for any n, i and j, the sets $\mathrm{supp}(\varrho_{ni})$ and $\mathrm{supp}(\tau_{nj})$ are contained in $\{c(w) \mid w$ belongs to the cyclic closure of $\mathrm{supp}(r)\}$.

Then continue as in the proof of Theorem 4.3. □

Theorem 4.5. *Suppose that $L \subseteq X^*$ is a language and $Z(L)$ is rational. Then there exist an alphabet Y, cyclic languages $L_1, L_2 \subseteq Y^*$ and a letter-to-letter morphism $h: Y^* \to X^*$ such that*

$$c(\mathrm{char}(L)) = h(c(\mathrm{char}(L_1)) - c(\mathrm{char}(L_2))).$$

Proof. First prove the following modification of Lemma 4.2. If $r \in \mathbb{Z}\langle\langle X^* \rangle\rangle$ and $Z(r)$ has integer coefficients then there exist two sequences (ϱ_{ni}), (τ_{nj}) $(n \geq 1,\ 1 \leq i \leq m_n,\ 1 \leq j \leq m'_n)$ of monomials in $c(X^*)$ such that the conditions (i)–(v) mentioned in the proof of Theorem 4.4 hold. Then continue as in the proof of Theorem 4.4. Notice that there exists a positive integer M such that m_n and m'_n are less than or equal to M^n for any n. The alphabet Y is chosen to contain M copies of each letter of X to guarantee that Y^* contains sufficiently many copies of each primitive Lyndon word in X^*. The morphism h maps every copy of $x \in X$ to x. □

Example 4.6. Define the series $t \in \mathbb{Z}\langle\langle \{x_1, x_2, x_3, x_4\}^* \rangle\rangle$ by

$$t = \sum_{\substack{n \geq 1 \\ 3 \text{ does not divide } n}} 12(x_1x_2x_3x_4)^n + \sum_{n \geq 1} 24(x_1x_2x_3x_4)^{6n}.$$

A straightforward computation shows that $Z(t)$ is rational. Clearly, there exists a language $L \subseteq \{x_1, \ldots, x_4\}^*$ such that $c(\mathrm{char}(L)) = c(t)$. We show that there does not exist a series $s \in \mathbb{Z}\langle\langle \{x_1, \ldots, x_4\}^* \rangle\rangle$ with nonnegative coefficients and cyclic support such that $Z(L) = Z(s)$. Suppose the contrary. We assume without loss of generality that $(s, \varepsilon) = 0$. Then $c(\mathrm{char}(L)) = c(s)$ and hence there exists a word w in $\mathrm{supp}(s)$ with $c(w) = c(x_1x_2x_3x_4)$. Because $\mathrm{supp}(s)$ is cyclic the word w^3 belongs to $\mathrm{supp}(s)$. This is impossible because L contains no word of length 12.

This shows that it cannot be supposed in Theorem 4.3 that the coefficients of s are nonnegative.

Example 4.7. In general, it cannot be assumed that $Y = X$ in Theorem 4.5. This can be seen by considering any language L commutatively equivalent to the series $\sum_{n \geq 1} 90(x_1x_2x_3)^{2n}$.

Theorem 4.1, [4, Lemma 3.1] and the proof of [4, Corollary 3.2] imply the following theorem.

Theorem 4.8. *Suppose that $L \subseteq X^*$ is a language. If $\zeta(L)$ is rational, then there exist two cyclic languages L_1 and L_2 such that*

$$G(L) = G(L_1) - G(L_2),$$

i.e., the generating function of L equals the difference of the generating functions of L_1 and L_2.

Theorems 4.3–4.5 and Theorem 4.8 can be generalized to series in $\mathbb{Z}\langle\langle X^*\rangle\rangle$ if certain additional assumptions are made.

Berstel and Reutenauer showed that $Z(L)$ and $\zeta(L)$ are rational if L is a cyclic recognizable language. Theorems 4.3, 4.5 and 4.8 show that if $Z(L)$ or $\zeta(L)$ is rational then L in a sense is not very far away from the cyclic languages.

5. Decidability of rationality

Theorem 5.1. *Given a $\mathbb{Q}$-algebraic series $r \in \mathbb{Q}^{\mathrm{alg}}\langle\langle X^*\rangle\rangle$ it is decidable whether or not $Z(r)$ is a rational function. If $Z(r)$ is rational it can be computed effectively.*

Proof. We decide first whether or not $c(r)$ belongs to $\mathbb{Q}^{\mathrm{rat}}\langle\langle c(X^*)\rangle\rangle$. This decision can be made effectively by Theorem 16.13 of Kuich and Salomaa [6]. If $c(r)$ does not belong to $\mathbb{Q}^{\mathrm{rat}}\langle\langle c(X^*)\rangle\rangle$, the function $Z(r)$ is not rational by Theorem 3.1. If $c(r)$ belongs to $\mathbb{Q}^{\mathrm{rat}}\langle\langle c(X^*)\rangle\rangle$, the decision procedure of Kuich and Salomaa effectively gives polynomials $P(x_1, \ldots, x_m)$, $Q(x_1, \ldots, x_m)$ in $\mathbb{Q}[X]$ such that

$$c(r) = \frac{P(x_1, \ldots, x_m)}{Q(x_1, \ldots, x_m)} + (r, \varepsilon)$$

and $Q(0, \ldots, 0) = 1$. Suppose that the greatest common factor of $P(x_1, \ldots, x_m)$ and $Q(x_1, \ldots, x_m)$ in $\mathbb{Q}[X]$ is 1.

Let

$$Q(x_1, \ldots, x_m) = Q_1(x_1, \ldots, x_m) \cdots Q_q(x_1, \ldots, x_m)$$

be the factorization of $Q(x_1, \ldots, x_m)$ into irreducible polynomials in $\mathbb{Q}[X]$. We assume that $Q_i(0, \ldots, 0) = 1$ for $1 \leq i \leq q$. This factorization can be obtained effectively. If $Q(x_1, \ldots, x_m)$ has a multiple factor, then $Z(r)$ is not rational by Lemma 3.3. Assume that $Q_{k_1}(x_1, \ldots, x_m) \neq Q_{k_2}(x_1, \ldots, x_m)$ if $k_1 \neq k_2$. By Lemma 3.3, $Z(r)$ is rational if and only if there exist integers $e_1, \ldots, e_q$ such that

$$Z(r) = Q_1(x_1, \ldots, x_m)^{e_1} \cdots Q_q(x_1, \ldots, x_m)^{e_q}. \tag{13}$$

A straightforward calculation shows that (13) holds if and only if

$$\frac{P(x_1 y, \ldots, x_m y)}{Q(x_1 y, \ldots, x_m y)}$$

$$= \sum_{i=1}^{q} e_i \cdot \frac{y}{Q_i(x_1 y, \ldots, x_m y)} \cdot \frac{\partial Q_i(x_1 y, \ldots, x_m y)}{\partial y}. \tag{14}$$

Denote

$$Q_j^*(x_1, \ldots, x_m) = \prod_{\substack{i=1 \\ i \neq j}}^{q} Q_i(x_1, \ldots, x_m).$$

The equation (14) implies that

$$P(x_1 y, \ldots, x_m y)$$

$$= \sum_{i=1}^{q} e_i Q_i^*(x_1 y, \ldots, x_m y)\, y \frac{\partial Q_i(x_1 y, \ldots, x_m y)}{\partial y}.$$

The comparison of the corresponding coefficients on both sides gives a system of linear equations in $e_1, \ldots, e_q$. From this system it can be decided whether or not there exist integers $e_1, \ldots, e_q$ such that (14) holds. (Clearly, the system has at most one solution in rationals.) If such integers $e_1, \ldots, e_q$ are found, $Z(r)$ is rational. Otherwise $Z(r)$ is not rational. □

Corollary 5.2. *Given a $\mathbb{Q}$-algebraic series $r \in \mathbb{Q}^{\text{alg}}\langle\langle X^* \rangle\rangle$ it is decidable whether or not $\zeta(r)$ is a rational function. If $\zeta(r)$ is rational it can be computed effectively.*

Proof. Let $\theta : X^* \to \{t\}^*$ be the morphism which maps every letter of X to t. By the closure properties of algebraic series, $\theta(r)$ belongs to $\mathbb{Q}^{\text{alg}}\langle\langle t^* \rangle\rangle$. The claim follows because $\zeta(r) = Z(\theta(r))$. □

Corollary 5.3. *Given an unambiguous context-free grammar G, it is decidable whether or not $Z(L(G))$ (respectively $\zeta(L(G))$) is a rational function. If $Z(L(G))$ (respectively $\zeta(L(G))$) is rational it can be computed effectively.*

Theorem 5.4. *Given a context-free grammar G, it is undecidable whether or not $\zeta(L(G))$ (respectively $Z(L(G))$) is rational.*

Proof. A slight modification of the proof of [5, Theorem 8.8] shows that given a Turing machine M and a word w we can effectively construct an instance PCP of Post Correspondence Problem with the following properties. The instance has a solution if and only if M accepts w. Furthermore, the set of the solutions of PCP has the form u^+, where u is a word. Construct now the language

$$L(M, w) = L(\text{PCP}) \cap L_{mi}$$

as in [9, p. 280]. If $L(M, w) = \emptyset$, the function $\zeta(L(M, w))$ (respectively $Z(L(M, w))$) is rational. Suppose $\zeta(L(M, w))$ is rational. Let n be the length of the shortest word in $L(M, w)$. Clearly, $n > 1$. Therefore, by Theorem 4.1, the number of words of length n is divisible by n. By construction, however, $L(M, w)$ has a unique word of length n. Therefore $\zeta(L(M, w))$ is not rational if $L(M, w)$ is not empty.

This shows that $\zeta(L(M, w))$ (respectively $Z(L(M, w))$) is rational if and only if M does not accept w. Because $L(M, w)^c$ is context-free and for any language L, the function $\zeta(L)$ (respectively $Z(L)$) is rational if and only if $\zeta(L^c)$ (respectively $Z(L^c)$) is rational, the claim follows. □

The proof of Theorem 5.4 implies:

Corollary 5.5. *Given a context-free grammar G, it is undecidable whether or not $\zeta(L(G))$ (respectively $Z(L(G))$) has integer coefficients.*

Acknowledgement

The author would like to thank Professor Arto Salomaa for his useful comments on the preliminary version of this paper. The author is grateful to the Academy of Finland for the excellent working conditions.

References

[1] J. Berstel and C. Reutenauer, Rational Series and Their Languages (Springer, Berlin, 1988).
[2] J. Berstel and C. Reutenauer, Zeta functions of recognizable languages, in: T. Lepistö and A. Salomaa, eds., Automata, Languages and Programming (Springer, Berlin, 1988) 93-104.
[3] B. Dwork, On the rationality of the zeta function of an algebraic variety, Amer. J. Math. 82 (1960) 631-648.
[4] J. Honkala, A necessary condition for the rationality of the zeta function of a regular language, Theoret. Comput. Sci. 66 (1989) 341-347.
[5] J. Hopcroft and J. Ullman, Introduction to Automata Theory, Languages and Computation (Addison-Wesley, Reading, MA, 1979).
[6] W. Kuich and A. Salomaa, Semirings, Automata, Languages (Springer, Berlin, 1986).
[7] S. Lang, Algebra (Addison-Wesley, Reading, MA, 2nd ed., 1984).
[8] M. Lothaire, Combinatorics on Words (Addison-Wesley, Reading, MA, 1983).
[9] A. Salomaa, Formal Languages (Academic Press, New York, 1973).
[10] A. Salomaa and M. Soittola, Automata-Theoretic Aspects of Formal Power Series (Springer, Berlin, 1978).