RAIRO. INFORMATIQUE THÉORIQUE

WOLFGANG WECHLER

Characterization of rational and algebraic power series

RAIRO. Informatique théorique, tome 17, nº 1 (1983), p. 3-11
<http://www.numdam.org/item?id=ITA_1983__17_1_3_0>

R.A.I.R.O. Informatique théorique/Theoretical Informatics
(vol. 17, n° 1, 1983, p. 3 à 11)

CHARACTERIZATION OF RATIONAL AND ALGEBRAIC POWER SERIES (*) (**)

by Wolfgang WECHLER ([1])

Communicated by M. NIVAT

Abstract. — *The paper presents a new characterization of algebraic formal power series: they are defined by finitely generated invariant subsemi-algebras of formal power series. This is comparable with the known characterization of rational power series.*

Résumé. — *L'article présente une nouvelle caractérisation des séries formelles algébriques : elles sont définies par des sous-semialgèbres invariantes et finiment engendrées. Ce résultat est à rapprocher de la caractérisation classique des séries formelles rationnelles.*

1. INTRODUCTION AND BASIC NOTIONS

Let R be a semiring and let M be a monoid. A mapping s from M into R is called a (formal) power series and s itself is written as formal sum

$$s = \sum_{m \in M} (s, m) m$$

where (s, m) is the image of $m \in M$ under the mapping s. The values (s, m) are referred to as coefficients of s. $R \langle\langle M \rangle\rangle$ denotes the set of all such mappings. The support $\mathrm{supp}(s)$ of a power series s is the set $\mathrm{supp}(s) = \{ m \in M \mid (s, m) \neq 0 \}$. Any power series with a finite support is called a polynomial. The set of all polynomials is denoted by $R \langle M \rangle$.

In this paper a new characterization of algebraic power series will be presented. The known characterization of rational power series shall also be established in our framework in order to emphasize the analogy of both kinds of characterization. To prepare such a characterization some necessary

(*) Received May 1978, revised April 1979.
(**) A preliminary version of this paper was presented at MFCS'79 Conference, Olomouc, CSSR [5].
([1]) Sektion Mathematik, Technische Universität Dresden, DDR-8027 Dresden, German Democratic Republic.

concepts from the representation theory of monoids and from an appropriate generalization of module theory must be introduced.

A commutative monoid A with the operation $+$ is called an R-semimodule if, for each r of a given semiring R and each a of A, a scalar product ra is defined in A such that the usual axioms are satisfied: $r(a+a')=ra+ra'$, $(r+r')a=ra+r'a$, $(r.r')a=r(r'a)$, $1a=a$, $0a=0$ and $r0=0$ for $r,r'\in R$, $a, a'\in A$. Obviously, $R\langle\langle M\rangle\rangle$ forms an R-semimodule with respect to the usual operations.

An R-semimodule is an algebraic structure in the sense of universal algebra. Therefore, the notions of an R-subsemimodule, of a generated R-subsemimodule and of an R-homomorphism are fixed in that sense and we can skip their definitions here. In order to define one of our main concept we have to consider the regular representation of a monoid M. Let $\mathrm{Hom}_R(R\langle\langle M\rangle\rangle, R\langle\langle M\rangle\rangle)$ denote the set of all R-homomorphisms from $R\langle\langle M\rangle\rangle$ into itself. By the regular representation $\rho: M \to \mathrm{Hom}_R(R\langle\langle M\rangle\rangle, R\langle\langle M\rangle\rangle)$ of M, a mapping ρ_m is assigned to each m of M as follows

$$\rho_m s = \sum_{n\in M} (s, m.n)n$$

for all s of $R\langle\langle M\rangle\rangle$.

We say that an R-subsemimodule A of $R\langle\langle M\rangle\rangle$ is invariant if, for each m of M, $s\in A$ implies $\rho_m s\in A$. By means of invariant R-subsemimodules of $R\langle\langle M\rangle\rangle$ rational power series can be characterized (cf. [2]). To do the same for algebraic power series invariant R-subsemialgebras are needed. An R-semimodule A is said to be an R-semialgebra if A is additionally a semiring and verifies $r\in R,\ a,\ a'\in A \Rightarrow r.(a.a')=(r.a).a'$. $R\langle\langle M\rangle\rangle$ forms an R-semialgebra provided a (Cauchy) product of power series can be defined. For that reason it has to be assumed that each m of M possesses only finitely many factorizations $m=m_1.m_2$. This condition is satisfied for a monoid with length-function, which is a mapping λ from M into the natural numbers $\mathbb{N}$ such that, for each $n\in\mathbb{N}$, $\lambda^{-1}(n)$ is a finite set, $\lambda^{-1}(0)=\{1\}$ (1 denotes also the unit element of M), and $\lambda(m.m')\geqq\lambda(m)+1$ as well as $\lambda(m'.m)\geqq\lambda(m)+1$ for all $m\in M$ and $m'\in M-\{1\}$ [1]. Clearly, the free monoid generated by a finite set is a monoid with length-function. If M is a monoid with length-function, then $R\langle\langle M\rangle\rangle$ is an R-semialgebra with respect to usual operations. An R-subsemialgebra of $R\langle\langle M\rangle\rangle$ is called invariant if it is invariant as R-subsemimodule.

2. MATRIX REPRESENTATIONS OF A MONOID

In this section we intend to introduce representations of a monoid by matrices over a semiring. Let n be a natural number. The set of all $n\times n$ matrices $A=(a_{ij})$

with $a_{ij} \in R$, $i, j = 1, \ldots, n$, is denoted by $(R)_n$. Obviously, $(R)_n$ forms a monoid with respect to matrix multiplication.

DEFINITION: Let M be a monoid and let n be a natural number. A homomorphism δ from M into $(R)_n$ is called a finite matrix representation of M.

We are now going to consider infinite matrices. Let N be a set. $(R)_N$ denotes the set of all mappings A from $N \times N$ into R, which will be written as (possible infinite) matrices $A = (a_{ij})$ with $a_{ij} = A(i, j)$ for $i, j \in N$. In order to generalize the matrix multiplication in that case we state the following requirement: in each row of A there are all but finitely many coefficients equal to 0. Under this assumption $(R)_N$ forms a monoid with respect to (generalized) matrix multiplication.

DEFINITION: Let M be a monoid with length-function and let N be a finitely generated monoid. A homomorphism δ from M into $(R)_N$ is called a locally finite matrix representation of M if the associated mapping $[\ ]: N \rightarrow R\langle\langle M \rangle\rangle$ defined by

$$[n] = \sum_{m \in M} \delta(m)_{n,e} m \qquad (e \text{ is the unit element of } N)$$

is a homomorphism from N into the multiplicative monoid of $R\langle\langle M \rangle\rangle$.

Since matrix representations shall be used as acceptors the question arises: Under which conditions is a locally finite matrix representation determined by finitely many datas. Assume that M and N are free monoids generated by finite sets X and P, resp. For each pair (x, p) of $X \times P$ let a finite set of elements $d(x, p, q)$ of R be chosen, where $q \in P^*$. Define a mapping $\delta: X \rightarrow (R)_{P^*}$ by

$$\delta(x)_{q_1, q_2} = \begin{cases} d(x, p, q) & \text{if there are } p \in P \text{ and } q, q' \in P^* \\ & \text{such that } q_1 = pq' \text{ and } q_2 = qq' \\ 0 & \text{otherwise.} \end{cases}$$

The unique extension $\delta^*: X^* \rightarrow (R)_{P^*}$ of δ is a locally finite matrix representation. It is easily seen that the associated mapping $[\ ]: P^* \rightarrow R\langle\langle X^* \rangle\rangle$ is a homomorphism. On this basis generalized acceptors for algebraic power series are introduced in [4].

3. RECOGNIZABLE POWER SERIES

Let M be a monoid and let R be a semiring. Our first aim is the definition of two kinds of recognizable power series using finite resp. locally finite matrix representations. It will be shown that recognizable power series can be characterized by means of invariant R-subseminodules resp. R-subsemialgebras of $R\langle\langle M\rangle\rangle$.

DEFINITION: A power series s of $R\langle\langle M\rangle\rangle$ is said to be f-recognizable (or, shortly, recognizable) if there exist a finite matrix representation $\delta: M \to (R)_n$, $n \geqq 1$, a row vector $\alpha=(\alpha_1, \ldots, \alpha_n)$ and a column vector $\beta=(\beta_1, \ldots, \beta_n)^{\mathrm{T}}$ such that

$$(s, m)=\alpha . \delta(m) . \beta \qquad \text{for all } m \in M .$$

If $s \in R\langle\langle M\rangle\rangle$ is recognizable, then the n power series s_i defined by $(s_i, m)=(\delta(m) . \beta)_i$ for $i=1, \ldots, n$ generate an R-subsemimodule

$$A=\sum_{i=1}^{n} R s_i$$

which contains s because of $s=\alpha_1 s_1+\ldots+\alpha_n s_n$. An easy calculation shows that A is invariant. Therefore, we get

THEOREM 1: Each recognizable power series s of $R\langle\langle M\rangle\rangle$ belongs to an invariant finitely generated R-subsemimodule of $R\langle\langle M\rangle\rangle$. □

In the case of free monoids the derived condition is necessary and sufficient.

THEOREM 2 [2]: Let M be a free monoid generated by a finite set. A power series s of $R\langle\langle M\rangle\rangle$ is recognizable if and only if s belongs to an invariant finitely generated R-subsemimodule of $R\langle\langle M\rangle\rangle$. □

Next, we are going to introduce lf-recognizable power series, which will be characterized in a similar way.

DEFINITION: Let M be a monoid with length-function. A power series s of $R\langle\langle M\rangle\rangle$ is said to be lf-recognizable if there exist a locally finite matrix representation $\delta: M \to (R)_N$, a row vector $\alpha=(\alpha_n)_{n \in N}$ with all but finitely many coefficients equal to 0, and a unit column vector $\beta=(\beta_n)_{n \in N}^{\mathrm{T}}$ with $\beta_e=1$ and $\beta_n=0$ for $n \neq e$ such that

$$(s, m)=\alpha . \delta(m) . \beta \qquad \text{for all } m \in M .$$

THEOREM 3: Let M be a monoid with length-function. Then each lf-recognizable power series s of R $\langle\langle M\rangle\rangle$ belongs to an invariant finitely generated R-subsemialgebra of $R\langle\langle M\rangle\rangle$.

Proof: Assume that s is an lf-recognizable power series of $R\langle\langle M\rangle\rangle$. Then there exist a locally finite matrix representation $\delta: M \to (R)_N$ and finitely many $\alpha_n \in R$ such that

$$(s, m)=\sum_{n \in N} \alpha_n . \delta(m)_{n, e} .$$

By definition, N is finitely generated. Thus, the R-subsemialgebra A of $R\langle\langle M\rangle\rangle$ consisting of all finite sums

$$s=\sum_{n\in N} r_n[n] \quad \text{where} \quad r_n\in R$$

is finitely generated too. Take into consideration that [ ] is a homomorphism. Evidently, $s=\Sigma\alpha_n[n]$ is contained in A.

It remains to show that A is invariant. Let s be an element of A. For an arbitrary element m of M we derive

$$(\rho_m s, m')=\sum_{n\in N} r_n(\rho_m[n], m')=\sum_{n\in N} r_n([n], m.m')$$
$$=\sum_{n'\in N}\Big(\sum_{n\in N} r_n\delta(m)_{n,n'}\Big)([n'], m')$$

where all sums are finite. Hence

$$\rho_m s=\sum_{n\in N} r'_n[n] \quad \text{with} \quad r'_n=\sum_{n'\in N} r_{n'}\delta(m)_{n',n}$$

and, consequently, $\rho_m s\in A$. □

THEOREM 4: Let M be a free monoid generated by a finite set. A power series s of $R\langle\langle M\rangle\rangle$ is *lf*-recognizable if and only if s belongs to an invariant finitely generated R-subsemialgebra of $R\langle\langle M\rangle\rangle$.

Proof: By Theorem 3, it suffices to show that each element of an invariant finitely generated R-subsemialgebra A of $R\langle\langle M\rangle\rangle$ is an *lf*-recognizable power series provided M is the free monoid X^* generated by a finite set X. Assume that A is generated by $\{s_p \mid p\in P\}$, where P is a finite set. Since A is invariant we get

$$\rho_x s_p=\sum_{q\in P^*} r_{p,q}(x)q[p/s_p] \quad \text{with} \quad r_{p,q}(x)\in R$$

whereby the sum is finite. $q[p/s_p]$ denotes the substitution of each p of P by the corresponding s_p in $q\in P^*$. Now we define a mapping $\delta: X \rightarrow (R)_{P^*}$ by the rule

$$\delta(x)_{q_1,q_2}=\begin{cases} r_{p,q}(x) & \text{if there are } p\in P \text{ and } q,\, q'\in P^* \\ & \text{such that } q_1=pq' \text{ and } q_2=qq' \\ 0 & \text{otherwise.}\end{cases}$$

We assert that the unique extension $\delta^*: X^* \rightarrow (R)_{P^*}$ of δ is a locally finite matrix representation of X^*. For that reason it must be shown that the associated mapping [ ] from P^* into the multiplicative monoid of $R\langle\langle X^*\rangle\rangle$ defined by

$$[q]=\sum_{w\in X^*}\delta^*(w)_{q,e}w \quad \text{for all} \quad q\in P^*$$

is a homomorphism. Evidently,

$$[e]=\sum_{w\in X^*}\delta^*(w)_{e,e}w=1$$

by definition. In order to show $[qq']=[q].[q']$ for $q, q'\in P^*$ we use the statement

$$\delta^*(w)_{qq',q''}=\sum_{\substack{uv=w\\ u\neq 1}}\ \sum_{q_1q_2=q''}\delta^*(u)_{q,q_1}.\delta^*(v)_{q',q_2}$$

for all non-empty words w over X and all $q, q', q''\in P^*$, which may be proved by induction over the length of w. Let q and q' be elements of P^*. Now we conclude

$$\begin{aligned}[qq']&=\sum_{w\in X^*}\delta^*(w)_{qq',e}w=\sum_{w\in X^*}\Big(\sum_{uv=w}\delta^*(u)_{q,e}.\delta^*(v)_{q',e}\Big)w\\&=[q].[q'].\end{aligned}$$

Without loss of generality we suppose that $(s_p, 1)=0$ for all p of P. We are now going to prove that each element of A is lf-recognizable by that δ^*. First we state

$$s_p=[p] \quad \text{for} \quad p\in P.$$

Obviously, it holds

$$\begin{aligned}(s_p, x)&=(\rho_x s_p, 1)=\sum_{q\in P^*}r_{p,q}(x)(q[p/s_p], 1)=r_{p,e}(x)\\&=([p], x)\end{aligned}$$

for all $x\in X$. Let $w\in X^*$. Then

$$(s_p, xw)=(\rho_x s_p, w)=\sum_{q\in P^*}r_{p,q}(x)(q[p/s_p], w).$$

Together with

$$(q[p/s_p], w)=\delta^*(w)_{q,e} \qquad (*)$$

we get

$$\begin{aligned}(s_p, xw)&=\sum_{q\in P^*}\delta^*(x)_{p,q}.\delta^*(w)_{q,e}=\delta^*(xw)_{p,e}\\&=([p], xw),\end{aligned}$$

that means $s_p = [p]$. Each s of A can be represented as follows

$$s = \sum_{q \in P^*} r_q q\,[p/s_p]$$

whereby the sum is finite. Because of (*) we obtain

$$(s, w) = \sum_{q \in P^*} r_q (q\,[p/s_p], w) = \sum_{q \in P^*} r_q \delta^*(w)_{q,e}$$

which proves that s is *lf*-recognizable. □

4. CHARACTERIZATION OF RATIONAL AND ALGEBRAIC POWER SERIES

Throughout this section M is always assumed to be a free monoid generated by a finite set X. As a conclusion of the well-known Schützenberger Theorem (cf. [3]) we obtain

THEOREM 5 [2]: A power series s of $R\langle\langle X^* \rangle\rangle$ is rational if and only if s belongs to an invariant finitely generated R-subsemimodule of $R\langle\langle X^* \rangle\rangle$. □

Algebraic power series are defined as solutions of systems of equations. Let $Z = \{z_1, \ldots, z_n\}$ be a finite set of variables disjoint from X. An algebraic system S is a set of equations

$$z_i = \varphi_i \qquad i = 1, \ldots, n,$$

where $\varphi_i \in R\langle V^* \rangle$ with $V = X \cup Z$. S is called proper whenever $(\varphi_i, 1) = 0$ and $(\varphi_i, z_j) = 0$ for each i and j. It is known (cf. [3]) that each proper algebraic system S has a unique solution $|S| = (\sigma_1, \ldots, \sigma_n)$ with $\sigma_i \in R\langle\langle X^* \rangle\rangle$ for $i = 1, \ldots, n$. We also write $|S|_i$ instead of σ_i.

THEOREM 6: A power series s of $R\langle\langle X^* \rangle\rangle$ is algebraic if and only if s belongs to an invariant finitely generated R-subsemialgebra of $R\langle\langle X^* \rangle\rangle$.

Proof: (1) Let s be an algebraic power series of $R\langle\langle X^* \rangle\rangle$ determined by a proper algebraic system S. Without loss of generality we may assume that S has the following form

$$z_i = \sum_{x \in X} \left(r_i(x)x + \sum_{j=1}^{n} r_{ij}(x) x z_j + \sum_{j,k=1}^{n} r_{ijk}(x) x z_j z_k \right)$$

for $i = 1, \ldots, n$, where $r_i(x)$, $r_{ij}(x)$ and $r_{ijk}(x)$ are elements of R (cf. Theorem 2.3, [3], p. 128). Let $|S| = (\sigma_1, \ldots, \sigma_n)$ be the solution of S. Define A to be the

R-subsemialgebra of $R\langle\langle X^*\rangle\rangle$ generated by $\{\sigma_1, \ldots, \sigma_n\}$. Evidently, s belongs to A because of $s=(s, 1)+\sigma_i$ for some σ_i of the generator set.

It remains to prove that A is invariant. Since each σ_i obeys the equation

$$\sigma_i=\sum_{x\in X}\left(r_i(x)x+\sum_{j=1}^{n} r_{ij}(x)x\sigma_j+\sum_{j,k=1}^{n} r_{ijk}(x)x\sigma_j\sigma_k\right)$$

we derive

$$\rho_x\sigma_i=r_i(x)+\sum_{j=1}^{n} r_{ij}(x)\sigma_j+\sum_{j,k=1}^{n} r_{ijk}(x)\sigma_j\sigma_k$$

which implies

$$\rho_x\sigma_i\in A \qquad \text{for} \qquad x\in X \quad \text{and} \quad i=1, \ldots, n.$$

Notice that an arbitrary element a of A is a finite sum $a=\Sigma r_\pi\pi$, where $r_\pi\in R$ and $\pi\in\{\sigma_1, \ldots, \sigma_n\}^*$. If we prove that $\rho_x\pi$ belongs to A for each non-empty word π, then $\rho_x a=\Sigma r_\pi\rho_x\pi$ belongs to A too, which implies that A is invariant. Now, assume that $\pi=\sigma_i\pi'$, where π' is an arbitrary word over $\{\sigma_1, \ldots, \sigma_n\}$. Observe that $(\sigma_i, 1)=0$ for $i=1, \ldots, n$. Because of

$$\rho_x(\sigma_i\pi')=(\rho_x\sigma_i)\pi'+(\sigma_i, 1)\rho_x\pi'$$

we thus derive

$$\rho_x(\sigma_i\pi')=(\rho_x\sigma_i)\pi'.$$

Since $\rho_x\sigma_i\in A$ and $\pi'\in A$, it follows the required condition $\rho_x\pi\in A$.

(2) Conversely, let A be an invariant R-subsemialgebra of $R\langle\langle X^*\rangle\rangle$ generated by the set $\{s_1, \ldots, s_n\}$. It has to be shown that each element of A is an algebraic power series. For that reason a proper algebraic system S must be constructed. Without loss of generality we may assume $(s_i, 1)=0$ for $i=1, \ldots, n$. Since A is invariant we derive

$$\rho_x s_i=\sum_{v\in Z^*} r_{i,v}(x)v\,[\underline{z}/\underline{s}],$$

where $Z=\{z_1, \ldots, z_n\}$ and $v[\underline{z}/\underline{s}]$ denotes the substitution of each z_i by s_i in v. Define S as follows

$$z_i=\sum_{x\in X}\sum_{v\in Z^*} r_{i,v}(x)xv \qquad i=1, \ldots, n.$$

Take into consideration that $(s_i, 1)=0$. Then we conclude

$$\begin{aligned} s_i&=\sum_{x\in X} x\rho_x s_i=\sum_{x\in X} x\Big(\sum_{v\in Z^*} r_{i,v}(x)v\,[\underline{z}/\underline{s}]\Big)\\ &=\sum_{x\in X}\sum_{v\in Z^*} r_{i,v}(x)(xv)\,[\underline{z}/\underline{s}]=z_i\,[\underline{z}/\underline{s}]\\ &=|\,S\,|_i \qquad i=1, \ldots, n \end{aligned}$$

Therefore, each s_i is an algebraic power series. Since the set of all algebraic power series is closed under scalar product, sum and product, each a of A is algebraic. □

REFERENCES

1. M. NIVAT, *Séries formelles algébriques*. In « Séries Formelles » (Ed. Berstel, J.). Laboratoire d'Informatique Théorique et Programmation, Paris, 1978.
2. M. FLIESS, *Matrices de Hankel*, J. Math. Pures et Appliqués, vol. 53, 1974, p. 197-222.
3. A. SALOMAA and M. SOITTOLA, *Automata-Theoretic Aspects of Formal Power Series*. Springer-Verlag, New York-Heidelberg-Berlin, 1978.
4. W. WECHLER, *The Concept of Fuzziness in Automata and Language Theory*. Akademie-Verlag, Berlin, 1978.
5. W. WECHLER, *Characterization of Rational and Algebraic Power Series*, *in* Mathematical Foundations of Computer Science, 1979, J. Bečvář. Ed., LNCS, n° 74, p. 499-507.