

DANIEL KROB

Matrix versions of aperiodic K -rational identities

Informatique théorique et applications, tome 25, n° 5 (1991), p. 423-444.

http://www.numdam.org/item?id=ITA_1991__25_5_423_0

© AFCET, 1991, tous droits réservés.

L'accès aux archives de la revue « Informatique théorique et applications » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/legal.php>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

MATRIX VERSIONS OF APERIODIC K-RATIONAL IDENTITIES (*)

by Daniel KROB ⁽¹⁾

Abstract. – We present the K -*-algebra of K -rational expressions on a semiring K . Then we introduce the notion of formal star of a matrix. Finally, we show that the two aperiodic identities (S) and (M):

$$(S) \quad (a+b)^* \approx (a^*b)^* \cdot a^* \quad \text{and} \quad (M) \quad (ab)^* \approx 1 + a \cdot (ba)^* \cdot b$$

imply together their matrix versions.

Résumé. – Nous présentons la K -*-algèbre des expressions K -rationnelles sur un semi-anneau K . Nous introduisons ensuite la notion d'étoile formelle d'une matrice. Puis, nous montrons que les deux identités a périodiques (S) et (M) :

$$(S) \quad (a+b)^* \approx (a^*b)^* \cdot a^* \quad \text{et} \quad (M) \quad (ab)^* \approx 1 + a \cdot (ba)^* \cdot b$$

entraînent ensemble leurs versions matricielles.

0. INTRODUCTION

Formal language theory has grown in several directions according to the way a language is considered. First of all and strictly speaking, a language is a subset of the free monoid. But, a language can also be seen as a formal series with coefficients in the boolean semiring \mathcal{B} . These two viewpoints have been widely investigated in the study of rational languages.

But there is an other and much less studied viewpoint which consists in considering the *formal expression* that is used to write a rational language. We call it a *rational expression* associated with this language. This concept leads immediately to difficulties since the uniqueness of the representation of a language is lost. Thus this situation brings us naturally to the study of

(*) Received December 1989, revised July 1990.

(1) C.N.R.S. (L.I.T.P.), Laboratoire d'Informatique de Rouen, Université de Rouen, B.P. n° 118, 76134 Mont-Saint-Aignan, France.

rational identities, i. e. of the pairs of rational expressions that denote the same language. The most important problem in this area, initiated by Redko [12] and Conway [3], is to construct a system of rational identities that would permit to obtain by a rewriting process every possible rational identity; such a system will be called *complete*.

Several important results are known for a long time on this problem. Let us recall the three following positive ones. First a theorem of Salomaa [15] shows that there exists a complete system composed of an *axiom scheme* which allows to solve formally linear systems and of the two aperiodic identities:

$$(S) \quad (a+b)^* \approx (a^*b)^* \cdot a^* \quad \text{and} \quad (M) \quad (ab)^* \approx 1 + a \cdot (ba)^* \cdot b$$

Secondly two theorems of Redko [13, 12] (*see also [3,10]*) give respectively complete *identities systems* for *commutative* rational expressions ⁽¹⁾ and for rational expressions over a *one letter* alphabet. On the other hand, a negative result was obtained independently by Redko [12] and Conway [3]. It shows that every complete system of identities is necessarily infinite.

But the problem of constructing a complete system of rational identities on an arbitrary alphabet was still open, though Conway proposed in [3] three conjectures whose resolution would permit to obtain a complete system. We recently solved two of these problems (*cf. [8]*), hence obtaining the first “well described” complete system of rational identities. A fundamental step in our proof obliges us to associate with every finite monoid M a rational identity $P(M)$ whose interpretation is:

$$A_M^* = \sum_{m \in M} \varphi_M^{-1}(m)$$

where $A_M = \{a_m, m \in M\}$ is an alphabet indexed by M and where φ_M is the monoid morphism from A_M^* into M which maps every letter $a_m \in A_M$ on m . Indeed it can be proved (*see [8]*) that the system composed of the identities $P(M)$ for all finite monoids and of the two aperiodic identities is complete. We can now also explain why (M) and (S) are called aperiodic identities: indeed, a monoid identity $P(M)$ is a consequence of (M) and (S) iff M is an aperiodic monoid (*see [8, 9]*).

However the formal construction of the identity $P(M)$ requires to compute the star of a rational expression matrix. But it is not possible to define

(¹) The first “good” proof of this result is from Pilling [10]

intrinsically such a star. The miracle is that this definition can be given if we accept to work modulo the two aperiodic identities. This explains the fundamental place (see [7, 8, 9]) of the identities (M) and (S) in the theory of rational identities. The present paper is completely devoted to the proof of this result in a more general framework.

Indeed we present here rational expressions with multiplicities in an arbitrary semiring K . This extends the usual rational expressions (appearing now as \mathcal{B} -rational expressions) exactly as the non commutative series over K generalize the rational languages. In this framework, we prove that (M) and (S) imply their matrix versions. This result though claimed obvious by Conway [3] is very long and cumbersome to prove. It permits us in particular to define modulo (M) , (S) the star of a matrix whose entries are rational expressions. Note that it also has other important consequences (cf. [8]).

Let us finally end with the structure of this paper. First section II is devoted to the presentation of the K - \star -algebra of K -rational expressions in the Kleene and the general case. In section III, we present the notions of K -rational identity and of deduction. Finally section IV is devoted to the proof of our main result.

I. PRELIMINARIES

We shall refer to [1] and to [4] for the definitions of a *semiring* and of a *K-algebra*. In the sequel, K will always denote a *commutative* semiring. Let us now recall some definitions from [4], [6] and [14]:

DEFINITION I. 1: A semiring $(K, +, \cdot)$ is said to be *countably complete* (or more simply *c-complete*) if and only if for each countable set I , there exists a mapping Σ_I from K^I into K such that:

- (i) For every finite set I and for every family $(x_i)_{i \in I} \in K^I$, we have:

$$\Sigma_I(x_i)_{i \in I} = \sum_{i \in I} x_i.$$

- (ii) For every countable set I , for every partition $(J_j)_{j \in J}$ of I and for every family $(x_i)_{i \in I}$ in K^I , we have:

$$\Sigma_I(x_i)_{i \in I} = \Sigma_J[\Sigma_{J_j}(x_i)_{i \in J_j}]_{j \in J}.$$

(iii) For every countable sets I and J and for every families $(x_i)_{i \in I}$ and $(y_j)_{j \in J}$ respectively in K^I and K^J , we have:

$$\sum_{I \times J} (x_i y_j)_{(i,j) \in I \times J} = (\sum_I (x_i)_{i \in I}) (\sum_J (y_j)_{j \in J}).$$

Remark: We shall equip every c -complete semiring K with the *star* operation defined as follows:

$$\forall k \in K, \quad k^* = \sum_{n \in \mathbb{N}} k^n.$$

DEFINITION I.2: A semiring K is said to be a *Kleene semiring* if and only if K is a \star -stable subsemiring of a c -complete semiring \mathcal{K} . This means that:

$$\forall k \in K, \quad k^* \in K.$$

Notes: 1. In fact these two definitions give just “good” generalizations of the boolean semiring \mathcal{B} on which is based classical language theory. The reader will refer to [6] in order to find examples of c -complete semirings.

2. Let us also recall that when K is a positive semiring (see [4, 6]), it is possible to embed K in the c -complete semiring $\mathcal{K} = K \cup \{\infty\}$ obtained from K by adding an absorbing element ∞ for addition and multiplication by non zero elements and whose summation is defined by:

$$\forall (k_i)_{i \in I} \in \mathcal{K}^I, \quad \sum_I (k_i) = \begin{cases} \sum_{i \in I} k_i & \text{if } I \text{ is finite} \\ \infty & \text{if } I \text{ is infinite} \end{cases}$$

This technique permits us to embed natural and usual positive semirings (like \mathbb{N} , \mathbb{Q}^+ or \mathbb{R}^+) in Kleene semirings.

DEFINITION I.3 [4, 7]: Let K be a semiring. Then, a K - \star -algebra \mathcal{A} is just a K -algebra equipped with a mapping \star from \mathcal{A} into \mathcal{A} .

When an algebraic structure is defined, it is always important to look on the corresponding morphisms. Here, if two K - \star -algebras \mathcal{C} and \mathcal{D} are given, we shall say that a mapping φ from \mathcal{C} into \mathcal{D} is a K - \star -morphism if and only if it is a morphism of K -algebras such that:

$$\forall x \in \mathcal{C}, \quad \varphi(x^*) = [\varphi(x)]^*.$$

It is easy to see that the class of K - \star -algebras equipped with K - \star -morphisms is a category.

Let us finally recall that $K \ll A^* \gg$ is the algebra of non commutative formal series over K on the alphabet A . A series $S \in K \ll A^* \gg$ is denoted by:

$$S = \sum_{w \in A^*} (S|w)w \quad \text{where } (S|w) \in K.$$

In particular, a series S will be called *proper* iff its *constant term* $(S|1)$ is equal to 0. We can define a star operation in $K \ll A^* \gg$ by the relation:

$$S^* = \sum_{n=0}^{\infty} S^n$$

which makes sense for every series S when K is a Kleene semiring and only for the proper ones in the general semiring case (see [1, 7]).

II. K-RATIONAL EXPRESSIONS

1. The K - \star -algebra of K -rational expressions over a Kleene semiring

In this section, K will always be a Kleene semiring. Let us now consider an alphabet A . Let Σ be the union of the sets $\Sigma(0)$, $\Sigma(1)$ and $\Sigma(2)$ of 0-ary, 1-ary and 2-ary product symbols which are respectively defined by:

$$\Sigma(0) = \{ \emptyset, \Lambda \}, \quad \Sigma(1) = \{ \star \} \cup K \quad \text{and} \quad \Sigma(2) = \{ +, . \}.$$

Then we can consider the free Σ -algebra $\mathcal{F} = F(\Sigma, A)$ constructed on A (cf. [5]). Let us introduce now the smallest Σ -algebra congruence \equiv of \mathcal{F} that identifies every pair of elements of \mathcal{F} corresponding to an axiom of the structure of K -algebra and that satisfies the relations:

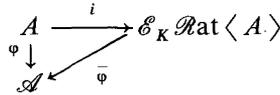
$$(\mathcal{C}\star) \quad \forall k \in K, \quad (k.\Lambda)^* \equiv k^*.\Lambda.$$

Then the K - \star -algebra of K -rational expressions over A is defined as the quotient algebra: $\mathcal{E}_K \mathcal{Rat} \langle A \rangle = \mathcal{F} / \equiv$. In order to give the fundamental property of $\mathcal{E}_K \mathcal{Rat} \langle A \rangle$, let us recall (cf. [7] for more details) that a K - \star -bound-algebra \mathcal{A} is a K - \star -algebra satisfying the condition:

$$\forall k \in K, \quad (k.1_{\mathcal{A}})^* = k^*.1_{\mathcal{A}}$$

which assures a compatibility between the star in K and the star in \mathcal{A} . The class of K - \star -bound-algebras equipped with K - \star -morphisms forms a category that admits $\mathcal{E}_K \mathcal{Rat} \langle A \rangle$ as an universal object relatively to the set category (see [5, 7]) as shows the following result:

PROPOSITION II.1 [7]: Let K be a Kleene semiring and let φ be a mapping from an alphabet A into a K - \star -bound-algebra \mathcal{A} . Then there is a unique K - \star -morphism $\bar{\varphi}$ from $\mathcal{E}_K \mathcal{Rat} \langle A \rangle$ in \mathcal{A} which extends φ , i.e. such that the following diagram is commutative (where i denotes the natural injection):



Consequences: 1. When K is a Kleene semiring, the K -algebra $K \ll A^* \gg$ has a natural structure of K - \star -bound-algebra. Hence, according to prop. II.1, we can define the *interpretation* mapping ε : it is the unique K - \star -morphism from $\mathcal{E}_K \mathcal{Rat} \langle A \rangle$ into $K \ll A^* \gg$ which satisfies the relations:

$$\forall a \in A, \quad \varepsilon(a) = a \quad (int)$$

2. In the same way, we can define the *constant coefficient* mapping c : it is the unique K - \star -morphism from $\mathcal{E}_K \mathcal{Rat} \langle A \rangle$ into K such that we have:

$$\forall a \in A, \quad c(a) = 0$$

3. More generally, a *substitution* σ will be any K - \star -morphism from $\mathcal{E}_K \mathcal{Rat} \langle A \rangle$ into $\mathcal{E}_K \mathcal{Rat} \langle A \rangle$. By proposition II.1, σ can be defined only by its image on A .

2. The K -algebra of K -rational proper expressions

When K is a general semiring, we must restrict the notion of K -rational expression. Indeed the star of an expression whose constant coefficient is not zero can not now have an interpretation in $K \ll A^* \gg$. This leads us to the construction of the K -algebra of proper K -rational expressions.

Hence let us define a mapping denoted \star from K into K by: $k^* = 1$ for every $k \in K$. We can now give a formal existence to $\mathcal{E}_K \mathcal{Rat} \langle A \rangle$ which is the K - \star -algebra constructed by the same method than the one used in section 1. Then we can define $\mathcal{P} \mathcal{E}_K \mathcal{Rat} \langle A \rangle$: it is the smallest K -subalgebra \mathcal{P} of $\mathcal{E}_K \mathcal{Rat} \langle A \rangle$ containing A and satisfying the following property:

$$c(E) = 0 \quad \text{and} \quad E \in \mathcal{P} \Rightarrow E^* \in \mathcal{P}.$$

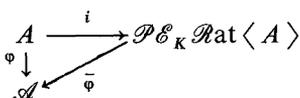
This condition obliges to restrict the star in $\mathcal{P} \mathcal{E}_K \mathcal{Rat} \langle A \rangle$ to expressions whose constant coefficient is zero. Then $\mathcal{P} \mathcal{E}_K \mathcal{Rat} \langle A \rangle$ will be called the *K -algebra of proper K -rational expressions* over the alphabet A . Let us now

recall (cf. [7]) that a $K\text{-}\star\text{-}0\text{-bound-algebra } \mathcal{A}$ is a $K\text{-}\star\text{-algebra } \mathcal{A}$ such that: $0_{\mathcal{A}}^{\star} = 1_{\mathcal{A}}$. Then we can give the following universal property of $\mathcal{P}\mathcal{E}_K\mathcal{Rat}\langle A \rangle$:

PROPOSITION II.2 [7]: *Let K be a semiring, let A be an alphabet and let φ be a mapping from A into a $K\text{-}\star\text{-}0\text{-bound-algebra } \mathcal{A}$. Then, there exists a unique $K\text{-morphism } \bar{\varphi}$ from $\mathcal{P}\mathcal{E}_K\mathcal{Rat}\langle A \rangle$ into \mathcal{A} satisfying the property:*

$$\forall E \in \mathcal{P}\mathcal{E}_K\mathcal{Rat}\langle A \rangle, \quad c(E) = 0 \quad \Rightarrow \quad \bar{\varphi}(E^{\star}) = [\bar{\varphi}(E)]^{\star} \quad (\mathcal{LM})$$

which extends φ , i. e. such that the following diagram commutes (where i is the natural injection):



Note: A $K\text{-algebra morphism } \psi$ from $\mathcal{P}\mathcal{E}_K\mathcal{Rat}\langle A \rangle$ into a $K\text{-}\star\text{-}0\text{-bound-algebra } \mathcal{A}$ which satisfies (\mathcal{LM}) will be said to be a *local $K\text{-}\star\text{-morphism}$.*

Consequences: 1. Using proposition II.2, it is easy to define the *interpretation mapping* ε : it is the unique $K\text{-morphism}$ from $\mathcal{P}\mathcal{E}_K\mathcal{Rat}\langle A \rangle$ into $K \ll A^{\star} \gg$ which satisfies the relations (int) and the property:

$$\forall E \in \mathcal{P}\mathcal{E}_K\mathcal{Rat}\langle A \rangle, \quad c(E) = 0 \quad \Rightarrow \quad (\varepsilon(E) | 1) = 0 \quad \text{and} \quad \varepsilon(E^{\star}) = [\varepsilon(E)]^{\star}$$

2. We can equip $\mathcal{P}\mathcal{E}_K\mathcal{Rat}\langle A \rangle$ with a $K\text{-}\star\text{-}0\text{-bound-algebra}$ structure by extending formally the star with $E^{\star} = 0$ when $c(E) \neq 0$. Then we say that a $K\text{-morphism } \sigma$ from $\mathcal{P}\mathcal{E}_K\mathcal{Rat}\langle A \rangle$ into $\mathcal{P}\mathcal{E}_K\mathcal{Rat}\langle A \rangle$ is a *proper substitution* if and only if it is a local $K\text{-}\star\text{-morphism}$ satisfying the condition:

$$\forall a \in A, \quad c(\sigma(a)) = 0 \quad (\mathcal{PS}).$$

Thus $c \circ \sigma$ and c are local $K\text{-}\star\text{-endomorphisms}$ of $\mathcal{P}\mathcal{E}_K\mathcal{Rat}\langle A \rangle$ which are equal on A . It follows by prop. II.2 that they are equal on $\mathcal{P}\mathcal{E}_K\mathcal{Rat}\langle A \rangle$, i. e. that:

$$\forall E \in E, \quad c(E) = 0 \quad \Rightarrow \quad c(\sigma(E)) = 0.$$

Thus, when the star of an expression $E \in \mathcal{P}\mathcal{E}_K\mathcal{Rat}\langle A \rangle$ can be taken in the usual sense [i. e. when $c(E) = 0$], $\sigma(E^{\star})$ is equal to the usual star of $\sigma(E)$. Hence the above star extension does not play any role for proper substitutions.

Remark: We can show that $\mathcal{P}\mathcal{E}_K\mathcal{Rat}\langle A \rangle$ embeds in $\mathcal{E}_K\mathcal{Rat}\langle A \rangle$ when K is Kleene (see [7]). This proves that the two theories are related when K is Kleene.

Note: In the sequel, when we will speak of K -rational expressions or of substitutions, we will refer to section II.1 or to section II.2 according as K is a Kleene or an arbitrary semiring.

III. K -RATIONAL IDENTITIES

1. K -rational identities

DEFINITION III.1: Let E, F be two K -rational expressions on the alphabet A . Then we shall say that (E, F) is a K -rational identity if and only if we have in $\mathcal{E}_K\mathcal{Rat}\langle A \rangle : \varepsilon(E) = \varepsilon(F)$. We shall denote it by: $E \approx F$.

As proved in [7], all the identities that follow are K -rational identities. They were introduced by Conway [3] in the boolean semiring case:

Exemples: 1. [8, 9] *Aperiodic identities:*

$$(M) \quad (ab)^* \approx 1 + a(ba)^*b \quad \text{and} \quad (S) \quad (a+b)^* \approx (a^*b)^*a^*$$

2. *Cyclic identities:*

$$\forall n \in \mathbb{N}, \quad (P(n)) \quad a^* \approx (1 + a + \dots + a^{n-1})(a^n)^*$$

3. “*Star-definition*” identities:

$$(A_l) \quad a^* \approx 1 + aa^* \quad \text{and} \quad (A_r) \quad a^* \approx 1 + a^*a.$$

The family consisting of all the identities given in 1 and 2 was called system of *classical identities* by Conway (see [3]).

Remark: In [3], Conway considered the \mathcal{B} -rational expressions as elements of the corresponding free Σ -algebra over A . His classical system was composed of the pairs of identities associated with the algebra rules, of (M) , (S) and of $(P(n))_{n \geq 2}$. This is equivalent to the algebraic viewpoint we took here.

2. Deduction

DEFINITION III.2: Let \mathcal{S} be a system of K -rational identities on the alphabet A . Then we shall say that a sequence $(E_i, F_i)_{i=1, n}$ of K -rational

identities is a \mathcal{S} -deduction iff one of the following cases holds for every $k < n$:

- (i) $(E_k, F_k) \in \mathcal{S}$
- (ii) $\exists i, j < k, (E_i + E_j, F_i + F_j) = (E_k, F_k)$ or $\exists i, j < k, (E_i \cdot E_j, F_i \cdot F_j) = (E_k, F_k)$ or $\exists i < k, (E_i^*, F_i^*) = (E_k, F_k)$ or $\exists i < k, \exists k \in K, (k \cdot E_i, k \cdot F_i) = (E_k, F_k)$
- (iii) $E_k = F_k$ or $\exists i, j < k, \exists U, (E_i, F_i) = (E_k, U)$ and $(E_j, F_j) = (U, F_k)$ or $\exists i < k, (E_k, F_k) = (F_i, E_i)$
- (iv) $\exists i < k, \exists \sigma$ substitution, $(E_k, F_k) = (\sigma(E_i), \sigma(F_i))$.

A K -rational identity (E, F) is then said to be a \mathcal{S} -consequence if and only if there exists a \mathcal{S} -deduction ending with (E, F) .

Notation: If $E \approx F$ is a consequence of \mathcal{S} , we will denote it by:

$$\mathcal{S} \vdash E \approx F \quad \text{or} \quad \vdash^{\mathcal{S}} E \approx F$$

Note: Definition III.2 is consistent: indeed each pair of K -rational expressions that can appear in a deduction is necessarily an identity (cf. [7]).

Example [7]: When K is Kleene, we have the *star-star identity*:

$$(M) \wedge (S) \vdash a^{**} \approx (1^* a)^* \cdot 1^*$$

The following proposition shows that the *symmetrical* version of (S) is a (M) - (S) consequence (see also [7]):

PROPOSITION III.1 (Conway; [3]): *For every semiring K , we have:*

$$(M) \wedge (S) \vdash (a + b)^* \approx a^* (ba^*)^*$$

Proof: – To prove this identity, it suffices to write:

$$\begin{aligned} (S) \vdash (a + b)^* &\approx (a^* b)^* a^* \\ &\vdash^{(M)} (a + b)^* \approx (1 + a^* (ba^*) b) \cdot a^* = a^* (1 + (ba^*)^* ba^*) \\ &\vdash^{(A_*)} (a + b)^* \approx a^* (ba^*)^* \end{aligned}$$

Since (A_*) is a consequence of (M) , this ends our proof. ■

IV. MATRIX IDENTITIES

1. Matrix identities

We can extend all definitions of the previous section to matrices. First we may define the *interpretation* mapping ε from $\mathcal{M}_{n \times m}(\mathcal{E}_K \text{Rat} \langle A \rangle)$ (resp. from $\mathcal{M}_{n \times m}(\mathcal{PE}_K \text{Rat} \langle A \rangle)$) into $\mathcal{M}_{n \times m}(K \ll A^* \gg)$ by:

$$\varepsilon(M) = [\varepsilon(M_{i,j})]_{1 \leq i \leq n, 1 \leq j \leq m}$$

We also use the same method to define the *constant coefficient* matrix $c(M)$ of a matrix M . Then a matrix M will be said to be *proper* iff $c(M) = 0$.

We shall now say that a pair (M, N) of matrices in $\mathcal{M}_{n \times m}(\mathcal{E}_K \text{Rat} \langle A \rangle)$ (resp. in $\mathcal{M}_{n \times m}(\mathcal{PE}_K \text{Rat} \langle A \rangle)$) forms a *matrix identity* iff we have: $\varepsilon(M) = \varepsilon(N)$. We shall denote it by: $M \approx N$. We can also extend the notion of deduction: a matrix identity (M, N) will be said to be a *consequence* of a family \mathcal{S} of K -rational identities iff we have:

$$\forall i \in [1, n], \forall j \in [1, m], \mathcal{S} \vdash M_{i,j} \approx N_{i,j}$$

As in the usual case, we shall denote it by: $\mathcal{S} \vdash M \approx N$.

The following proposition (left to the reader) shows that a matrix deduction acts relatively to the K -algebra operations as a usual deduction:

PROPOSITION IV.1: *Let \mathcal{S} be a system of K -rational identities and let M, N, P, Q be matrices whose entries are K -rational expressions. When the following relations make sense, we have:*

$$\left. \begin{array}{l} \mathcal{S} \vdash M \approx N \\ \mathcal{S} \vdash P \approx Q \end{array} \right\} \Rightarrow \left\{ \begin{array}{l} \mathcal{S} \vdash M \cdot P \approx N \cdot Q \\ \mathcal{S} \vdash M + P \approx N + Q \end{array} \right.$$

2. The formal star of a matrix

The matrices of K -rational expressions have a natural K -algebra structure. We are now going to see how to equip them with a star operation.

Recall [2]: $\mathcal{M}g$ will denote the free magma constructed on the one element set $\{x\}$. Let us recall that $\mathcal{M}g$ is the union of the sequence $(\mathcal{M}g_n)_{n \in \mathbb{N}}$ of sets which are constructed inductively as follows: we have $\mathcal{M}g_1 = \{x\}$; then, for every $n \geq 2$, $\mathcal{M}g_n$ is the sum of the sets $\mathcal{M}g_p \times \mathcal{M}g_{n-p}$ for $p \in [1, n-1]$. Observe that $\mathcal{M}g$ is exactly the set of complete binary trees.

DEFINITION IV.1: Let K be a Kleene (resp. a general) semiring, let $n \geq 1$ be an integer and let M be a matrix (resp. a proper matrix) in $\mathcal{M}_{n \times n}(\mathcal{E}_K \mathcal{R}at \langle A \rangle)$ [resp. in $\mathcal{M}_{n \times n}(\mathcal{PE}_K \mathcal{R}at \langle A \rangle)$]. Then, for every $\omega \in \mathcal{M}g_n$, we will denote by M_ω^* the star of M relatively to ω that is inductively defined as follows:

- (i) If $n = 1$, M_ω^* is just the usual star of the K -rational expression $M_{1,1}$.
- (ii) If $n \geq 2$, there exists a unique pair (p, q) in $\mathbb{N}^* \times \mathbb{N}^*$ with $p + q = n$ such that $\omega = (\alpha, \beta)$ with $\alpha \in \mathcal{M}g_p$ and $\beta \in \mathcal{M}g_q$. Then we can cut M as follows:

$$M = \begin{matrix} & \begin{matrix} p & q \end{matrix} \\ \begin{matrix} p \\ q \end{matrix} & \begin{pmatrix} A & B \\ C & D \end{pmatrix} \end{matrix}$$

Then M_ω^* is defined by:

$$M_\omega^* = \begin{matrix} & \begin{matrix} p & q \end{matrix} \\ \begin{matrix} p \\ q \end{matrix} & \begin{pmatrix} (A + BD_\beta^* C)_\alpha^* & A_\alpha^* B (D + CA_\alpha^* B)_\beta^* \\ D_\beta^* C (A + BD_\beta^* C)_\alpha^* & (D + CA_\alpha^* B)_\beta^* \end{pmatrix} \end{matrix}$$

We recall without proof the following result. It shows that the previous definition is consistent with the natural star in $\mathcal{M}_{n \times n}(K \langle\langle A^* \rangle\rangle)$ which comes from its isomorphism with $\mathcal{M}_{n \times n}(K) \langle\langle A^* \rangle\rangle$:

PROPOSITION IV.2 [7]: Let K be a Kleene (resp. a general) semiring, let $n \geq 1$ be an integer and let M be a matrix of $\mathcal{M}_{n \times n}(\mathcal{E}_K \mathcal{R}at \langle A \rangle)$ (resp. a proper matrix of $\mathcal{M}_{n \times n}(\mathcal{PE}_K \mathcal{R}at \langle A \rangle)$). Then, for every element $\omega \in \mathcal{M}g_n$, we have:

(1) $\varepsilon(M_\omega^*) = [\varepsilon(M)]^*$.

Consequence: For every $(\mu, \nu) \in \mathcal{M}g_n \times \mathcal{M}g_n$ and for every square matrix (possibly proper) M of order n , we have the following matrix identity:

$$M_\mu^* \approx M_\nu^*$$

which is not in general an equality in $\mathcal{M}_{n \times n}(\mathcal{E}_K \mathcal{R}at \langle A \rangle)$ or in $\mathcal{M}_{n \times n}(\mathcal{PE}_K \mathcal{R}at \langle A \rangle)$.

The following result, that the reader will easily prove by induction on n , is similar to proposition IV.1:

PROPOSITION IV.3: Let K be a Kleene (resp. a general) semiring, let \mathcal{S} be a system of K -rational identities and let M, N be two $n \times n$ matrices (resp. proper

matrices) of K -rational expressions. Then, for every $\omega \in \mathcal{M}g_n$, we have:

$$\mathcal{S} \vdash M \approx N \Rightarrow \mathcal{S} \vdash M_\omega^* \approx N_\omega^*.$$

3. Matrix versions of aperiodic identities

We will prove in this section the main result of this paper: it shows that the two aperiodic identities imply their matrix versions. But we will first prove the following result:

PROPOSITION IV.4 [7]: *Let K be a Kleene (resp. a general) semiring, let $n \geq 1$ be an integer and let M be a matrix (resp. a proper matrix) of $\mathcal{M}_{n \times n}(\mathcal{E}_K \mathcal{R} \text{ at } \langle A \rangle)$ [resp. of $\mathcal{M}_{n \times n}(\mathcal{P}\mathcal{E}_K \mathcal{R} \text{ at } \langle A \rangle)$]. Then, for every element ω of $\mathcal{M}g_n$, we have:*

$$(A_l) \vdash M_\omega^* \approx I_n + M M_\omega^* \quad \text{and} \quad (A_r) \vdash M_\omega^* \approx I_n + M_\omega^* M.$$

Proof: – We will only prove the first of these two identities in the Kleene semiring case since the arguments are similar in the other cases. To show our result, we will use an induction on the order n of M . For $n = 1$, the result is clear. Hence let us suppose $n \geq 2$ and our result true at any order $l < n$. Then let M be a matrix of $\mathcal{M}_{n \times n}(\mathcal{E}_K \mathcal{R} \text{ at } \langle A \rangle)$ and let $\omega = (u, v)$ be an element of $\mathcal{M}g_n$ with $u \in \mathcal{M}g_p$, $v \in \mathcal{M}g_q$ and $p + q = n$. Thus we can write:

$$M = \begin{matrix} & \begin{matrix} p & q \end{matrix} \\ \begin{matrix} p \\ q \end{matrix} & \begin{pmatrix} A & B \\ C & D \end{pmatrix} \end{matrix}$$

According to definition IV.1, an easy computation shows that:

$$\begin{aligned} & I_n + M \cdot M_\omega^* \\ &= \begin{matrix} p & q \\ q & \end{matrix} \left(\begin{matrix} I_p + (A + B D_v^* C)(A + B D_v^* C)_u^* & (A A_u^* + I_p) B (D + C A_u^* B)_v^* \\ (D D_v^* + I_q) C (A + B D_v^* C)_u^* & I_q + (C A_u^* B + D) (D + C A_u^* B)_v^* \end{matrix} \right) \end{aligned}$$

Therefore, by the induction hypothesis applied at orders p and q , by proposition IV.1 and by definition IV.1, it is straightforward to conclude that:

$$(A_l) \vdash M_\omega^* \approx I_n + M \cdot M_\omega^*$$

Hence our proposition is proved. ■

Let us now give our main result. Observe that the situation is here not the same as in the previous proposition: indeed, the identities (M) and (S) do not imply independently their matrix versions.

THEOREM IV.5 [7]: *Let K be a Kleene (resp. a general) semiring, let $n, m \geq 1$ be two integers, let M, N be two $n \times m$ and $m \times n$ matrices (resp. proper matrices) of K -rational expressions and let P, Q be two $n \times n$ matrices (resp. proper matrices) of K -rational expressions. Then the following deductions hold for every $\nu \in \mathcal{M}g_n$ and $\mu \in \mathcal{M}g_m$:*

$$(M) \wedge (S) \mid \text{---} (MN)_\nu^* \approx I_n + M(NM)_\mu^* N$$

$$(M) \wedge (S) \mid \text{---} (P + Q)_\nu^* \approx (P_\nu^* Q_\nu^*)^* P_\nu^*$$

Proof. — Since the proof is similar in the general case, we will only do it when K is Kleene. More precisely, we will show by induction on k that, for every matrices M, N of order (i, j) and (j, i) with $i, j \leq k$ and for every square matrices P, Q of order $\leq k$, we have:

$$(M) \wedge (S) \mid \text{---} (MN)_\nu^* \approx I_n + M(NM)_\mu^* N$$

$$(M) \wedge (S) \mid \text{---} (P + Q)_\nu^* \approx (P_\nu^* Q_\nu^*)^* P_\nu^*$$

This result is obvious for $k=1$. Let us now suppose it being proved at the order $k-1$ with $k \geq 2$. According to proposition III.1's proof and to proposition IV.1, it follows obviously that the symmetrical version of (S):

$$(M) \wedge (S) \mid \text{---} (P + Q)_\nu^* \approx P_\nu^* (QP_\nu^*)^*$$

holds for every square matrices P, Q of order $\leq k-1$:

1st step: Computation of the matrix version of (M).

Let $m, n \leq k$ and let M, N be two matrices respectively in $\mathcal{M}_{n \times m}(\mathcal{E}_K \mathcal{R} \text{ at } \langle A \rangle)$ and in $\mathcal{M}_{m \times n}(\mathcal{E}_K \mathcal{R} \text{ at } \langle A \rangle)$. Then let $\nu = (\alpha, \beta) \in \mathcal{M}g_n$ and $\mu = (\gamma, \delta) \in \mathcal{M}g_m$ with $\alpha \in \mathcal{M}g_p, \beta \in \mathcal{M}g_q, \gamma \in \mathcal{M}g_r$ and $\delta \in \mathcal{M}g_s$, where $p + q = n$ and $r + s = m$. Thus we can write:

$$M = \begin{matrix} & \begin{matrix} r & s \end{matrix} \\ \begin{matrix} p \\ q \end{matrix} & \begin{pmatrix} A & B \\ C & D \end{pmatrix} \end{matrix} \quad \text{and} \quad N = \begin{matrix} & \begin{matrix} p & q \end{matrix} \\ \begin{matrix} r \\ s \end{matrix} & \begin{pmatrix} E & F \\ G & H \end{pmatrix} \end{matrix}$$

Hence it follows that:

$$N.M = \begin{matrix} r \\ s \end{matrix} \begin{pmatrix} EA + FC & EB + FD \\ GA + HC & GB + HD \end{pmatrix} = \begin{pmatrix} \mathcal{W} & \mathcal{X} \\ \mathcal{Y} & \mathcal{Z} \end{pmatrix}$$

Let us introduce:

$$\Phi = \mathcal{W} + \mathcal{X} . \mathcal{Z}_\delta^* . \mathcal{Y} \quad \text{and} \quad \Gamma = \mathcal{Z} + \mathcal{Y} . \mathcal{W}_\gamma^* . \mathcal{X}$$

According to definition IV.1, we obtain:

$$M(NM)_\mu^* N = \begin{pmatrix} (A + B \mathcal{Z}_\delta^* \mathcal{Y}) \Phi_\gamma^* E + (A \mathcal{W}_\gamma^* \mathcal{X} + B) \Gamma_\delta^* G & (A + B \mathcal{Z}_\delta^* \mathcal{Y}) \Phi_\gamma^* F + (A \mathcal{W}_\gamma^* \mathcal{X} + B) \Gamma_\delta^* H \\ (C + D \mathcal{Z}_\delta^* \mathcal{Y}) \Phi_\gamma^* E + (C \mathcal{W}_\gamma^* \mathcal{X} + D) \Gamma_\delta^* G & (C + D \mathcal{Z}_\delta^* \mathcal{Y}) \Phi_\gamma^* F + (C \mathcal{W}_\gamma^* \mathcal{X} + D) \Gamma_\delta^* H \end{pmatrix}$$

2nd step: Computation of the matrix version of (S).

Let P, Q be two matrices of $\mathcal{M}_{k \times k}(\mathcal{E}_K \mathcal{R} \text{ at } \langle A \rangle)$ and let $v = (u, v)$ be in $\mathcal{M}g_k$ with $u \in \mathcal{M}g_p, v \in \mathcal{M}g_q$ and $p + q = k$. Then, we can write:

$$P = \begin{matrix} p & q \\ & \end{matrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} \quad \text{and} \quad Q = \begin{matrix} p & q \\ & \end{matrix} \begin{pmatrix} E & F \\ G & H \end{pmatrix}.$$

According to definition IV.1, we have:

$$\begin{aligned} QP_v^* &= \begin{pmatrix} (E + FD_v^* C)(A + BD_v^* C)_u^* & (EA_u^* B + F)(D + CA_u^* B)_v^* \\ (G + HD_v^* C)(A + BD_v^* C)_u^* & (GA_u^* B + H)(D + CA_u^* B)_v^* \end{pmatrix} \\ &= \begin{pmatrix} \mathcal{W} & \mathcal{X} \\ \mathcal{Y} & \mathcal{Z} \end{pmatrix} \end{aligned}$$

Let us introduce the following denotations:

$$\begin{aligned} \Phi &= A + B . D_v^* . C & \text{and} & \quad \Gamma = D + C . A_u^* . B \\ \mathcal{P} &= \mathcal{W} + \mathcal{X} . \mathcal{Z}_v^* . \mathcal{Y} & \text{and} & \quad \mathcal{Q} = \mathcal{Z} + \mathcal{Y} . \mathcal{W}_u^* . \mathcal{X} \end{aligned}$$

Therefore, according to definition IV.1, we can now write:

$$P_v^* (QP_v^*)_v^* = \begin{pmatrix} (\Phi_u^* + A_u^* B \Gamma_v^* \mathcal{Z}_v^* \mathcal{Y}) \mathcal{P}_u^* & (\Phi_u^* \mathcal{W}_u^* \mathcal{X} + A_u^* B \Gamma_v^*) \mathcal{Q}_v^* \\ (D_v^* C \Phi_u^* + \Gamma_v^* \mathcal{Z}_v^* \mathcal{Y}) \mathcal{P}_u^* & (D_v^* C \Phi_u^* \mathcal{W}_u^* \mathcal{X} + \Gamma_v^*) \mathcal{Q}_v^* \end{pmatrix}$$

3rd step: Study of particular cases.

We shall prove here several lemmas: they show all that particular matrix versions of (M) and (S) are still consequences of (M) and (S). We shall first study two particular cases of the identity (S):

LEMMA IV.6: When $C = D = 0$ in the matrix P of the second step, we have:

$$(M) \wedge (S) \mid \text{---} (P + Q)_v^* \approx P_v^* (QP_v^*)^*.$$

Proof. — Indeed, it follows from our computations that we have here:

$$P_v^* (QP_v^*)^* = \begin{pmatrix} A_u^* (I_p + B \mathcal{L}_v^* G A_u^*) \mathcal{P}_u^* & A_u^* (B + \mathcal{W}_v^* \mathcal{X}) Q_v^* \\ \mathcal{L}_v^* G A_u^* \mathcal{P}_u^* & \mathcal{Q}_v^* \end{pmatrix} \tag{0}$$

where we defined

$$\begin{aligned} \mathcal{W} &= EA_u^*, & \mathcal{L} &= GA_u^* B + H, & \mathcal{X} &= EA_u^* B + F \\ \mathcal{Q} &= \mathcal{L} + GA_u^* \mathcal{W}_v^* \mathcal{X} & \text{and} & & \mathcal{P} &= \mathcal{W} + \mathcal{X} \mathcal{L}_v^* G A_u^* \end{aligned}$$

We are now going to study each entry of (0). First let us look at \mathcal{Q} :

$$\mathcal{Q} = H + GA_u^* \cdot ((I_p + (EA_u^*)_u^* EA_u^*) B + (EA_u^*)_u^* F)$$

Applying first propositions IV.4 and IV.1, using then the induction hypothesis with proposition IV.1 and applying finally proposition IV.3, we obtain:

$$\begin{aligned} (M) \mid \text{---} \mathcal{Q} &\approx H + GA_u^* (EA_u^*)_u^* (B + F) \\ \mid \xrightarrow{(M), (S)} \mathcal{Q} &\approx H + G (E + A)_u^* (B + F) \\ \mid \text{---} \mathcal{Q}_v^* &\approx [H + G (E + A)_u^* (B + F)]_v^* \end{aligned} \tag{1}$$

But, we also have:

$$A_u^* (B + \mathcal{W}_u^* \mathcal{X}) = A_u^* \cdot ((I_p + (EA_u^*)_u^* EA_u^*) B + (EA_u^*)_u^* F)$$

By propositions IV.4 and IV.1 and by the induction hypothesis, we immediately have:

$$\begin{aligned} (M) \mid \text{---} A_u^* (B + \mathcal{W}_u^* \mathcal{X}) &\approx A_u^* (EA_u^*)_u^* (B + F) \\ \mid \xrightarrow{(S), (M)} A_u^* (B + \mathcal{W}_u^* \mathcal{X}) &\approx (E + A)_u^* (B + F) \end{aligned} \tag{2}$$

Let us now study \mathcal{P} . First we have:

$$\mathcal{P} = EA_u^* + (EA_u^* B + F)(GA_u^* B + H)_v^* GA_u^*$$

It follows from the induction hypothesis and from proposition IV.1 that:

$$\begin{aligned} (M) \wedge (S) & \vdash \mathcal{P} \approx EA_u^* (I_p + B(H_v^* GA_u^* B)_v^* H_v^* GA_u^*) \\ & \quad + FH_v^* (GA_u^* BH_v^*)_v^* GA_u^* \\ & \stackrel{(M), (S)}{\vdash} \mathcal{P} \approx EA_u^* (BH_v^* GA_u^*)_u^* + FH_v^* (I_p + GA_u^* (BH_v^* GA_u^*) BH_v^*)_v^* GA_u^* \\ & \stackrel{(M), (S)}{\vdash} \mathcal{P} \approx EA_u^* (BH_v^* GA_u^*)_u^* + FH_v^* GA_u^* (I_p + (BH_v^* GA_u^*) BH_v^*)_v^* GA_u^* \\ & \stackrel{(M), (S)}{\vdash} \mathcal{P} \approx EA_u^* (BH_v^* GA_u^*)_u^* + FH_v^* GA_u^* (BH_v^* GA_u^*) \\ & \stackrel{(M), (S)}{\vdash} \mathcal{P} \approx (E + FH_v^* G)(BH_v^* G + A)_u^* \end{aligned} \quad (\alpha)$$

It follows from these relations that we have:

$$(M) \wedge (S) \vdash \mathcal{L}_v^* GA_u^* \mathcal{P}_u^* = (GA_u^* B + H)_v^* GA_u^* \mathcal{P}_u^* \approx H_v^* (GA_u^* BH_v^*)_v^* GA_u^* \mathcal{P}_u^*.$$

According to an argument already used, we obtain by the induction hypothesis and by proposition IV.1:

$$\begin{aligned} (M) \wedge (S) & \vdash \mathcal{L}_v^* GA_u^* \mathcal{P}_u^* \approx H_v^* GA_u^* (BH_v^* GA_u^*)_u^* \mathcal{P}_u^* \\ & \stackrel{(M), (S)}{\vdash} \mathcal{L}_v^* GA_u^* \mathcal{P}_u^* \approx H_v^* G (BH_v^* G + A)_u^* \mathcal{P}_u^* \end{aligned} \quad (\beta)$$

According to (α) , to the induction hypothesis and to proposition IV.1, we have:

$$\begin{aligned} (M) \wedge (S) & \vdash \mathcal{L}_v^* GA_u^* \mathcal{P}_u^* \approx H_v^* G (E + FH_v^* G + BH_v^* G + A)_u^* \\ & \vdash \mathcal{L}_v^* GA_u^* \mathcal{P}_u^* \approx H_v^* G (E + A + (F + B) H_v^* G)_u^* \end{aligned} \quad (3)$$

Let us end our study with:

$$A_u^* (I_p + B \mathcal{L}_v^* GA_u^*) \mathcal{P}_u^* = A_u^* \mathcal{P}_u^* + A_u^* B \mathcal{L}_v^* GA_u^* \mathcal{P}_u^*.$$

Then, according to relation (β) , it follows from the induction hypothesis and from proposition IV.1 that the following deductions hold:

$$(M) \wedge (S) \vdash A_u^* \mathcal{P}_u^* + A_u^* B \mathcal{L}_v^* GA_u^* \mathcal{P}_u^* \approx A_u^* (I_p + BH_v^* G (BH_v^* G + A)_u^*) \mathcal{P}_u^*$$

$$\begin{aligned}
 & \overline{(M), (S)} A_u^* (I_p + B \mathcal{L}_v^* G A_u^*) \mathcal{P}_u^* \approx A_u^* (I_p + B H_v^* G A_u^* (B H_v^* G A_u^*)_u^*) \mathcal{P}_u^* \\
 & \overline{(M), (S)} A_u^* (I_p + B \mathcal{L}_v^* G A_u^*) \mathcal{P}_u^* \approx A_u^* (B H_v^* G A_u^*)_u^* \mathcal{P}_u^* \\
 & \overline{(M), (S)} A_u^* (I_p + B \mathcal{L}_v^* G A_u^*) \mathcal{P}_u^* \approx (B H_v^* G + A)_u^* \mathcal{P}_u^* \\
 & \overline{(M), (S)} A_u^* (I_p + B \mathcal{L}_v^* G A_u^*) \mathcal{P}_u^* \approx (E + F H_v^* G + B H_v^* G + A)_u^* \\
 & \overline{(M), (S)} A_u^* (I_p + B \mathcal{L}_v^* G A_u^*) \mathcal{P}_u^* \approx (E + A + (B + F) H_v^* G)_u^* \tag{4}
 \end{aligned}$$

This last deduction follows from (α) and from the induction hypothesis. Then observe that the identities (1), (2), (3) and (4) mean exactly that we have:

$$(M) \wedge (S) \mid \text{---} (P + Q)_v^* \approx P_v^* (Q P_v^*)_v^*$$

Therefore this ends the proof of our lemma. ■

LEMMA IV.7: *When $A = B = 0$ in the matrix P of the second step, we have:*

$$(M) \wedge (S) \mid \text{---} (P + Q)_v^* \approx P_v^* (Q P_v^*)_v^*$$

Proof. – The proof is symmetrical to the proof of lemma IV.6. ■

We shall now show two lemmas concerning (M) . Let us give first:

LEMMA IV.8: *When $A = B = 0$ in the matrix M of the first step, we have:*

$$(M) \wedge (S) \mid \text{---} (MN)_\nu^* \approx I_n + M (NM)_\mu^* N.$$

Proof. – Let us take again the denotations of the first step. Since $A = B = 0$, we have here the following identity:

$$I_n + M (NM)_\mu^* N = \begin{pmatrix} I_p & 0 \\ \mathcal{R} & \mathcal{S} \end{pmatrix}$$

where we set :

$$\begin{aligned}
 \mathcal{R} &= (C + D \mathcal{L}_\delta^* H C) \Phi_\gamma^* E + (C \mathcal{W}_\gamma^* F D + D) \Gamma_\delta^* G \\
 \mathcal{S} &= I_q + (C + D \mathcal{L}_\delta^* H C) \Phi_\gamma^* F + (C \mathcal{W}_\gamma^* F D + D) \Gamma_\delta^* H
 \end{aligned}$$

where $\mathcal{L} = HD$, $\mathcal{W} = FC$ and:

$$\Phi = FC + FD (HD)_\delta^* H C \quad \text{and} \quad \Gamma = HD + HC (FC)_\gamma^* F D.$$

According to the induction hypothesis and to proposition IV.1, we obviously have:

$$\begin{aligned} (M) \wedge (S) &\vdash \Phi \approx F(DH)_\beta^* C \\ (M) \wedge (S) &\vdash \Gamma \approx H(CF)_\beta^* D \end{aligned}$$

The induction hypothesis and proposition IV.1 permit us also to write:

$$\begin{aligned} (M) \wedge (S) &\vdash (C + D\mathcal{Z}_\delta^* HC) \Phi_\gamma^* E + (C\mathcal{W}_\gamma^* FD + D) \Gamma_\delta^* G \\ &\approx (DH)_\beta^* C \Phi_\gamma^* E + (CF)_\beta^* D \Gamma_\delta^* G \quad (\alpha) \end{aligned}$$

It follows now from the induction hypothesis, from propositions IV.1 and IV.4 that:

$$\begin{aligned} (M) \wedge (S) &\vdash (DH)_\beta^* C \Phi_\gamma^* \approx (DH)_\beta^* C [I_n + F((DH)_\beta^* CF)_\beta^* (DH)_\beta^* C] \\ &\vdash (DH)_\beta^* C \Phi_\gamma^* \approx [I_n + (DH)_\beta^* CF((DH)_\beta^* CF)_\beta^*] (DH)_\beta^* C \\ &\stackrel{(M)}{\vdash} (DH)_\beta^* C \Phi_\gamma^* \approx ((DH)_\beta^* CF)_\beta^* (DH)_\beta^* C \\ &\vdash (DH)_\beta^* C \Phi_\gamma^* \approx (DH + CF)_\beta^* . C \quad (\beta) \end{aligned}$$

A similar argument would prove that:

$$(M) \wedge (S) \vdash (CF)_\beta^* D \Gamma_\delta^* \approx (DH + CF)_\beta^* . D \quad (\gamma)$$

Hence relations (α) , (β) , (γ) show with proposition IV.1 that we have:

$$\begin{aligned} (M) \wedge (S) &\vdash (C + D\mathcal{Z}_\delta^* HC) \Phi_\gamma^* E + (C\mathcal{W}_\gamma^* FD + D) \Gamma_\delta^* G \\ &\approx (DH + CF)_\beta^* . (CE + DG) \quad (1) \end{aligned}$$

In the same way, it follows from the two identities (β) and (γ) , from our reduction work and from propositions IV.4 and IV.1 that we have:

$$\begin{aligned} (M) \wedge (S) &\vdash I_q + (C + D\mathcal{Z}_\delta^* HC) \Phi_\gamma^* F \\ &\quad + (C\mathcal{W}_\gamma^* FD + D) \Gamma_\delta^* H \approx I_q + (DH + CF)_\beta^* . (CF + DH) \\ &\stackrel{(A_r)}{\vdash} I_q + (C + D\mathcal{Z}_\delta^* HC) \Phi_\gamma^* F \\ &\quad + (C\mathcal{W}_\gamma^* FD + D) \Gamma_\delta^* H \approx (DH + CF)_\beta^* \quad (2) \end{aligned}$$

Then, according to relations (1) and (2), we have:

$$(M) \wedge (S) \vdash (MN)_\nu^* \approx I_n + M(NM)_\mu^* N$$

Thus this ends the proof of our lemma. ■

LEMMA IV.9: *When $C=D=0$ in the matrix M of the first step, we have:*

$$(M) \wedge (S) \mid \text{---} (MN)_\nu^* \approx I_n + M(NM)_\mu^* N$$

Proof. — The proof is symmetrical to the proof of lemma IV.8. ■

4th step: Symmetrical version of (S) at rank k.

We can now obtain the symmetrical version of (S). Let us take again all the denotations of the second step. Let us also introduce the matrices:

$$P_0 = \begin{matrix} & \begin{matrix} p & q \end{matrix} \\ \begin{matrix} p \\ q \end{matrix} & \begin{pmatrix} 0 & 0 \\ C & D \end{pmatrix} \end{matrix} \quad \text{and} \quad P_1 = \begin{matrix} & \begin{matrix} p & q \end{matrix} \\ \begin{matrix} p \\ q \end{matrix} & \begin{pmatrix} A & B \\ 0 & 0 \end{pmatrix} \end{matrix}$$

Then, according to lemma IV.7, we have:

$$\begin{aligned} (M) \wedge (S) \mid \text{---} (Q+P)_\nu^* &= (Q+P_0+P_1)_\nu^* \\ &\approx (P_0)_\nu^* ((Q+P_1)(P_0)_\nu^*)_\nu^* \\ \mid \text{---} (Q+P)_\nu^* &\approx (P_0)_\nu^* (Q(P_0)_\nu^* + P_1(P_0)_\nu^*)_\nu^* \end{aligned}$$

Since the matrix $P_1(P_0)_\mu^*$ has the same structure as P_1 , lemma IV.6 can be applied to it. Hence it follows from this lemma and from proposition IV.1 that the following deduction holds:

$$(M) \wedge (S) \mid \text{---} (Q+P)_\nu^* \approx (P_0)_\nu^* \cdot (P_1(P_0)_\nu^*)_\nu^* \cdot (Q(P_0)_\nu^* (P_1(P_0)_\nu^*)_\nu^*)_\nu^*$$

But we have by lemma IV.7:

$$(M) \wedge (S) \mid \text{---} (P_0+P_1)_\nu^* \approx (P_0)_\nu^* \cdot (P_1(P_0)_\nu^*)_\nu^*$$

It follows now from propositions IV.1 and IV.4 and from the two previous identities that we have:

$$\begin{aligned} (M) \wedge (S) \mid \text{---} (Q+P)_\nu^* &\approx (P_1+P_0)_\nu^* \cdot (Q(P_1+P_0)_\nu^*)_\nu^* \\ \mid \text{---} (Q+P)_\nu^* &\approx P_\nu^* (QP_\nu^*)_\nu^* \end{aligned}$$

Hence we proved that we have for every matrices Q and P of order k :

$$(M) \wedge (S) \mid \text{---} (P+Q)_\nu^* \approx P_\nu^* (QP_\nu^*)_\nu^*$$

5th step: Matrix version of (M) at rank k.

Let us use again the denotations of the first step. Then let us define:

$$M_0 = \begin{matrix} & \begin{matrix} r & s \end{matrix} \\ \begin{matrix} p \\ q \end{matrix} & \begin{pmatrix} O & O \\ C & D \end{pmatrix} \end{matrix} \quad \text{et} \quad M_1 = \begin{matrix} & \begin{matrix} r & s \end{matrix} \\ \begin{matrix} p \\ q \end{matrix} & \begin{pmatrix} A & B \\ 0 & 0 \end{pmatrix} \end{matrix}$$

According to the previous step, we have:

$$(M) \wedge (S) \mid \text{---} (MN)_v^* = (M_0 N + M_1 N)_v^* \approx (M_0 N)_v^* \cdot (M_1 N \cdot (M_0 N)_v^*)_v^* \quad (\alpha)$$

But it follows from lemma IV.8 that we have:

$$(M) \wedge (S) \mid \text{---} (M_0 N)_v^* \approx I_n + M_0 (NM_0)_\mu^* N \quad (\beta)$$

Hence, according to proposition IV.1 and to proposition IV.4, we obtain:

$$\begin{aligned} (M) \wedge (S) \mid \text{---} M_1 N \cdot (M_0 N)_v^* &\approx M_1 (I_n + NM_0 (NM_0)_\mu^*) N \\ &\stackrel{(A)}{\mid \text{---}} M_1 N \cdot (M_0 N)_v^* \approx M_1 (NM_0)_\mu^* N \end{aligned} \quad (\gamma)$$

Since the matrix $M_1 (NM_0)_\mu^*$ has the same structure as M_1 , it follows from lemma IV.9, from proposition IV.3 and from relation (γ) that we have:

$$(M) \wedge (S) \mid \text{---} (M_1 N \cdot (M_0 N)_v^*)_v^* \approx I_n + M_1 (NM_0)_\mu^* (NM_1 (NM_0)_\mu^*)_\mu^* N$$

Thus, according to the fourth step, the following deduction holds:

$$\begin{aligned} (M) \wedge (S) \mid \text{---} (M_1 N \cdot (M_0 N)_v^*)_v^* \\ \approx I_n + M_1 (NM_1 + NM_0)_\mu^* N = I_n + M_1 (NM)_\mu^* N \end{aligned}$$

It follows now from relations (α) and (β), from the fourth step and from propositions IV.4 and IV.1 that we have the following identities:

$$\begin{aligned} (M) \wedge (S) \mid \text{---} (MN)_v^* &\approx I_n + M_1 (NM)_\mu^* N \\ &\quad + M_0 (NM_0)_\mu^* [I_n + NM_1 (NM_1 + NM_0)_\mu^*] N \\ &\mid \text{---} (MN)_v^* \approx I_n + M_1 (NM)_\mu^* N \\ &\quad + M_0 (NM_0)_\mu^* [I_n + NM_1 (NM_0)_\mu^* (NM_1 (NM_0)_\mu^*)_\mu^*] N \\ &\stackrel{(M)}{\mid \text{---}} (MN)_v^* \approx I_n + M_1 (NM)_\mu^* N + M_0 (NM_0)_\mu^* (NM_1 (NM_0)_\mu^*)_\mu^* N \\ &\mid \text{---} (MN)_v^* \approx I_n + M_1 (NM)_\mu^* N + M_0 (NM)_\mu^* N = I_n + M (NM)_\mu^* N \end{aligned}$$

Hence the matrix version of (M) is proved at rank k . According to the steps 4 and 5 and to the symmetrical proof of proposition III.1, it is now easily

shown that the matrix version of (S) remains valid at order k . Thus this ends our induction and our proof. ■

COROLLARY IV.10 [7]: *Let K be a Kleene (resp. a general) semiring and let M be a $n \times n$ matrix (resp. proper matrix) of K -rational expressions. Then, for every ν, μ in $\mathcal{M}g_n$ the following deduction holds:*

$$(M) \wedge (S) \vdash M_\mu^* \approx M_\nu^*.$$

Proof. — It follows immediately from theorem IV.5 applied with $n = m$ and $N = I_n$ that the following deduction holds:

$$(M) \wedge (S) \vdash M_\nu^* \approx I_n + M \cdot M_\mu^*$$

Therefore our corollary follows obviously from proposition IV.4 since the identity (A_i) is a consequence of (M) . ■

The previous result plays a main role. Indeed it asserts that the star of a square matrix in $\mathcal{M}_{n \times n}(\mathcal{E}_K \mathcal{R} \text{ at } \langle A \rangle)$ or in $\mathcal{M}_{n \times n}(\mathcal{PE}_K \mathcal{R} \text{ at } \langle A \rangle)$ is independent of the cutting chosen to compute it, when we work modulo (M) and (S) . Hence we can define the star of a matrix of K -rational expressions modulo (M) and (S) .

Remark: Theorem IV.5 permits also to prove that every $(M), (S)$ deduction gives another $(M), (S)$ deduction when a matrix substitution is applied to it. This is one of the basic tools in our proof of the completeness of the system of semigroup identities (see [8]).

ACKNOWLEDGEMENTS

I would like to thank an anonymous referee for pointing out the reference of Pilling's work.

REFERENCES

1. J. BERSTEL and C. REUTENAUER, Rational Series and their Languages, *E.A.T.C.S. Monographs in Comput. Sci.*, Springer Verlag, 1988.
2. N. BOURBAKI, *Algèbre*, Chap. 1 à 3, C.C.L.S., 1970.
3. J. H. CONWAY, *Regular Algebras and Finite Machines*, Chapman & Hall, 1971.
4. S. EILENBERG, *Automata, Languages and Machines*, A, Academic Press, 1974.
5. N. JACOBSON, *Basic Algebra*, Vol. 2, Freeman, 1980.
6. D. KROB, Monoïdes et semi-anneaux complets, *Semigroup Forum*, 1989, 36, pp. 323-339.

7. D. KROB, Expressions K-Rationnelles, *Doctorat d'Université*, University Paris-VII, March 1988, L.I.T.P. Technical Report 88-27.
8. D. KROB, *Complete Systems of \mathcal{B} -Rational Identities*, L.I.T.P. Technical Report 89-42, 1989, *Theoret. Comput. Sci.* (to appear).
9. D. KROB, *On Aperiodic Semigroups*, L.I.T.P. Technical Report 89-76, 1989.
10. D. L. PILLING, Commutative Regular Equations and Parikh's Theorem, *J. London Math. Soc.*, (2), 1973, 6, pp. 663-666.
11. J. E. PIN, Varieties of formal languages, Masson, Paris, 1984; Plenum, New York and North-Oxford, London, 1986.
12. V. N. REDKO, On the Determining Totality of Relations of an Algebra of Regular Events, *Ukrain. Math. Zh.*, 1964, 16, pp. 120-126 (In russian).
13. V. N. REDKO, On the Algebra of Commutative Events, *Ukrain. Math. Zh.*, 1964, 16, pp. 185-195 (In russian).
14. J. SAKAROVITCH, Théorie algébrique des automates à piles, *Cours de D.E.A.*, University Paris-VI, 1987/88 (Non published).
15. A. SALOMAA, Two Complete Axiom Systems for the Algebra of Regular Events, *J. Assoc. Comput. Mach.*, 1966, 13, n° 1, pp. 158-169.