ELSEVIER

Theoretical Computer Science 292 (2003) 85–96

Theoretical Computer Science

www.elsevier.com/locate/tcs

On a valuation of rational subsets of $\mathbf{Z}^k$ Dédié à Jean Berstel ☆

Srečko Brlek[a], Christophe Reutenauer[b,*]

[a] *LACIM, Département de Mathématiques et Informatique, UQAM, Montréal, P.Q., Succ. Centre-Ville, Canada H3C 3P8*

[b] *UFR Mathématiques, Université Louis Pasteur, 7, rue René Descartes, F-67084 Strasbourg, France*

Abstract

A well-known construction associates to each rational subset of $\mathbf{N}^k$ a rational function in k commuting variables. We extend this construction to rational subsets of $\mathbf{Z}^k$. As a consequence, we derive a multivariate generalization of Popoviciu's theorem and a classical valuation on rational polyhedra.

Keywords: Rational subset; Commutative monoid; Rational function; Valuation; Polyhedra; Popoviciu theorem

1. Introduction

A well-known construction, essentially a corollary of Kleene's theorem and of the existence of deterministic automata, associates to each rational language a commutative multivariate rational function. A commutative analogue exists: given a rational subset of $\mathbf{N}^k$, one associates to it a rational function in k commutative variables, which actually represents it completely.

In the present article, we extend this second construction to each rational subset of $\mathbf{Z}^k$. The construction is not difficult: consider a non-ambiguous rational expression for the subset (which exists according to Eilenberg and Schützenberger) and, viewing the free abelian group $\mathbf{Z}^k$ multiplicatively, interpret it naturally as a rational function (union becomes sum, product remains product, star of S becomes $(1-S)^{-1}$). Since, by unambiguity, only stars of singletons are admitted, it is not difficult to see that the function exists (that is, one never inverts 0). The main difficulty is to show that the rational function depends only on the subset.

☆ Research supported by a NSERC grant (Canada).

* Corresponding author. Tel.: +33-3-90-24-01-35; fax: +33-3-90-24-03-28.

E-mail address: reutenau@math.u-strasbg.fr (C. Reutenauer).

0304-3975/02/$ - see front matter
PII: S0304-3975(01)00216-X

Actually, we generalize this construction in a more general setting: define rational power series on a free abelian group, by allowing sums, products and stars, each time these are locally finite. For instance, neither the square of $\sum_{n\in\mathbf{Z}} x^n$ is defined, nor its star; however the star of $\sum_{n\in\mathbf{Z}} x^n y^{|n|+1}$ is defined. The rational function is then associated naturally as above. However, it is not evident that one does not invert 0, and this is shown by a lemma on the minors of a matrix. After that, we deduce that the function depends only on the rational series, and not on the chosen rational expression. The proof uses some Kleene-like characterization of rational series, for which we have followed Sakarovitch.

It is not true that the rational function faithfully represents the series. For instance, the rational series $\sum_{n\in\mathbf{Z}} x^n$ (actually the characteristic series of a rational subset) maps onto 0. The exact determination of the kernel leads to a multivariate generalization of Popoviciu's theorem.

We deduce from our construction a valuation on the set of rational polyhedra. This was actually the motivation of our paper. To a rational polyhedra, one canonically associates a rational subset of $\mathbf{Z}^k$; actually, the set of its integral points. Then the rational function of this subset is the valuation of the polyhedron. We conjecture that it is the same rational function as the one associated to polyhedra by Lawrence and Khovanskii-Pukhlikov.

We conclude the paper by showing that a non-commutative analogue of the main result is not possible. Indeed, the free group, considered as an unambiguous subset of itself, leads to a rational expression which is degenerate in the free field (one inverts 0 at some step).

2. Rational subsets of a monoid

A subset S of a monoid M is *rational* if it can be obtained from finite subsets by the *rational operations*, namely union, product and star. Recall that the product of two subsets S_1 and S_2 is $S_1S_2 = \{m_1m_2 \mid m_i \in S_i\}$ and that the star of a subset S is $S^* = \bigcup_{n\in\mathbf{N}} S^n$; note that S^* is the submonoid generated by S.

Following [2] (see also [1, p. 186]), we define the class of *unambiguously rational* subsets of M to be the least class $\mathscr{E}$ of subsets of M such that:

- each finite subset is in $\mathscr{E}$;
- if S_1 and $S_2 \in \mathscr{E}$ and $S_1 \cap S_2 = \emptyset$ then $S_1 \cup S_2 \in \mathscr{E}$;
- if S_1 and $S_2 \in \mathscr{E}$ and if their product is unambiguous (that is $x_1x_2 = y_1y_2$ with $x_i, y_i \in S_i$ implies $x_i = y_i$), then $S_1S_2 \in \mathscr{E}$;
- if $S \in \mathscr{E}$ and if S is the basis of a free submonoid of M, then $S^* \in \mathscr{E}$.

By definition each rational subset of M is described by some *rational expression*, which is a well-formed formula involving elements of M and the rational operations. Similarly, an unambiguously rational subset has an unambiguous

rational expression; loosely speaking, a rational expression is unambiguous if it is multiplicity-free.

Observe that each unambiguously rational subset of M is clearly rational. Moreover, if M is a free monoid then every rational subset is also unambiguously rational. This fact is a direct consequence of the Kleene theorem [1]. It appears that the freeness assumption is essential (see [2, p. 174], or [1, p. 187, the monoid $\{a,b\}^* \times \{c\}^*$ contains rational subsets which are not unambiguously rational]). However, Eilenberg and Schützenberger showed that when M is commutative, then each rational subset of M is unambiguous [2, Theorem IV].

3. A rational function

Our concern here is the case $M = \mathbf{Z}^k$, where the Eilenberg–Schützenberger theorem applies. It allows us to associate a rational function with each rational subset of $\mathbf{Z}^k$ in the following way:

Let $\mathbf{F}$ be a field and $x_1,\ldots,x_k$ be commutative variables. We identify $\mathbf{Z}^k$ with the multiplicative group of Laurent monomials in the variables $x_1,\ldots,x_k$:

$$\mathbf{Z}^k = \{x_1^{i_1}x_2^{i_2}\ldots x_k^{i_k} \mid i_j \in \mathbf{Z}\}.$$

Now, to each rational expression E over M we associate the expression $f(x_1,\ldots,x_k)$ in the field $\mathbf{F}(x_1,\ldots,x_k)$ by replacing the rational operations as follows:

- $\cup \to +$;
- $S^* \to (1-S)^{-1}$.

For instance, the rational expression $x^* \cup yz$ is replaced by $(1-x)^{-1} + yz$ and the expression $x^*(y^{-1})^* \cup x^{-1}(x^{-1})^*$ by $(1-x)^{-1}(1-y^{-1})^{-1} + x^{-1}(1-x^{-1})^{-1}$.

The objective of this paper is to study the rational function $f(x_1,\ldots,x_k)$ and to establish the following theorem.

Theorem 1. *If E is unambiguous, then $f(x_1,\ldots,x_k)$ is a well-defined rational function in $\mathbf{F}(x_1,\ldots,x_k)$, depending only on the subset S of $\mathbf{Z}^k$ represented by E.*

The fact that f is well-defined is not too difficult to show, since, in the commutative case, the unambiguous star operation applies only to singletons. Nevertheless we shall prove a more general result which in turn implies the more difficult uniqueness assertion in the theorem.

It turns out that when the subset is actually a rational subset of $\mathbf{N}^k$, then f is represented by the formal power series $\sum_{m\in S} m$, which is well-known to be rational. Recall that a formal power series in the commuting variables $x_1,\ldots,x_k$ is called rational if it is the quotient of two polynomials, with a denominator having non-zero constant term, that is, invertible as formal power series.

The mapping $S \mapsto f$ is far from being injective as the following example shows: $S = \{x^n \mid n \in \mathbf{Z}\}$ has the unambiguous expression $x^* \cup x^{-1}(x^{-1})^*$. Then

$$f(x) = \frac{1}{1-x} + \frac{x^{-1}}{1-x^{-1}} = \frac{1}{1-x} + \frac{1}{x-1} = 0.$$

The previous example has the following generalization.

Corollary 2. *If S is the union (possibly infinite) of cosets of a non-trivial cyclic subgroup in $\mathbf{Z}^k$, then $f = 0$.*

The converse of Corollary 2 is not true, as shows the counter-example: $S = x^*y^* \cup x^{-2}(x^{-1})^*(x^{-1}y)^* \cup y^{-2}(y^{-1})^*(y^{-1}x)^*$.

4. Rational series on a monoid

Let M be a multiplicative monoid and $\mathbf{F}$ be a field. A *series* on M over $\mathbf{F}$ is a formal sum $\sum_{m\in M} \alpha_m m$, where the coefficients $\alpha_m \in \mathbf{F}$. The set of series is an $\mathbf{F}$-vector space.

We introduce now the product and star, which are partially defined operations. The product of two series $S = \sum_{m\in M} \alpha_m m$, and $T = \sum_{m\in M} \beta_m m$, is the series

$$ST = \sum_{m\in M} \gamma_m m, \quad \text{with } \gamma_m = \sum_{xy=m} \alpha_x \beta_y$$

this product is *defined* (or *convergent*) provided that each γ_m is obtained as a finite sum. The star of S is the series

$$S^* = \sum_{m\in M} \delta_m m \quad \text{with } \delta_m = \sum_{i\geqslant 0, x_1\ldots x_i = m} \alpha_{x_1} \ldots \alpha_{x_i};$$

this star is *defined* (or *convergent*) provided that each δ_m is obtained as a finite sum.

The set $\mathscr{S}$ of *rational series* is the vector space of series such that

- each polynomial (that is, a finite series) is in $\mathscr{S}$;
- if $S, T \in \mathscr{S}$ and if the product ST is defined then $ST \in \mathscr{S}$;
- if $S \in \mathscr{S}$ and S^* is defined then $S^* \in \mathscr{S}$.

For later use we observe that if P is an unambiguous rational subset of M then its *characteristic series* $\sum_{m\in P} m \in \mathscr{S}$ is a rational series.

We give now a matrix characterization of rational series. Let A be a square matrix over the monoid algebra $\mathbf{F}[M]$. We say that A^* is *defined* (or *convergent*) if for each $m \in M$ there are only finitely many $n \in \mathbf{N}$ such that m appears (with non-zero coefficient) in A^n. Then the star of A is defined as $A^* = \sum_{n\in\mathbf{N}} A^n$.

Theorem 3. *A series S is rational if and only if there exists a matrix A as before, row and column matrices λ, γ over $\mathbf{F}$ such that $S = \lambda A^* \gamma$.*

This theorem is proved in [9]. We say that S is represented by (λ, A, γ). Note that we may suppose that this triple is *trim*, in the sense of [1]; that is, the following condition holds: for each index j, there are indices i and k such that $\lambda_i \neq 0$, the entries i,j and j,k of A^* are non-zero and γ_k is non-zero; in the automata terminology, this means that each index, or state, is accessible and coaccessible, where the initial (resp. final) states are those i (resp. k) such that λ_i (resp. γ_k) is non-zero.

There is a complete equivalence between representations (λ, A, γ) and $\mathbf{F}$–M-automata: such an automaton is a directed graph, whose edges have labels of the form αm, with α in $\mathbf{F}$ and m in M; there is such an edge from i to j for each such monomial appearing in entry i,j of matrix A. Each initial state i (resp. final state j) of the automaton has a weight λ_i (resp. γ_j). A path is *successful* if it leads from an initial state to a final state. The weight of such a path is the product of the weights of the edges, and the *behaviour* of the automaton is the (infinite) sum of all successful paths; it is *defined*, or *convergent* if this sum converges in $\mathbf{F}^M$, viewing each monomial αm as an element of this space, which gets the product topology, once $\mathbf{F}$ has the discrete topology; in other words, there are only finitely many monomials αm for fixed m in this sum.

In Section 7, we shall use the construction of a representation (λ, A, γ) for each rational series. This construction is the classical one, in the proof Kleene's theorem, leading from a rational expression to an automaton in the case of a free monoid: sum corresponds to union of automata; product to union together some edges from the final states of the first to the initial states of the second; and star to the addition of a new state with some edges from and into it.

The main difference here is the requirement of convergence. It is obtained by transferring the convergence of the rational expression to that of the representation. In the case of the product and the star operation, one has to work with trim automata (or representations). Note indeed that if the automaton is trim, and if its behaviour is convergent, then the star of the matrix A is convergent; and conversely (without the trim assumption). Note also that it is not difficult to have a trim automaton at each stage, by removing unnecessary states.

For later use, we quote the following lemma. Note first that the product of a polynomial (which is an element of $\mathbf{F}[M]$) by a series is always defined.

Lemma 4. *If A^* is defined then $(1-A)A^* = A^*(1-A) = I_n$.*

5. The main results

We focus now on $M = \mathbf{Z}^k$ viewed again multiplicatively as in Section 3. Each rational series S on M over F has a rational expression E. We associate to E an expression $f(x_1,\ldots,x_k)$ in the field $\mathbf{F}(x_1,\ldots,x_k)$ by replacing the star operation as in Section 3.

Theorem 5. *The function $f(x_1,\ldots,x_k)$ is a well-defined rational function in $\mathbf{F}(x_1,\ldots,x_k)$ depending only on S. If S is represented by (λ, A, γ), then $\det(1-A) \neq 0$ ($1-A$ is a matrix of Laurent polynomials) and $f(x_1,\ldots,x_k) = \lambda(1-A)^{-1}\gamma$.*

Observe that this result implies Theorem 1 of Section 3.

If S is a formal power series in $\mathbf{F}[[x_1,\ldots,x_k]]$ which is rational, that is, a quotient of two polynomials, then S is an element of $\mathscr{S}$ and the corresponding rational function f is this quotient (cf. [5]).

The kernel of the mapping $\Phi : S \mapsto f$ is completely described by the following result. Observe first that the definition of Φ implies that it is a $\mathbf{F}[x_1,\ldots,x_k,x_1^{-1},\ldots,x_k^{-1}]$-linear homomorphism.

Theorem 6. *A series S is in $\ker(\Phi)$ if and only if $PS=0$ for some non-zero Laurent polynomial P.*

We show that this result implies the Corollary 2 of Section 3. Indeed, identify each subset of $\mathbf{Z}^k$ with its characteristic series. Let S be a subset which is a union of cosets of the cyclic subgroup generated by the Laurent monomial $m \neq 1$. Then we have $(1-m)S=0$.

The following result, known as Popoviciu's theorem (see [10, Theorem 4.2.3], with a slightly different formulation) is easily derived from the previous theorem.

Corollary 7. *Let $d \in \mathbf{N}$ and $(a_n)_{n\in\mathbf{Z}}$ be a sequence satisfying a proper linear recurrence, that is*

$$a_{n+d} = \alpha_1 a_{n+d-1} + \alpha_2 a_{n+d-2} + \cdots + \alpha_d a_n$$

with $\alpha_i \in \mathbf{F}$ and $\alpha_d \neq 0$. Then

$$\sum_{n<0} a_n x^n \quad \text{and} \quad \sum_{n\geqslant 0} a_n x^n$$

are rational functions in x^{-1} and x, respectively, and their sum in $\mathbf{F}(x)$ is 0.

Proof. The series $S = \sum_{n\in\mathbf{Z}} a_n x^n$ splits in the negative and positive parts

$$S = \sum_{n<0} a_n x^n + \sum_{n\geqslant 0} a_n x^n,$$

where both series are rational in $\mathbf{F}[[x^{-1}]]$ and $\mathbf{F}[[x]]$, respectively, since the sequences $(a_n)_{n\geqslant 0}$ and $(a_n)_{n<0}$ both satisfy a linear recurrence (the latter because $\alpha_d \neq 0$). This implies that these two series are in $\mathscr{S}$, hence so is S. Let

$$P = x^d - \alpha_1 x^{d-1} - \cdots - \alpha_d.$$

Then $PS=0$ since the (a_n) satisfy the indicated recurrence. Thus by Theorem 6, $\Phi(S)=0$ and this implies the corollary. □

6. A lemma on minors

Let R be a commutative ring and M an R-module containing R as a submodule (in our case R is $\mathbf{F}[x_1,\ldots,x_k,x_1^{-1},\ldots,x_k^{-1}]$, and M is the set of series). We consider

matrices with coefficients in M. We may multiply a matrix over R by a matrix over M: the result is a matrix over M, since R is commutative and M is an R-module.

Moreover, if only one column of a square matrix has coefficients in M, the others having coefficients in R, then we may compute its determinant by the usual formula, using the symmetric group. The value of such a determinant is an element of M. These determinants have the usual linear properties.

Lemma 8. *Let A and B be two $n \times n$ matrices over R and M, respectively, such that $AB = I_n$. Then* $\det(A) \neq 0$.

Proof. The proof proceeds by contradiction. Suppose that $\det(A) = 0$. We prove by descending induction on p, that each $p \times p$ minor of A vanishes. It is true for $p = n$. Assume now it is true for p. Let H be a $(p-1) \times (p-1)$-minor of A. We may assume that H is located in rows and columns 1 to $p-1$. For a column-vector X of length n, denote by X' its projection on its first p components. Let C_i be the ith column of A and C be the pth column of I_n. Then $\det(H) = \det(C'_1, \ldots, C'_{p-1}, C')$. Since $AB = I_n$ there exists elements $m_1, \ldots, m_n$ of M such that

$$C_1 m_1 + \cdots + C_n m_n = C.$$

Therefore the projections also satisfy

$$C'_1 m_1 + \cdots + C'_n m_n = C'.$$

It follows that

$$\begin{aligned}
\det(C'_1, \ldots, C'_{p-1}, C') &= \det(C'_1, \ldots, C'_{p-1}, C'_1 m_1 + \cdots + C'_n m_n) \\
&= \sum_{i=1}^{n} \det(C'_1, \ldots, C'_{p-1}, C'_i m_i) \\
&= \sum_{i=1}^{n} \det(C'_1, \ldots, C'_{p-1}, C'_i) m_i \\
&= \sum_{i=p}^{n} \det(C'_1, \ldots, C'_{p-1}, C'_i) m_i \\
&= 0,
\end{aligned}$$

since each term of this sum is a $p \times p$-minor of A, which vanishes by the inductive hypothesis. We conclude that $A = 0$ (for $p = 1$), a contradiction. □

7. Proofs of the main theorems

We prove Theorem 5. Suppose that S is a rational power series represented by (λ, A, γ). By Lemmas 4 and 8, $1 - A$ is invertible in $\mathbf{F}(x_1, \ldots, x_k)$. We then define

$$f(x_1, \ldots, x_k) = \lambda(1 - A)^{-1}\gamma.$$

We show first that f depends only on S, and not on the triple (λ, A, γ) representing it; then we show that f is obtained from each rational expression representing S as described at the beginning of Section 5.

Lemma 9. *If* $S = 0$, *then* $\lambda(1-A)^{-1}\gamma = 0$.

Proof. We may suppose that $\lambda = (1, 0, \ldots, 0)$, and $\gamma = \lambda^{\mathrm{T}}$. Let $(S_1, \ldots, S_n)^{\mathrm{T}}$ denote the first column of A^*. Then $S = S_1$ and $(1-A)(S_1, \ldots, S_n)^{\mathrm{T}} = \gamma$. Using Cramer's technique, we obtain $\det(1-A)S_1 = \mu$, where μ is the lower right $(n-1)$-minor of $1-A$. Since $S = 0$, $\mu = 0$ which implies that $(1-A)^{-1}_{1,1} = 0$, that is $\lambda(1-A)^{-1}\gamma = 0$. □

Suppose now that S is represented by (λ, A, γ) and (λ', A', γ'). Then

$$\left((\lambda, \lambda'), \begin{pmatrix} A & 0 \\ 0 & A' \end{pmatrix}, \begin{pmatrix} \gamma \\ -\gamma' \end{pmatrix}\right)$$

represents 0: indeed

$$(\lambda, \lambda') \begin{pmatrix} A & 0 \\ 0 & A' \end{pmatrix}^{-1} \begin{pmatrix} \gamma \\ -\gamma' \end{pmatrix} = \lambda(1-A)^{-1}\gamma - \lambda'(1-A')^{-1}\gamma' = 0.$$

The lemma then implies that $\lambda(1-A)^{-1}\gamma = \lambda'(1-A')^{-1}\gamma'$. This proves that f depends only on S.

We show now by induction on the size of a convergent rational expression E representing S that the rational function f associated to E is well-defined and equal to $\lambda(1-A)^{-1}\gamma$ for some (λ, A, γ) representing S. If E is a polynomial then we take

$$A = \begin{pmatrix} 0 & E \\ 0 & 0 \end{pmatrix}, \quad \text{with } \lambda = (1, 0),\ \gamma = (0, 1)^{\mathrm{T}};$$

then A^* is convergent, $\lambda(1-A)^{-1}\gamma = E$ and the function associated to E is E itself.

If $E = E_1 + E_2$, with E_i representing S_i and associated to $(\lambda_i, A_i, \gamma_i)$, then let

$$A = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}, \quad \text{with } \lambda = (\lambda_1, \lambda_2),\ \gamma = (\gamma_1, \gamma_2)^{\mathrm{T}};$$

then A^* is convergent, $\lambda A^* \gamma = S_1 + S_2 = S$ and $\lambda(1-A)^{-1}\gamma = f_1 + f_2 = f$.

If $E = E_1 E_2$, with E_i representing S_i and associated to $(\lambda_i, A_i, \gamma_i)$, then let

$$A = \begin{pmatrix} A_1 & \gamma_1\lambda_2 \\ 0 & A_2 \end{pmatrix}, \quad \text{with } \lambda = (\lambda_1, 0),\ \gamma = (0, \gamma_2)^{\mathrm{T}};$$

then

$$A^* = \begin{pmatrix} A_1^* & A_1^*\gamma_1\lambda_2 A_2^* \\ 0 & A_2^* \end{pmatrix}$$

and

$$(1-A)^{-1} = \begin{pmatrix} (1-A_1)^{-1} & (1-A_1)^{-1}\gamma_1\lambda_2(1-A_2)^{-1} \\ 0 & (1-A_2)^{-1} \end{pmatrix}.$$

Since E_1E_2 is a convergent product, the product of series $\lambda_1 A_1^*\gamma_1\lambda_2 A_2^*\gamma_2$ is convergent. Now, we may suppose that A_i is trim, therefore the product $A_1^*\gamma_1\lambda_2 A_2^*$ is also convergent, which implies that A^* is convergent. Now, $\lambda A^*\gamma = S_1S_2 = S$ and $\lambda(1-A)^{-1}\gamma = f_1f_2 = f$.

Finally, if $E = E_1^*$ and E_1 is associated to $(\lambda_1, A_1, \gamma_1)$ representing S_1, then let

$$A = \begin{pmatrix} A_1 & \gamma_1 \\ \lambda_1 & 0 \end{pmatrix},$$

with $\lambda = (0,1)$, $\gamma = (0,1)^{\mathrm{T}}$; then

$$A^* = \begin{pmatrix} (A_1+\gamma_1\lambda_1)^* & (A_1+\gamma_1\lambda_1)^*\gamma_1 \\ \lambda_1(A_1+\gamma_1\lambda_1)^* & 1+\lambda_1(A_1+\gamma_1\lambda_1)^*\gamma_1 \end{pmatrix}.$$

By hypothesis $S_1^* = \sum_{n\geqslant 0}(\lambda_1 A_1^*\gamma_1)^n$ is convergent. But this series is equal to $1+\lambda_1(A_1+\gamma_1\lambda_1)^*\gamma_1$. Hence $(A_1+\gamma_1\lambda_1)^*$ is also convergent (since we have supposed that A_1 has no unnecessary entries), and this implies that A^* is convergent. Moreover, we have $\lambda A^*\gamma = S_1^* = S$. Denoting by f_1 the rational function associated to E_1, the rational function associated to $E = E_1^*$ is $(1-f_1)^{-1}$; we have thus to show that $f_1 \neq 1$. The matrix $1-A$ is invertible by Lemmas 4 and 8. Denote by $(g_1,\ldots,g_n,h)^{\mathrm{T}}$ the last column of its inverse. With $G = (g_1,\ldots,g_n)^{\mathrm{T}}$ we have

$$\begin{aligned} (1-A_1)G - \gamma_1 h &= 0, \\ -\lambda_1 G + h &= 1. \end{aligned}$$

Solving this system we obtain successively $G = (1-A_1)^{-1}\gamma_1 h$ and $h = 1+\lambda_1 G = 1+\lambda_1(1-A_1)^{-1}\gamma_1 h = 1+f_1 h$. This implies that $f_1 \neq 1$ and that $h = (1-f_1)^{-1}$. Finally this computation also shows that $\lambda(1-A)^{-1}\gamma = (1-f_1)^{-1}$ which concludes the proof of Theorem 5.

Note that we have not used Theorem 3; moreover, the previous arguments prove one implication of Theorem 3: if S is rational, then it has a triple (λ, A, γ) representing it.

We prove now Theorem 6. The construction of Φ by rational expressions implies that Φ is $\mathbf{F}[x_1,\ldots,x_k,x_1^{-1},\ldots,x_k^{-1}]$-linear. So, if $PS = 0$ then $P\Phi(S) = 0$, and $\Phi(S) = 0$, since $P \neq 0$. Conversely, suppose that $\Phi(S) = 0$. Borrowing the notations from the proof of Lemma 9, we obtain $\mu = 0$, since

$$0 = \Phi(S) = (1-A)^{-1}_{1,1} = \frac{\mu}{\det(1-A)}.$$

Thus $\det(1-A)S = 0$ which concludes the proof.

8. Rational polyhedra

A *polyedron* in $\mathbf{R}^k$ is a finite intersection of closed half-spaces. It is called *rational* if the half-spaces are defined by rational coordinates. The *algebra of polyhedra* $\mathscr{P}$ is the vector space over $\mathbf{R}$ spanned by the characteristic functions of all rational polyhedra. A *valuation* on polyhedra is a linear mapping defined on $\mathscr{P}$. We mention as an example the *Euler characteristic* which is the valuation sending each characteristic function of a polyhedron to 1; the existence of this valuation is not evident (see [8] or [3, Theorem 2.2]).

We construct now a valuation on $\mathscr{P}$. To a rational polyhedron P associate the series $S_P = \sum_{m\in P\cap \mathbf{Z}}^{k} m$, where we identify once more Laurent monomials and vectors in $\mathbf{Z}^k$. Since rational subsets of $\mathbf{Z}^n$ are closed under intersection and projection [2], and since a rational polyhedron can be described by linear functions having integer coordinates, $P\cap\mathbf{Z}^k$ is a rational subset of $\mathbf{Z}^k$ for any rational polyhedron P. Hence $S_P\in\mathscr{S}$ (see Section 4). The mapping $P\mapsto S_P$ extends to a linear mapping $\mathscr{P}\to\mathscr{S}$. Therefore we obtain a valuation $\mathfrak{V}:\mathscr{P}\to\mathbf{R}(x_1,\ldots,x_k)$ defined by $P\mapsto\Phi(S_P)$.

Theorem 10. *Let* $[P]$ *denote the characteristic function of a polyhedron* P.

(1) *If* $P_1,\ldots,P_n$ *are rational polyhedra and* $\alpha_1,\ldots,\alpha_n$ *are real coefficients such that* $\alpha_1[P_1]+\cdots+\alpha_n[P_n]=0$, *then*

$$\alpha_1\mathfrak{V}[P_1]+\cdots+\alpha_n\mathfrak{V}[P_n]=0.$$

(2) *If* P' *is the translation of* P *by* $v\in\mathbf{Z}^k$, *then*

$$\mathfrak{V}[P']=x^v\mathfrak{V}[P],$$

where $x^v=x_1^{i_1}\ldots x_k^{i_k}$ *if* $v=(i_1,\ldots,i_k)$.

(3) *If* P *contains some* 1*-dimensional affine subspace in* $\mathbf{R}^k$ *then* $\mathfrak{V}[P]=0$.

Proof. The first assertion simply means that $\mathfrak{V}$ is a valuation. The second follows from the fact that Φ is $\mathbf{R}[x_1,\ldots,x_k,x_1^{-1},\ldots,x_k^{-1}]$-linear. With respect to the third, we observe that if P contains a 1-dimensional subspace then we may suppose that this line is rationally defined; since P is closed and convex, it is the union of translates of this line and hence, $P\cap\mathbf{Z}^k$ is the union of cosets of a non-trivial subgroup of $\mathbf{Z}^k$. We then conclude using Corollary 2. □

We conjecture that the valuation $\mathfrak{V}$ is the same as the valuation $\mathfrak{F}$ of Lawrence [7] and Khovanskii and Pukhlikov [6] (see [3, Theorem 3.1]). It is also shown in [3] that $\mathfrak{F}$ has the following property: if for $(x_1,\ldots,x_k)\in\mathbf{C}^k$, the series $\sum_{v\in P}x^v$ converges absolutely, then its limit is equal to $\mathfrak{F}([P])(x_1,\ldots,x_k)$.

When $\mathbf{F}$ has an absolute value and is complete, it is likely that the following conjecture is true: let $S=\sum_{v\in\mathbf{Z}^k}\alpha_v x^v$ be a rational series as in Section 4 and f be its associated rational function as in Theorem 5. Suppose that $\sum_{v\in\mathbf{Z}^k}\alpha_v a^v$ converges absolutely for some k-tuple $(a_1,\ldots,a_k)\in\mathbf{F}^k$; then the limit is equal to $f(a_1,\ldots,a_k)$.

9. A counterexample

Observe that the definitions and the main results make sense in the following more general situation: $\mathbf{Z}^k$ is replaced by any group G and $\mathbf{F}(x_1,\ldots,x_k)$ by a field containing the group algebra $\mathbf{F}[G]$. The commutative case reduces to the case treated in this article, since G must be torsion-free (otherwise $\mathbf{F}[G]$ has no field of fractions) and since one may suppose that G is finitely generated. We show now that when G is the free group on two generators x, y, then Theorem 5 does not hold. Indeed let S be the sum of all elements of G. It is a well-known result of classical automata theory that G is an unambiguous subset of itself (cf. [4]): indeed, the set of reduced words, that is, of words containing no occurrence of a variable preceded or followed by its inverse, is easily seen to be recognizable by a finite automaton, hence unambiguously rational in the free monoid over $L=\{x,y,x^{-1},y^{-1}\}$. Thus S is a rational series in the sense of Section 4. More precisely, for $u\in L$, denote by S_u the sum in G of all reduced words which do not begin with u^{-1}. Then

$$S = 1 + xS_x + x^{-1}S_{x^{-1}} + yS_y + y^{-1}S_{y^{-1}}$$

and for any $u\in L$,

$$S_u = 1 + \sum_{v\in L-u^{-1}} vS_v.$$

This shows that S is defined by the triple (λ,A,γ), with $\lambda=(1,0,0,0,0)$, $\gamma=(1,1,1,1,1)^{\mathrm{T}}$ and

$$A = \begin{pmatrix} 0 & x & x^{-1} & y & y^{-1} \\ 0 & x & 0 & y & y^{-1} \\ 0 & 0 & x^{-1} & y & y^{-1} \\ 0 & x & x^{-1} & y & 0 \\ 0 & x & x^{-1} & 0 & y^{-1} \end{pmatrix}.$$

The matrix A^* is convergent, but the matrix $1-A$ is not invertible in any field containing the group algebra $\mathbf{F}[G]$. Indeed, denoting by R_i the ith row of $1-A$ (and not A!), it is easy to verify that

$$x(1-x)^{-1}R_2 + x^{-1}(1-x^{-1})^{-1}R_3 - (1-y)^{-1}yR_4 + (1-y)^{-1}R_5 = 0.$$

This example raises many interesting questions. In particular, we know that each rational subset of the free group is unambiguous. For which of them is the corresponding element of the free field defined?

Acknowledgements

The authors would like to thank Ira Gessel for interesting discussions on Ehrhart polynomials, rational polytopes and Popoviciu's theorem, which lead to the present

article; and also the anonymous referee, for his careful reading of the paper and useful suggestions.

References

[1] S. Eilenberg, Automata, Languages and Machines, Academic Press, San Diego, CA, 1974.
[2] S. Eilenberg, M.P. Schützenberger, Rational sets in commutative monoids, J. Algebra 13 (1969) 101–173.
[3] A. Barvinok, J.E, Pommersheim, An algorithmic theory of lattice points in polyhedra, in: L.J. Billera, A. Björner, C. Greene, R. Simion, R.P. Stanley (Eds.) New Perspectives in Algebraic Combinatorics, MSRI Publications, Volume 38, Cambridge University Press, Cambridge, 1999, pp. 91–147.
[4] M. Fliess, Deux applications de la représentation matricielle d'une série rationnelle non commutative, J. Algebra 19 (1971) 344–353.
[5] I. Gessel, Two theorems of rational power series, Utilitas Math. 19 (1981) 247–254.
[6] A.G. Khovanskii, A.V. Pukhlikov, The Riemann–Roch theorem for integrals and sums of quasipolynomials on virtual polytopes, Algebra Anal. 4 (4) (1992) 188–121 (in Russian); translation in St. Petersburg Math. J. 4 (4) (1993) 789–812.
[7] J. Lawrence, Rational-function-valued valuations on polyhedra, in: Discrete and Computational Geometry (New Brunswick, NJ, 1989/1990), DIMACS Series of Discrete Mathematics and Theoretical Computer Science, vol. 6, American Mathematical Society, Providence, RI, 1991, pp. 199–208.
[8] P. McMullen, R. Schneider, Valuations in convex bodies, in: Birkhäuser (Ed.) Convexity and its applications, Basel, MA, 1983, pp. 170–247.
[9] J. Sakarovitch, Kleene's theorem revisited, Trends, Techniques, and Problems in Theoretical Computer Science (Smolenice, 1986), Lecture Notes in Computer Science, vol. 281, Springer, Berlin, 1987, pp. 39–50.
[10] R.P. Stanley, Enumerative Combinatorics, vol I, Wadworth & Brooks/Cole, Monterey, CA, 1986.