Theoretical Computer Science 89 (1991) 207-343
Elsevier

Fundamental Study

Complete systems of $\mathcal{B}$-rational identities

Daniel Krob

CNRS (LITP), Laboratoire d'Informatique de Rouen, Faculté des Sciences, Université dē Rouen, B.P. 118, 76134 Mont Saint-Aignan - Cedex, France

Communicated by D. Perrin
Received June 1989
Revised June 1990

Contents

0. Introduction

The theory of formal languages has grown in several directions according to the way a language is considered. First, strictly speaking, a language is just a part of the free monoid. But a language can also be seen as a formal series with coefficients in the boolean semiring $\mathscr{B}$. These two representations have been widely investigated for rational languages.

Nevertheless, there is another viewpoint which consists of considering the *formal expression* that is used to write a rational language. We shall call it a *rational expression* associated with this language. This concept has been studied much less than the classical approaches because it leads immediately to several difficulties: for instance, the uniqueness of the representation of a language is lost since a rational language is generally described by many distinct rational expressions.

Therefore this situation brings us naturally to the study of the *rational identities*, i.e. of the pairs of rational expressions that denote the same rational language. The most important problem in this area is to construct a "good" system of rational identities that would permit us to obtain by a logical deductive process (i.e. by a rewriting process) every possible rational identity; such a system will be called *complete.*

Several important results are known on this problem. Let us recall the following three positive ones. First, a theorem of Salomaa from 1966 (see [23] or [11, Chap. 5, Theorem III.5]) shows that there exists a complete system formed of two identities and of an *axiom scheme* which permits essentially to solve linear systems formally. Secondly a theorem of Redko (cf. [20]) whose proof was simplified and corrected by Pilling (cf. [7, Chap. 11]), gives a complete *system of identities* for the *commutative* rational expressions. Finally, another result of Redko (cf. [19] or [7, Chap. 4]) constructs a complete *system of identities* for the usual rational expressions over a *one-letter* alphabet. In the other direction, a negative result was proved independently by Redko and Conway (see [19] and [7, pp. 105–118]); it shows that every complete system of identities for the usual rational expressions is necessarily infinite.

For the non-commutative rational expressions over arbitrary alphabets, the construction of a "good" complete system was still open though candidates were proposed by Conway [7, pp. 116–119]). Indeed, Conway associated with every finite

monoid M the *monoid 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 denotes the natural monoid morphism from A_M^* into M which maps every letter a_m in A_M on m in M. Conway conjectured in [7, pp. 116, 118] that:

(1) the *system of monoid identities* which is the system composed of all the monoid identities $P(M)$ as well as of the two identities (M): $(ab)^* \approx 1 + a(ba)^*b$ and (S): $(a+b)^* \approx (a^*b)^*a^*$ is complete;

(2) the *system of group identities* which is the system composed only of the monoid identities $P(G)$ associated with the finite *groups* and of (M) and (S) is equivalent to the system of monoid identities;

(3) the system of group identities is equivalent to the system composed of (M), (S) and the *two* letter identities $(R(n))_{n \geqslant 2}$ which are defined by

$$R(n) \quad (a+b)^* \approx [(a+b)(b+(ab^*)^{n-2}a)]^* \left(1 + (a+b)\left(\sum_{i=0}^{n-2} (ab^*)^i\right)\right)$$

and which are naturally related to the dicyclicity of the symmetric group.

Thus, if these three conjectures were proved, we would obtain that the system formed of (M), (S) and the two letter identities $(R(n))_{n \geqslant 2}$ is complete.

This article is devoted to the resolution of the first two conjectures of Conway given above. Therefore, it follows that we have proved the following theorem.

Theorem 0.1. *The system of group identities is complete.*

Since we show that this last system is equivalent to the subsystem which consists of (M), (S) and of the monoid identities $(P(\mathfrak{S}_n))_{n \geqslant 2}$ associated with the symmetric groups, we also obtain the completeness of this last system. Hence we construct in this paper the first well described complete system of rational identities.

Moreover, in order to solve Conway's conjectures, we were led to prove several important results that permit us to answer other open questions. In particular, we showed, with the help of a theorem of Boffa (cf. [3]), the completeness of several systems of meta-rules for which this problem was still open (cf. [23; 7, p. 103]). We obtained also a new characterization of aperiodic semigroups in terms of $\mathcal{B}$-rational identities: indeed, we proved that a semigroup S is aperiodic iff an identity naturally associated with S is trivial, i.e. is just a consequence of the two identities (M) and (S).

But more important are the new methods we developed here: indeed, when we work with rational expressions, the only methods we can use are formal. When these formal ideas are interpreted at the level of rational languages, we can obtain new powerful methods. In particular, we brought out the notion of *universal language* associated with a monoid (cf. [12]) which permitted us to shed new light

on old results: for instance, we obtained with this notion a "formal" proof of Schützenberger's theorem on the characterization of star-free languages (see [12]). Let us remark that the family $(L_m)_{m\in M}$ of universal languages associated with a finite monoid M is defined by

$$\forall m \in M, \quad L_m = \varphi_M^{-1}(m).$$

Thus, it consists exactly of the languages that appear in the interpretation of the identity $P(M)$. Moreover, it plays a main role at the level of rational expressions as we will see in the sequel. We called these languages universal since up to an alphabetic morphism, every rational language L is a finite union of universal languages associated with the syntactic monoid of L (see [12]). Thus, in several cases, we can restrict the study of the *infinite* class of languages recognized by a monoid M to the study of the *finite* family of its associated universal languages.

Let us also point out that we constructed in [11] a theory of K-rational expressions on a general semiring K that shows the specific difficulties of the study of $\mathcal{B}$-rational expressions, i.e. of usual rational expressions. The fact is that the research of a complete system of K-rational identities is a very simple problem when K is a ring: in this case, the system reduced to *one* of the identities (A_l) or (A_r) (cf. Section 2.2) is complete (cf. [13] or [11, Chap. 5, Theorem II.3]). On the other hand, when K is a positive semiring (such as $\mathcal{B}$ or $\mathbb{N}$ for example) every complete system of K-rational identities is necessarily infinite.

Let us end this introduction by giving the structure of our paper, which is self-contained. This will also allow us to outline the approach that we have followed in order to solve the two open problems of Conway presented above. First, let us give its general structure. This paper is divided into sixteen sections: the first six are just preliminaries for later results. The following four sections (7–10) are the heart of this paper: there we prove the two main theorems on which the proof of the completeness of the system of monoid identities is based (given in Section 11). Then Sections 12–14 are devoted to the simplification of the complete system we obtained: here we study the completeness of systems of identities that are associated with certain group families. Finally, the two last sections deal with complete systems of meta-rules and with independence.

Section 1 recalls some classical definitions and notations. The real beginning of our work is Section 2 where we present the framework of our study that originates from [11]. We begin with the construction of the $\mathcal{B}$-$*$-algebra $\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle$ of the $\mathcal{B}$-rational expressions. Then we recall the basic definitions and properties of rational identities, identity models, rational inequalities and formal derivatives with respect to a letter.

The third section deals only with matrix identities, i.e. with identities between matrices of rational expressions. This kind of identity will be very important in all the sequel since it allows us to handle very concisely several rational identities at the same time. First, we show how to equip $\mathcal{M}_{n\times n}(\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle)$ with a $\mathcal{B}$-$*$-algebra

structure: thus we just recall the results of [11, Chap. 3], concerning the formal star of a matrix and its interpretation. Then we show how to extend to matrices the different notions related to usual identities and usual deductions: we introduce especially the notion of matrix substitution and we study under which conditions a usual deduction is stable when the letters are substituted by matrices.

Section 4 is very short and only devoted to the + operation. For technical reasons, some results concerning the identities associated with semigroups can be more easily written with + than with $*$. Then, we have grouped here the few specific properties of + which will be used in the sequel.

In the same way, we have grouped in Section 5 all the results concerning the maximal ideals of a finite semigroup that will be used in the proof of the main theorem of Section 7.

In Section 6, we associate with every finite semigroup S acting on the right on a finite set E, a family $(P(S, E, e))_{e\in E}$ of rational identities that we call *semigroup identities*: it generalizes Conway's definition (cf. [7, p. 116]) who only considered rational identities associated with monoids right acting naturally on themselves. This generalization is motivated by technical reasons since as it is proved in the sequel, we do not really extend Conway's system. Indeed, the proof of our main structure theorem to which is devoted all of Section 7, is more natural in our framework than in Conway's. This main result consists of proving that, if $(M_s)_{s\in S}$ denote the matrices associated with the right action of S on E, we have modulo some identities

$$\left(\sum_{s\in S} a_s M_s\right)^+ \approx \sum_{s\in S} E_s M_s \qquad (*)$$

where $(E_s)_{s\in S}$ is a family of $\mathscr{B}$-rational expressions which is independent of E. When S is a monoid, the interpretation of the expression E_s is exactly the universal language L_s we presented previously, except when $s = 1_s$ where the interpretation of E_s is $L_s - \{1\}$.

Section 8 is devoted to the first applications of the central theorem we have proved in Section 7. First, we show that the identities $(P(S, E, e))_{e\in E}$ we associated with the right action of a semigroup S on a set E are equivalent modulo a certain family of group identities. Thus, this result allows us to speak of the family of the semigroup identities which is defined modulo the family of group identities. It also follows from the main theorem of Section 6 that every semigroup identity implies its matrix version: this result is important since it permits us to use the powerful tool of matrix deduction with semigroup identities.

We prove in Section 9 the second essential result on our way to the proof of the completeness of the system of semigroup identities. More precisely, we show that for every boolean matrix representation μ of a semigroup S, if we denote by $\bar{\mu}$ its natural extension to $\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A_S\rangle$, we have

$$(M) \wedge (S) \vdash \bar{\mu}(E_s) \approx E_s \mu(s),$$

where $(E_s)_{s\in S}$ are the rational expressions associated with S by $(*)$.

In Section 10, we obtain several important consequences of this result. In particular, we show that the relation (*) can be extended to general kinds of matrices. Indeed, we prove that if μ is a boolean matrix representation of a semigroup S, then we have modulo some group identities

$$\left(\sum_{s\in S} a_s\mu(s)\right)^+ \approx \sum_{s\in S} E_s\mu(s) \qquad (**)$$

where $(E_s)_{s\in S}$ are still the rational expressions associated with S by (*). This last result is the fundamental tool which will permit us to prove in the next section the completeness of the system of monoid identities proposed by Conway. Therefore, Section 11 ends the first part of our paper where the first conjecture of Conway recalled above is solved.

In Section 12, we have grouped all the results that show how the usual algebraic operations on semigroups (subsemigroup, quotient, direct product, semidirect product) can be expressed in terms of deductions for the associated semigroup identities. Therefore, using Krohn-Rhodes theorem, these results allow us to show in Section 13 that the system of group identities is still complete, thus solving the second conjecture of Conway. Also they permit us to reduce this last system to different equivalent systems formed of group identities associated with certain classes of groups. In particular, we prove that the system formed of the group identities associated with all the symmetric groups and of (M) and (S) is complete.

In Section 14, we give the formulation in our framework of the third open problem of Conway presented above. We propose a more general conjecture which implies Conway's: it concerns the relations existing between the group identity associated with a group G and another identity constructed from the generators of G. We show particularly how a result of Conway provides an answer to our conjecture in the case of commutative groups.

In Section 15, we apply our completeness theorems to prove the completeness of several systems of meta-rules. A theorem of Boffa allows us in particular to prove the completeness of a rule conjectured by Salomaa. We also give new proofs for the completeness of several other rules.

Finally, the last section is devoted to the study of the independence of group identities. We have developed in particular, the study of a model that Conway introduced in [7, p. 117]). It permits us to show independence results for group identities. We prove also by a different method than Conway's that a complete system of $\mathcal{B}$-rational identities on an alphabet with two or more letters contains necessarily an infinite number of two letter identities.

1. Preliminaries

1.1. $\mathcal{B}$-semialgebras

In the sequel of the paper, $\mathcal{B}$ will denote the boolean semiring:

$$\mathcal{B} = \{0, 1\}, \quad \text{with } 1+1=1.$$

Definition 1.1. A *$\mathcal{B}$-semialgebra* $\mathcal{A}$ is a semiring equipped with a compatible $\mathcal{B}$-semimodule structure. This means that $\mathcal{A}$ has two internal laws denoted by $+$ and $\times$ and an external law from $\mathcal{B} \times \mathcal{A}$ into $\mathcal{A}$ denoted by . such that

(i) $(\mathcal{A}, +)$ is a commutative monoid whose unity is denoted by 0;
(ii) $(\mathcal{A}, \times)$ is a monoid whose unity is denoted by 1;
(iii) the product $\times$ is distributive with the sum $+$;
(iv) $\forall a \in \mathcal{A}$, $a \times 0 = 0 \times a = 0$;
(v) $\forall a \in \mathcal{A}$, $0_{\mathcal{B}}.a = 0$, $1_{\mathcal{B}}.a = a$, $a + a = a$.

Note. The $\mathcal{B}$-semimodule structure is defined here by (v): indeed, the structure of $\mathcal{B}$ avoids adding the other compatibility conditions between the external law and the internal product. One may refer to [2, pp. 10–17]) or [11] to see the general definitions of a semimodule and a semialgebra.

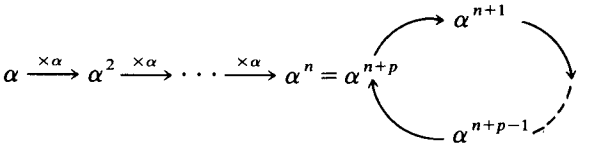
For every $\mathcal{B}$-semialgebra $\mathcal{A}$, we will identify $\mathcal{B}$ to a sub-$\mathcal{B}$-semialgebra of $\mathcal{A}$. This is possible by (v). Note finally that we will just speak in the sequel of a $\mathcal{B}$-algebra instead of a $\mathcal{B}$-semialgebra.

Definition 1.2. Let $\mathcal{E}$, $\mathcal{F}$ be two $\mathcal{B}$-semialgebras. Then we shall call *morphism of $\mathcal{B}$-algebras* from $\mathcal{E}$ into $\mathcal{F}$ every mapping φ from $\mathcal{E}$ to $\mathcal{F}$ such that

(i) $\forall a, b \in \mathcal{E}$, $\varphi(a+b) = \varphi(a) + \varphi(b)$;
(ii) $\forall a, b \in \mathcal{E}$, $\varphi(a \times b) = \varphi(a) \times \varphi(b)$;
(iii) $\varphi(0) = 0$, $\varphi(1) = 1$.

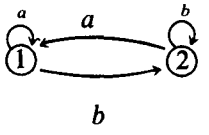
1.2. Generalities

Notation 1.1. We will denote by $\mathbb{N}^*_{n,p}$ the *monogenic* semigroup generated by a single element α which satisfies only the relation $\alpha^n = \alpha^{n+p}$. $\mathbb{N}^*_{n,p}$ is often represented by the classical "frying-pan" diagram:



$\mathbb{N}^*_{n,p}$ contains obviously a unique maximal group $G = \{\alpha^n, \ldots, \alpha^{n+p-1}\} \simeq \mathbb{Z}/p\mathbb{Z}$. We will denote by $[n]$ the class of $n \in \mathbb{N}^*$ into $\mathbb{N}^*_{n,p}$.

Notation 1.2. U_2 denotes the transition monoid of the "reset" automaton:



We can also define U_2 by the following generators and relators:

$$U_2 = \{1, \sigma, \tau\}\ , \quad \text{where } \sigma^2 = \tau\sigma = \sigma,\ \tau^2 = \sigma\tau = \tau.$$

Notation 1.3. For every semigroup S, we denote by S^1 the monoid defined by

$$S^1 = \begin{cases} S \cup \{1\}, & \text{if } 1 \notin S, \\ S, & \text{if } S \text{ is a monoid.} \end{cases}$$

Notation 1.4. We will denote by u_m the *row vector* of $\mathcal{B}^n$ whose mth entry is 1 and whose other entries are all 0 and by u the *column vector* of $\mathcal{B}^n$ whose entries are all 1. When we use these vectors in the sequel, n and m will often not be specified since the context will remove the possible ambiguities.

Definition 1.3. A semigroup is said to be *aperiodic* if it does not contain any non-trivial group as subsemigroup.

1.3. Action of a semigroup on a set

We regroup here some definitions concerning right actions of a semigroup on a set. They can be always easily transposed to left actions. Note finally that only *finite* sets and semigroups will be considered in the sequel.

Definition 1.4. A semigroup S *acts on the right* on a set E if there is a mapping from $E \times S$ into E denoted by . such that

$$\forall e \in E, \forall s, t \in S, \quad (e.s).t = e.(st).$$

Then we will say that $e.s$ is the result of the *right action* of s on e.

Notes. (1) Observe that the above definition is not compatible with the usual notion of group action on a set (cf. [4, Section I.5.1]) since we do not ask that 1_S induces the identity on E when the semigroup has a unity.

(2) When we speak of a group action on a set in the sequel, it will always refer to Definition 1.4.

Example. Every semigroup S acts on the right on itself by the *natural action* of S on S which is defined by

$$\forall s, t \in S, \quad s.t = st.$$

More generally, every T of a semigroup S acts also on the right on S by a natural action defined as above.

Definition 1.5. Let S be a semigroup which acts on the right on the sets E and F. We will say that a bijective mapping φ from E into F is an *isomorphism* for the

right action of S on these two sets if and only if

$$\forall s \in S, \forall e \in E, \quad \varphi(e.s) = \varphi(e).s.$$

Then we will denote it by $E \simeq F$.

2. $\mathscr{B}$-Rational expressions

2.1. *Construction of the $\mathscr{B}$-$*$-algebra of the $\mathscr{B}$-rational expressions*

Let A be an alphabet and let Σ be the union of the sets of product symbols of arity 0, 1 and 2 denoted $\Sigma(0)$, $\Sigma(1)$ and $\Sigma(2)$ and defined by

- $\Sigma(0)$ contains two elements denoted by $\emptyset$ and Λ;[1]
- $\Sigma(1)$ contains the elements $0_{\mathscr{B}}$ and $1_{\mathscr{B}}$ and the symbol $*$;
- $\Sigma(2)$ contains the symbols $+$ and $\times$.

Then we can construct the free Σ-algebra $W = F(\Sigma, A)$ on A (see [10, Section 2.5.]). Let us introduce now the smallest congruence $\equiv$ of the Σ-algebra W such that

$$\forall a, b, c \in W, \quad a+(b+c) \equiv (a+b)+c, \quad a \times (b \times c) \equiv (a \times b) \times c,$$

$$\forall a, b, c \in W, \quad a \times (b+c) \equiv a \times c + b \times c, \quad (b+c) \times a \equiv b \times a + c \times a,$$

$$\forall a \in W, \quad a+\emptyset \equiv \emptyset + a \equiv a, \quad a \times \Lambda \equiv \Lambda \times a \equiv a, \quad a \times \emptyset \equiv \emptyset \times A \equiv \emptyset,$$

$$\forall a, b \in W, \quad b+a \equiv b+a, \quad a+a \equiv a, \quad 1.a \equiv a, \quad 0.a \equiv \emptyset,$$

$$(0.\Lambda)^* \equiv (1.\Lambda)^* = \Lambda.^2$$

We can now define the $\mathscr{B}$-algebra of $\mathscr{B}$-rational expressions as follows.

Definition 2.1. We will call *$\mathscr{B}$-$*$-algebra of $\mathscr{B}$-rational expressions on the alphabet A* and we will denote by $\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle$ the quotient $\mathscr{B}$-algebra $W/\equiv$.

Remark. $\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle$ is obviously a $\mathscr{B}$-algebra since all the properties of $\equiv$, except the last two, are just the axioms of the $\mathscr{B}$-algebra structure.

Let us recall [8, p. 160] that a *$\mathscr{B}$-$*$-algebra* is a $\mathscr{B}$-algebra $\mathscr{A}$ equipped with a mapping $*$ from $\mathscr{A}$ into $\mathscr{A}$. The $\mathscr{B}$-$*$-algebras are clearly the objects of a category **B-$*$-Alg** with evident morphisms called *$*$-morphisms*.[3] Then, we can consider the subcategory **B-$*$-Bound-Alg** of the *$\mathscr{B}$-$*$-bound-algebras* of **B-$*$-Alg**. Its objects are the $\mathscr{B}$-$*$-algebras $\mathscr{A}$ which satisfy

$$(0.1_{\mathscr{A}})^* = (1.1_{\mathscr{A}})^* = 1_{\mathscr{A}}.$$

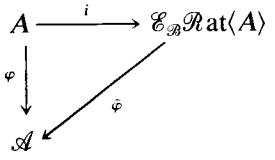
[1] $\emptyset$ and Λ are intended to be the unities of the $\mathscr{B}$-algebra $\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle$.

[2] This last relation means that we can identify the star in $\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle$ and the star in $\mathscr{B}$ which exists independently of rational expressions.

[3] A *$*$-morphism* φ from $\mathscr{E}$ into $\mathscr{F}$ is a $\mathscr{B}$-algebra morphism such that $\forall E \in \mathscr{E}$, $\varphi(E^*) = (\varphi(E))^*$.

This condition ensures the compatibility between the star of $\mathcal{B}$ and the star of $\mathcal{A}$. By construction, $\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle$ is obviously a $\mathcal{B}$-$*$-bound-algebra. But, it is moreover a universal object for the category **B-*-Bound-Alg**.

Proposition 2.1 (Krob [11, Chap. 1, Proposition III.1]). *Let A be an alphabet, let $\mathcal{A}$ be a $\mathcal{B}$-$*$-bound-algebra and let φ be a mapping from A into $\mathcal{A}$. Then, there exists a unique $*$-morphism $\bar{\varphi}$ such that the following diagram (where i denotes the canonical injection) is commutative:*



Remarks. (1) From now on, we will consider that $\mathcal{B}$ is embedded into $\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle$.

(2) The above universal property of $\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle$ allows us to consider the unique $\mathcal{B}$-$*$-morphism c from $\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle$ into the $\mathcal{B}$-$*$-bound-algebra $\mathcal{B}$ such that

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

Then, we shall say that $c(E)$ is the *constant coefficient* of $E \in \mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle$.

2.2. Rational identities

In the previous section, we defined a syntax which allowed us to speak of the $\mathcal{B}$-rational expressions. It remains now to provide a semantics with these formal expressions. Thus let us denote by $\mathrm{Rat}\langle A^*\rangle$ the set of the rational languages in A^*. Then $\mathrm{Rat}\langle A^*\rangle$ is a $\mathcal{B}$-$*$-bound-algebra if we equip it with the usual $*$ operation defined by

$$\forall L \in \mathrm{Rat}\langle A^*\rangle, \quad L^* = \bigcup_{n \geq 0} L^n$$

By the universal property given in Proposition 2.1, there exists a $\mathcal{B}$-$*$-morphism λ called *interpretation* from $\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle$ into $\mathrm{Rat}\langle A^*\rangle$ which is defined by

$$\forall a \in A, \quad \lambda(a) = a.$$

Remark (Krob [11, Chap. 2, Proposition II.2]). We can clearly identify the constant coefficient of a $\mathcal{B}$-rational expression with the constant coefficient of its interpretation.

Definition 2.2. Let $E, F \in \mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle$. Then the pair (E, F) is said to be a *rational identity* iff we have $\lambda(E) = \lambda(F)$. We will denote it by $E \approx F$.

This means that two $\mathcal{B}$-rational expressions form a rational identity if and only if they denote the same rational language.

Examples. (1) We will call *aperiodic classical identities* the two following rational identities on the alphabet $A=\{a, b\}$:

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

(2) We introduce also the two "star definition" identities:

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

(3) The following identities will be called *cyclic classical identities*:

$$(P(n))_{n\in\mathbb{N}^*} \quad a^* \approx (1+a+\cdots+a^{n-1}).(a^n)^*.$$

Note. The family composed of the identities given in (1) and (3) was called the *system of classical identities* by Conway (cf. [7, p. 25]).

2.3. Deductions

The identities (A_l) and (A_r) are consequences of (M) since it suffices to replace a or b by 1 in (M) to obtain them. We shall try now to give a precise meaning to this notion of consequence. At first, we shall call *substitution* of $\mathscr{C}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle$ every $\mathscr{B}$-$*$-endomorphism σ of $\mathscr{C}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle$. By the universal property of $\mathscr{C}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle$, a substitution is completely determined by its image on A.

Definition 2.3. Let $\mathscr{A}$ be a set of $\mathscr{B}$-rational identities. Then we will call *$\mathscr{A}$-deduction* any finite sequence $(E_i, F_i)_{i\in[1,n]}$ of $\mathscr{B}$-rational identities such that one of the following cases holds for every $k\in[1, n]$:

(D_1) $(E_k, F_k)\in\mathscr{A}$,
(D_2) $\exists i, j<k$, $E_k=E_i+E_j$ and $F_k=F_i+F_j$,
(D_3) $\exists i, j<k$, $E_k=E_i.E_j$ and $F_k=F_i.F_j$,
(D_4) $\exists i<k$, $E_k=E_i^*$ and $F_k=F_i^*$,
(D_5) $\exists i<k$ and a substitution σ, $E_k=\sigma(E_i)$ and $F_k=\sigma(F_i)$,
(D_6) $E_k=F_k$,
(D_7) $\exists i<k$, $E_k=F_i$ and $F_k=E_i$,
(D_8) $\exists i, j<k$, $E_k=E_i$ and $F_k=F_j$ and $F_i=E_j$.

We will say that a $\mathscr{B}$-rational identity (E, F) is a *consequence* of $\mathscr{A}$ if and only if there exists a $\mathscr{A}$-deduction ending with (E, F). We will denote it by

$$\mathscr{A}\vdash E\approx F.$$

Remark. The above definition is consistant since each term of a $\mathscr{A}$-deduction is necessarily a rational identity: indeed, the only problem which may occur concerns the rule (D_5) and is solved in [11, Chap. 2, Proposition II.6].

Notation. We will denote equivalently

$$\mathscr{A}\vdash E\approx F \quad \text{of} \quad \overset{\mathscr{A}}{\vdash\!\!\!-} E\approx F.$$

Example. Let us show for instance that the following deduction holds:

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

Indeed, we can write the following sequence of elementary deductions:

$$(S) \vdash\!\!\!- (a+b)^* \approx (a^*b)^*a^*$$

$$\vdash\!\!\!\!\!\!^{(M)}\!\!\!- (a+b)^* \approx [1+a^*(ba^*)^*b].a^* = a^*.[1+(ba^*)^*(ba^*)]$$

$$\vdash\!\!\!\!\!\!^{(M)}\!\!\!- (a+b)^* \approx a^*.(ba^*)^*.$$

Let us now give the following two results;

Proposition 2.2 (Star-Star) (Conway [7, p. 35] or Krob [11, Chap. 2, Proposition IV.15]). *We have the following deduction*:

$$(M) \wedge (S) \vdash (A_r) \wedge (S) \vdash a^{**} \approx a^*.$$

Proposition 2.3 (Krob [11, Chap. 2, Lemma IV.20). *For every E in $\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle$, there exists a $\mathcal{B}$-rational expression F with $c(F)=0$ such that*

$$(M) \wedge (S) \vdash E \approx c(E)+F.$$

Definition 2.4. Let $\mathcal{A}$ be a set of $\mathcal{B}$-rational identities. An identity (E, F) will be said to be *independent* of $\mathcal{A}$ iff it cannot be deduced from $\mathcal{A}$.

Example (Krob [11, Chap. 2, Proposition IV.8]). The identity (A_r) is independent of (A_l) and conversely the identity (A_l) is independent of (A_r).

Note. A system $\mathcal{A}$ of $\mathcal{B}$-rational identities is made of *independent identities* iff every identity (E, F) of $\mathcal{A}$ is independent of $\mathcal{A}-\{(E, F)\}$.

Definition 2.5. Let $A \subset B$ be two alphabets. Then a system $\mathcal{A}$ of $\mathcal{B}$-rational identities on $\mathcal{B}$ is said to be *complete* for A if and only if every $\mathcal{B}$-rational identity on A can be deduced from $\mathcal{A}$.

Definition 2.6. Two systems $\mathcal{S}$ and $\mathcal{T}$ of $\mathcal{B}$-rational identities are *equivalent* iff every rational identity which is a consequence of $\mathcal{S}$ is also a consequence of $\mathcal{T}$ and conversely.

Notation. When two systems $\mathcal{S}$ and $\mathcal{T}$ are equivalent, we will denote it by

$$\mathcal{S} \vdash\!\dashv \mathcal{T}.$$

In particular, such a notation will be often be used in the sequel when two identities are equivalent.

Let us recall now the following fundamental results.

Theorem 2.4 (Conway [7, p. 105] or Krob [11, Chap. 2, Theorem IV.13]). *Let $A \subset B$ be two alphabets. Then every complete system of $\mathcal{B}$-rational identities on B for A is infinite.*

Theorem 2.5 (Conway [7, pp. 104–105] and Krob [11, Chap. 2, Theorem IV.7]). *Let $\mathcal{P}$ be the set of the prime integers in $\mathbb{N}^* - \{1\}$. Then the following system of $\mathcal{B}$-rational identities is formed of independent rational identities and is equivalent to the system of classical identities:*

$$(M), \quad (S), \quad (P(p))_{p \in \mathcal{P}}.$$

2.4. Models of a systems of rational identities

For every $\mathcal{B}$-$*$-bound-algebra $\mathcal{M}$ and every family $x = (x_a)_{a \in A}$ of elements of $\mathcal{M}$, there exists by Proposition 2.1 a unique $\mathcal{B}$-$*$-morphism from $\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle$ into $\mathcal{M}$ which maps every letter a of A onto x_a: it will be denoted by $\varepsilon_{\mathcal{M},x}$.

Definition 2.7. Let $\mathcal{A}$ be a set of $\mathcal{B}$-rational identities on A. Then we will call *model* of $\mathcal{A}$ every $\mathcal{B}$-$*$-bound-algebra $\mathcal{M}$ such that

$$\forall x \in \mathcal{M}^A, \forall (E, F) \in \mathcal{A}, \quad \varepsilon_{\mathcal{M},x}(E) = \varepsilon_{\mathcal{M},x}(F).$$

Example. $\mathcal{B}\langle\langle A^*\rangle\rangle$, $\mathcal{P}(A^*)$ and $\mathrm{Rat}\langle A\rangle$ are models of every system of identities.

The next result is very important since the independence proofs rely on it. Indeed, to show that the identity α is not a consequence of an identity β, it will suffice by it to construct a model for α where β does not hold.

Proposition 2.6 (Krob [11, Chap. 2, Proposition III.5). *Let $\mathcal{A}$ be a system of $\mathcal{B}$-rational identities and let $\mathcal{M}$ be a model of $\mathcal{A}$. Then, for every family $(x_a)_{a \in A}$ of elements of $\mathcal{M}$, we have*

$$\mathcal{A} \vdash E \approx F \Rightarrow \varepsilon_{\mathcal{M},x}(E) = \varepsilon_{\mathcal{M},x}(F).$$

Notes. (1) The above proposition says exactly that every model of $\mathcal{A}$ is also a model of every $\mathcal{A}$-consequence.

(2) As in first order logic, we can prove a completeness theorem that shows the equivalence between $\mathcal{A}$-deduction and validity in all the models of $\mathcal{A}$ for every system $\mathcal{A}$ of rational identities [11, Chap. 2, Proposition III.6].

2.5. Rational inequalities

The rational inequalities were introduced by Conway [7, p. 27] where they play an important role. In this paper, we will use them only in Section 15.

Definition 2.8. Let A be an alphabet and let $E, F \in \mathscr{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle$. Then, the pair (E, F) is said to be a *rational inequality* and will be denoted by $E \leqslant F$ iff

$$\lambda(E) \subset \lambda(F) \Leftrightarrow \lambda(F) = \lambda(E) \cup \lambda(F).$$

The notions of rational inequality and of rational identity are dual. Thus it is straightforward to define the following deduction notion.

Definition 2.9. Let $\mathscr{A}$ be a $\mathcal{B}$-rational identities system and let (E, F) be a rational inequality on an alphabet A. Then the inequality $E \leqslant F$ is said to be an *$\mathscr{A}$-consequence* iff one of the two following equivalent conditions holds:

$$\exists T \in \mathscr{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle, \quad \mathscr{A} \vdash F \approx E + T \Leftrightarrow \mathscr{A} \vdash F \approx E + F.$$

The following results show that we can work modulo (M), (S) with rational inequalities deductions exactly as with rational identities deductions.

Proposition 2.7 (Conway [7, p. 36] or Krob [11, Chap. 6]). *Let $\mathscr{A}$ be a system of rational identities. Then, for every substitution σ and for every E, F, G, H in $\mathscr{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle$, we have*

$$\left.\begin{array}{l}\mathscr{A} \vdash E \leqslant F \\ \mathscr{A} \vdash G \leqslant H\end{array}\right\} \Rightarrow \begin{cases}\mathscr{A} \vdash E + G \leqslant F + H \\ \mathscr{A} \vdash E.G \leqslant F.H \\ \mathscr{A} \vdash \sigma(E) \leqslant \sigma(F).\end{cases}$$

Proposition 2.8 (Conway [7, p. 36] or Krob [11, Chap. 6]). *Let $\mathscr{A}$ be a system of rational identities on an alphabet A. For every $E, F \in \mathscr{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle$, we have*

$$\mathscr{A} \vdash E \leqslant F \Rightarrow \mathscr{A} \overset{(M),(S)}{\vdash\!\!\!-\!\!\!-} E^* \leqslant F^*.$$

Note. Transivity and reflexivity hold for inequalities deductions:

$$\left.\begin{array}{l}\mathscr{A} \vdash E \leqslant F \\ \mathscr{A} \vdash F \leqslant G\end{array}\right\} \Rightarrow \mathscr{A} \vdash E \leqslant G \quad \text{and} \quad \mathscr{A} \vdash E \leqslant E.$$

The following result is important since it allows us to connect rational inequality deductions with usual rational identity deductions.

Proposition 2.9 (Conway [7, p. 36] or Krob [11, Chap. 6]). *Let $\mathscr{A}$ be a system of rational identities on an alphabet A. For every $E, F \in \mathscr{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle$, we have*

$$\left.\begin{array}{l}\mathscr{A} \vdash E \leqslant F \\ \mathscr{A} \vdash F \leqslant E\end{array}\right\} \Rightarrow \mathscr{A} \vdash E \approx F.$$

Note. The above result shows the antisymmetry of the inequality deductions.

Proposition 2.10 (Conway [7, p. 36] or Krob [11, Chap. 6, Proposition III.6]). *Let A be an alphabet and let E be in $\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle$. Then, we have*

$$(M) \wedge (S) \vdash E \leqslant A^*.$$

2.6. Proper rational expressions

We define a $\mathscr{B}$-algebra filtration in $\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle$ by

$$\mathscr{P}_0 = \mathscr{B}\langle A\rangle \quad \text{and} \quad \forall n \geqslant 1, \quad \mathscr{P}_{n+1} = \langle \mathscr{P}_n, (\mathscr{P}_n \cap \mathrm{Ker}\, c)^*\rangle,$$

where $\mathscr{B}\langle A\rangle$ denotes the non-commutative polynomials constructed over A and where the notation $\langle \mathscr{F}\rangle$ denotes the $\mathscr{B}$-subalgebra of $\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle$ generated by the family $\mathscr{F}$. Thus, the elements of $\mathscr{P}_{n+1}$ are sums of products of elements in $\mathscr{P}_n$ with stars of elements of $\mathscr{P}_n$ whose *constant coefficient* is 0.

Definition 2.10. We shall call *$\mathscr{B}$-algebra of proper rational expressions* and we shall denote by $\mathscr{P}\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle$ the $\mathscr{B}$-subalgebra of $\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle$ defined by $\bigcup_{n\geqslant 0} \mathscr{P}_n$.

Remark. Thus we can say that a rational expression E is proper iff under a star in E there are only expressions whose constant coefficient is 0.

Note. $\mathscr{P}\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle$ is obviously the smallest subalgebra of $\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle$ containing A and satisfying the property

$$E \in \mathscr{P}\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle \quad \text{and} \quad c(E) = 0 \Rightarrow E^* \in \mathscr{P}\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle.$$

Proposition 2.11 (Krob [11, Chap. 2, Proposition IV.21]). *For every E in $\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle$, there exists a proper $\mathscr{B}$-rational expression F in $\mathscr{P}\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle$ such that*

$$(M) \wedge (S) \vdash E \approx F.$$

2.7. Derivative of a rational expression

Let us define now the derivative of an element of $\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle$.

Proposition 2.12 (Conway [7, p. 41] or Krob [11, Chap. 4, Corollary II.2]). *Let A be an alphabet. Then, for every letter a of A, there exists a unique mapping ∂_a from $\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle$ into $\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle$ which satisfies the properties*

$$\forall E, F \in \mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle, \quad \partial_a(E+F) = \partial_a(E) + \partial_a(F),$$

$$\forall E, F \in \mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle, \quad \partial_a(E.F) = \partial_a(E).F + c(E).\partial_a(F),$$

$$\forall E \in \mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle, \quad \partial_a(E^*) = \partial_a(E).E^*.$$

Definition 2.11. The mapping ∂_a defined by the previous proposition is called *derivative with respect to the letter a* in $\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle$.

The following result connects ∂_a with the usual notion of derivative (or residual) of a language with respect to a letter.

Proposition 2.13 (Conway [7, Chap. 5] or Krob [11, Chap. 4, Proposition II.4]). *Let a be a letter of an alphabet A. Then, for every expression $E \in \mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle$, we have*

$$\lambda(\partial_a(E)) = a^{-1}(\lambda(E)).$$

Note. Thus the interpretation of the derivative of a rational expression is the derivative of the interpretation of this expression.

3. Matrix identities

3.1. Definitions

Definition 3.1. Let M and N be two matrices of $\mathcal{M}_{n\times m}(\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle)$. We shall say that the pair (M, N) forms a *matrix identity* if and only if we have

$$\forall i \in [1, n], \forall j \in [1, m], \quad \lambda(M_{i,j}) = \lambda(N_{i,j})$$

Then we shall denote it by $M \approx N$.

We extend in the same way the notion of deduction: indeed, we shall say that a matrix identity is a *consequence* of a system of identities $\mathcal{A}$ iff each entry of this identity can be $\mathcal{A}$-deduced in the usual sense. We also define the *constant coefficient* $c(M)$ of a matrix M of $\mathcal{M}_{n\times m}(\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle)$ as the matrix of the constant coefficients of the entries of M. Finally, we shall say that a pair (M, N) of matrices in $\mathcal{M}_{n\times m}(\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle)$ forms a *matrix inequality* and we shall denote it by $M \leqslant N$ iff we have

$$\forall i \in [1, n], \forall j \in [1, m], \quad M_{i,j} \leqslant N_{i,j}.$$

We also extend as above the notion of deduction to matrix inequalities.

3.2. The formal star of a matrix

We can now come to the most important definition for matrices of $\mathcal{B}$-rational expressions: the notion of formal star of a square matrix in $\mathcal{M}_{n\times n}(\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle)$. To define this concept, it seems natural to use an inductive method. This will lead us to define a notion of star relatively to a cutting of [1, n]: to formalize this situation, we must introduce the free magma on one letter.

Recall (Bourbaki [4, Section I.7.1]). We denote $\mathcal{M}\mathcal{g}$ the free magma constructed on the one element set $\{X\}$. $\mathcal{M}\mathcal{g}$ is the union of the sequence of sets $(\mathcal{M}\mathcal{g}_n)_{n\in\mathbb{N}}$ constructed

inductively as follows: at first, we get $\mathcal{M}g_1 = \{X\}$; then, for every $n \geq 2$, $\mathcal{M}g_n$ is the sum set of the sets $\mathcal{M}g_p \times \mathcal{M}g_{n-p}$ for $p \in [1, n-1]$.

Definition 3.2. Let M be a matrix of $\mathcal{M}_{n\times n}(\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle)$ and let α be in $\mathcal{M}g_n$. Then we shall denote by M^*_α the *star of M relative to α*: it is the matrix inductively defined as follows:

(a) when $n = 1$, $\alpha = X$ and the star of M relative to α will be the star in the usual sense of the rational expression $M_{1,1}$;

(b) If $n \geq 2$, there exists a unique pair $(p, q) \in \mathbb{N}^* \times \mathbb{N}^*$ with $p + q = n$ such that $\alpha = (\beta, \gamma)$ with $\beta \in \mathcal{M}g_p$ and $\gamma \in \mathcal{M}g_q$. Then we can decompose M in the following way:

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

and we define

$$M^*_\alpha = \begin{matrix} \\ p \\ q \end{matrix} \begin{pmatrix} \overset{p}{(A + BD^*_\gamma C)^*_\beta} & \overset{q}{A^*_\beta B(D + CA^*_\beta B)^*_\gamma} \\ D^*_\gamma C(A + BD^*_\gamma C)^*_\beta & (D + CA^*_\beta B)^*_\gamma \end{pmatrix}$$

Remark. If Γ_n is the nth Catalan number, there are exactly Γ_n distinct ways to compute the star of a $n \times n$ matrix with the above inductive formulas.

Let us recall the following miraculous result which shows that (M) and (S) together imply their matrix versions.

Theorem 3.1 (Krob [11, Chap. 3, Proposition IV.2]). *Let A be an alphabet, let P, Q be two square matrices of $\mathcal{M}_{n\times n}(\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle)$, let M be in $\mathcal{M}_{n\times m}(\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\{A\rangle)$ and let N be in $\mathcal{M}_{m\times n}(\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle)$. Then, for every α in $\mathcal{M}g_n$ and β in $\mathcal{M}g_m$, we have*

$$(M) \wedge (S) \vdash (MN)^*_\alpha \approx I_n + M(NM)^*_\beta N,$$

$$(M) \wedge (S) \vdash (P + Q)^*_\alpha \approx (P^*_\alpha Q)^*_\alpha P^*_\alpha.$$

Corollary 3.2 (Conway [7, p. 110], Krob [11]). *Let M be a matrix of $\mathcal{M}_{n\times n}(\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle)$. Then, for every pair (α, β) of elements of $\mathcal{M}g_n$, we have*

$$(M) \wedge (S) \vdash M^*_\alpha \approx M^*_\beta.$$

Proof. Let (α, β) be a pair of elements in $\mathcal{M}g_n$. Let us now apply the previous theorem with $N = I_n$. Thus, we obtain the identity

$$(M) \wedge (S) \vdash M^*_\alpha \approx I_n + M.M^*_\beta. \tag{1}$$

But, this identity gives in particular, when $\alpha = \beta$,

$$(M) \wedge (S) \vdash M^*_\beta \approx I_n + M.M^*_\beta. \tag{2}$$

We can now immediately conclude to our corollary. □

Remark (Krob [11, Chap. 3, Proposition IV.1]). It can also be proved that each identity (A_l) or (A_r) implies its own matrix version.

Consequence. From now on, we will always work modulo (M) and (S). Thus, we can now speak of *the* star of a matrix.

Note. This convention is equivalent to identifying the $\mathcal{B}$-algebra $\mathcal{M}_{n\times n}(\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle)$ with its quotient algebra with the finest $\mathcal{B}$-algebra congruence that identifies the consequences of (M) and (S). By Corollary 3.2, $\mathcal{M}_{n\times n}(\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle)$ is now clearly a $\mathcal{B}$-$*$-bound-algebra since we can easily check by induction on n that

$$0_n^* = \mathrm{Id}_n \quad \text{and} \quad \mathrm{Id}_n^* = \mathrm{Id}_n.$$

It remains to check that the $\mathcal{B}$-$*$-bound-algebra structure of $\mathcal{M}_{n\times n}(\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle)$ defined above is consistent. In other words, we must see if our definition of the formal star is related to the natural star that exists in $\mathcal{M}_{n\times n}(\mathcal{P}(A^*))$. At first, observe that $(\mathcal{M}_{n\times n}(\mathcal{P}(A^*)), \cup, \times)$ has a natural $\mathcal{B}$-algebra structure inherited from $\mathcal{P}(A^*)$. Moreover, we can give it a $\mathcal{B}$-$*$-algebra structure if we extend the star of $\mathcal{P}(A^*)$ by defining for every M in $\mathcal{M}_{n\times n}(\mathcal{P}(A^*))$,

$$M^* = \bigcup_{n\geq 0} M^n \qquad (\mathcal{P})$$

This gives a $\mathcal{B}$-$*$-bound-algebra structure to $\mathcal{M}_{n\times n}(\mathcal{P}(A^*))$ as can be easily checked. Let us still denote by λ the $\mathcal{B}$-algebra morphism from $\mathcal{M}_{n\times m}(\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle)$ into $\mathcal{M}_{n\times m}(\mathcal{P}(A^*))$, called *matrix interpretation*, which is defined by

$$\forall M \in \mathcal{M}_{n\times m}(\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle), \quad \lambda(M) = [\lambda(M_{i,j})]_{1\leq i,j\leq n} \in \mathcal{M}_{n\times m}(\mathcal{P}(A^*)) \qquad (\Lambda)$$

Notes. (1) With this definition, we can rewrite Definition 3.1 as follows:

$$\forall M, N \in \mathcal{M}_{n\times m}(\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle), \quad M \approx N \text{ iff } \lambda(M) = \lambda(N).$$

(2) The morphism λ maps in fact $\mathcal{M}_{n\times m}(\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle)$ into $\mathcal{M}_{n\times m}(\mathrm{Rat}(A^*))$.

Then, the following result establishes that the formal star of a matrix in $\mathcal{M}_{n\times n}(\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle)$ has for interpretation the star, in the sense of relation $(\mathcal{P})$, of the interpretation of this matrix.

Proposition 3.3 (Krob [11, Chap. 3, Proposition III.9]). *The mapping λ from $\mathcal{M}_{n\times n}(\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle)$ into $\mathcal{M}_{n\times n}(\mathcal{P}(A^*))$, which is defined by (Λ), is a $\mathcal{B}$-$*$-morphism.*

3.3. Deductions and matrices

In this section, we show that several properties of the usual deductions hold also for matrix deductions. The two first results concern deductions of sums and products of matrices: their proofs are easy and are left to the reader.

Proposition 3.4. *Let A be an alphabet and let $\mathscr{A}$ be a system of $\mathscr{B}$-rational identities. Then, for every M, N, P, $Q \in \mathscr{M}_{n\times m}(\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle)$, we have*

$$\left.\begin{array}{l}\mathscr{A} \vdash M \approx N \\ \mathscr{A} \vdash P \approx Q\end{array}\right\} \Rightarrow \mathscr{A} \vdash M + P \approx N + Q.$$

Proposition 3.5. *Let A be an alphabet and let $\mathscr{A}$ be a system of $\mathscr{B}$-rational identities. Then, for M, $N \in \mathscr{M}_{n\times m}(\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle)$, P, $Q \in \mathscr{M}_{m\times p}(\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle)$, we have*

$$\left.\begin{array}{l}\mathscr{A} \vdash M \approx N \\ \mathscr{A} \vdash P \approx Q\end{array}\right\} \Rightarrow \mathscr{A} \vdash M.P \approx N.Q.$$

We can now study how a star can be deduced in a matrix deduction.

Proposition 3.6. *Let A be an alphabet and let $\mathscr{A}$ be a system of $\mathscr{B}$-rational identities. Then, for every M, N, P, $Q \in \mathscr{M}_{n\times n}(\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle)$, we have*

$$\mathscr{A} \vdash M \approx N \Rightarrow \mathscr{A} \overset{(M),(S)}{\vdash\!\!\!-\!\!\!-} M^* \approx N^*.$$

Proof. We shall prove this result by induction on n. If $n = 1$, the proposition is clear. Now let $n \geqslant 2$ and let us suppose that our result is proved for every order $< n$. Then let M, N be two matrices of $\mathscr{M}_{n\times n}(\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle)$ such that

$$\mathscr{A} \vdash M \approx N \qquad (\mathscr{H})$$

Let us write M and N as follows:

$$M = \begin{array}{c} \\ 1 \\ n-1 \end{array}\!\!\left(\begin{array}{c|c} \overset{1}{A} & \overset{n-1}{B} \\ \hline C & D \end{array}\right) \quad \text{and} \quad N = \begin{array}{c} \\ 1 \\ n-1 \end{array}\!\!\left(\begin{array}{c|c} \overset{1}{E} & \overset{n-1}{F} \\ \hline G & H \end{array}\right).$$

then relation $(\mathscr{H})$ gives us immediately

$$\mathscr{A} \vdash A \approx E, \qquad \mathscr{A} \vdash B \approx F,$$

$$\mathscr{A} \vdash C \approx G, \qquad \mathscr{A} \vdash D \approx H.$$

It follows from the induction hypothesis that

$$\mathscr{A} \overset{(M),(S)}{\vdash\!\!\!-\!\!\!-} D^* \approx H^*. \qquad (\mathrm{O})$$

Using the two previous propositions, it follows from (O) that

$$\mathscr{A} \overset{(M),(S)}{\vdash\!\!\!-\!\!\!-} A + BD^*C \approx E + FH^*G$$

$$\vdash\!\!\!-\!\!\!- (A + BD^*C)^* \approx (E + FH^*G)^* \qquad (1)$$

$$\overset{(M),(S)}{\vdash\!\!\!-\!\!\!-} D^*C(A + BD^*C)^* \approx H^*G(E + FH^*G)^*. \qquad (2)$$

However, using Propositions 3.4 and 3.5, $(\mathcal{H})$ also implies

$$\mathcal{A} \vdash D + CA^*B \approx H + GE^*F.$$

Hence, applying the induction hypothesis to this matrix identity of order $n-1$, we obtain the following deductions:

$$\mathcal{A} \overset{(M),(S)}{\vdash\!\!\!-\!\!\!-} (D + CA^*B)^* \approx (H + GE^*F)^* \tag{3}$$

$$\overset{(M),(S)}{\vdash\!\!\!-\!\!\!-} A^*B(D + CA^*B)^* \approx E^*F(H + GE^*F)^*, \tag{4}$$

due to Propositions 3.4 and 3.5. Therefore, according to Definition 3.2 and Corollary 3.2, relations (1), (2), (3) and (4) shows that

$$\mathcal{A} \overset{(M),(S)}{\vdash\!\!\!-\!\!\!-} M^* \approx N^*.$$

Hence, this ends the induction and proves our proposition. □

3.4. Matrix substitutions

According to the results of the last section, it seems natural to see if we can also replace letters by matrices in a deduction. Therefore let us give now the following definition.

Definition 3.3. Let A, B be two alphabets. Then we call *matrix substitution* of order n from A into B, every $\mathcal{B}$-*-morphism from the $\mathcal{B}$-*-algebra $\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle$ into the $\mathcal{B}$-*-algebra $\mathcal{M}_{n\times n}(\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle B\rangle)$.

Remark. We can easily extend this notion to matrix substitutions in matrices of $\mathcal{M}_{n\times m}(\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle)$ when this operation makes sense.

Proposition 3.7. *Let A, B be alphabets and let σ be a matrix substitution of order n from A into B. Then, there is a unique $\mathcal{B}$-*-morphism $\bar{\sigma}$ from* $\mathrm{Rat}(A^*)$ *into* $\mathcal{M}_{n\times n}(\mathrm{Rat}(B^*))$ *which makes the following diagram commutative*:

$$\begin{array}{ccc} \mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle & \xrightarrow{\sigma} & \mathcal{M}_{n\times n}(\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle B\rangle) \\ {\scriptstyle\lambda}\downarrow & & \downarrow{\scriptstyle\lambda} \\ \mathrm{Rat}(A^*) & \xrightarrow{\bar{\sigma}} & \mathcal{M}_{n\times n}(\mathrm{Rat}(B^*)) \end{array}$$

Proof. Observe that the unicity of $\bar{\sigma}$ is obvious. Indeed, if the previous diagram is commutative, we have necessarily for every letter $a \in A$,

$$\bar{\sigma}(a) = \bar{\sigma}(\lambda(a)) = \lambda(\sigma(a)). \tag{1}$$

Hence this relation clearly imposes the value of the $\mathcal{B}$-*-morphism $\bar{\sigma}$ on every

rational language L over A. Conversely, let us define for every $L \in \mathrm{Rat}(A^*)$,

$$\bar{\sigma}(L) = \bigcup_{w \in L} \lambda(\sigma(w)) \in \mathcal{M}_{n\times n}(\mathcal{P}(B^*)),$$

where we denote for every $w = a_1 \dots a_n$ in A^*, $\sigma(w) = \sigma(a_1) \dots \sigma(a_n)$. Then we can easily check that the mapping $\bar{\sigma}$ is a $\mathcal{B}$-$*$-morphism from the $\mathcal{B}$-$*$-algebra $\mathrm{Rat}(A^*)$ in the $\mathcal{B}$-$*$-algebra $\mathcal{M}_{n\times n}(\mathcal{P}(B^*))$. But, we have by construction,

$$\forall a \in A, \quad \bar{\sigma}(a) = \lambda(\sigma(a)) \in \mathcal{M}_{n\times n}(\mathrm{Rat}(B^*)).$$

It follows clearly that $\bar{\sigma}$ is a $\mathcal{B}$-$*$-morphism from $\mathrm{Rat}(A^*)$ into $\mathcal{M}_{n\times n}(\mathrm{Rat}(B^*))$. Therefore, since we may easily check that this mapping $\bar{\sigma}$ makes the desired diagram commutative, this ends our proof. □

It follows from the above result that rational identities are stable by matrix substitutions.

Corollary 3.8. *Let A, B be two alphabets, let σ be a matrix substitution of order n from A into B and let E, F be expressions of $\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle$. Then, we have*

$$E \approx F \Rightarrow \sigma(E) \approx \sigma(F).$$

Proof. Let us denote by $\bar{\sigma}$ the morphism associated with σ by Proposition 3.7 and let $E \approx F$ be a rational identity. Thus we have $\lambda(E) = \lambda(F)$. Therefore, we can write, according to the previous proposition,

$$\lambda(\sigma(E)) = \bar{\sigma}(\lambda(E)) = \bar{\sigma}(\lambda(F)) = \lambda(\sigma(F)).$$

This means exactly that we have the matrix identity $\sigma(E) \approx \sigma(F)$. □

Let $\mathcal{A}$ be a system of identities that implies all the matrix identities obtained by matrix substitutions from $\mathcal{A}$. Then the following proposition shows that the $\mathcal{A}$-deductions are stable by matrix substitutions for such a system.

Proposition 3.9. *Let A, B be alphabets and let $\mathcal{A}$ be a system of $\mathcal{B}$-rational identities over A. Let us suppose that we have for every matrix substitution σ from A into B,*

$$\mathcal{A} \overset{(M),(S)}{\vdash\!\!\!-\!\!\!-} \sigma(\mathcal{A}) \qquad (*)$$

Then, for every matrix substitution σ from A into B and for every rational expression E, F in $\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle$, we have

$$\mathcal{A} \vdash E \approx F \Rightarrow \mathcal{A} \overset{(M),(S)}{\vdash\!\!\!-\!\!\!-} \sigma(E) \approx \sigma(F).$$

Proof. First, observe that Corollary 3.8 ensures the consistency of our result. We shall now show by induction on the length l of the deduction

$$\mathcal{A} \vdash E \approx F,$$

that we have for every matrix substitution σ,

$$\mathcal{A} \overset{(M),(S)}{\vdash\!\!\!-\!\!\!-} \sigma(E) \approx \sigma(F).$$

If $l = 1$, then either $E = F$ or $E \approx F$ is an identity of $\mathcal{A}$. In these two cases, it follows clearly from (*) that $\mathcal{A}$ implies the identity $\sigma(E) \approx \sigma(F)$. Let us suppose now that the result is proved at order $l-1$ and let $(E_i, F_i)_{i=1,l}$ be an $\mathcal{A}$-deduction of length l. If the identity (E_l, F_l) comes from the previous ones by product, sum or star, it follows easily from Propositions 3.4, 3.5 and 3.6 and from the induction hypothesis that we have

$$\mathcal{A} \overset{(M),(S)}{\vdash\!\!\!-\!\!\!-} \sigma(E_l) \approx \sigma(F_l). \tag{1}$$

If (E_l, F_l) comes from the previous identities by symmetry, transitivity, if it is an element of $\mathcal{A}$ or if $E_l = F_l$, (1) is obvious. Finally, if (E_l, F_l) comes from a previous identity by use of a usual substitution τ, we have

$$\exists i < l, \quad E_l = \tau(E_i) \quad \text{and} \quad F_l = \tau(F_i).$$

Then the induction hypothesis applied to the matrix substitution $\sigma \circ \tau$ gives

$$\mathcal{A} \overset{(M),(S)}{\vdash\!\!\!-\!\!\!-} \sigma \circ \tau(E_i) \approx \sigma \circ \tau(F_i).$$

This means exactly that the relation (1) is true in this case. Therefore this ends our induction and proves our proposition. □

3.5. Matrix version of a rational identity

Let A be an alphabet. Let us now define the family $(X_a)_{a \in A}$ of alphabets by $X_a = \{x_{i,j}^a, 1 \leqslant i, j \leqslant n\}$ for every $a \in A$ and let us denote for every $a \in A$,

$$G_a = (x_{i,j}^a)_{1 \leqslant i,j \leqslant n} \in \mathcal{M}_{n \times n}(\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle X_a \rangle).$$

Let us also denote by X the union of the alphabets X_a. We will call *generic substitution of order n* the matrix substitution γ_A^n from A into X defined by

$$\forall a \in A, \quad \gamma_A^n(a) = G_a.$$

This leads us to the definition of the matrix version of an identity.

Definition 3.4. Let A be an alphabet. Then we call *matrix version* of order n of a $\mathcal{B}$-rational identity (E, F) over A, the matrix identity

$$\gamma_A^n(E) \approx \gamma_A^n(F).$$

Proposition 3.10. *Let A, B be alphabets, let (E, F) be a $\mathcal{B}$-rational identity and let σ be a matrix substitution of order n from A into B. Then we have*

$$\gamma_A^n(E) \approx \gamma_A^n(F) \overset{(M),(S)}{\vdash\!\!\!-\!\!\!-} \sigma(E) \approx \sigma(F).$$

Proof. Let us define a substitution τ from $\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle X\rangle$ into $\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle B\rangle$ by

$$\forall a \in A, \forall i,j \in [1,n], \quad \tau(x_{i,j}^{a}) = (\sigma(a))_{i,j}.$$

The universal property of $\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle$ implies clearly that we have $\sigma = \tau \circ \gamma_A^n$ and our result follows easily from this last equality. □

Remark. This proposition explains why only the generic version of a given rational identity was called its matrix version.

According to Propositions 3.9 and 3.10, it is interesting to find under which conditions a system of $\mathscr{B}$-rational identities $\mathscr{A}$ implies its matrix versions.

Lemma 3.11. *Let $\mathscr{A}$ be a system of $\mathscr{B}$-rational identities over an alphabet A. Then, for every n, p in $\mathbb{N}^*$, we have*

$$\forall p \leqslant n, \quad [\mathscr{A} \overset{(M),(S)}{\vdash\!\!\!-\!\!\!-} \gamma_A^n(\mathscr{A})] \Rightarrow [\mathscr{A} \overset{(M),(S)}{\vdash\!\!\!-\!\!\!-} \gamma_A^p(\mathscr{A})].$$

Proof. Let $p \leqslant n$ be two integers in $\mathbb{N}^*$ and let us suppose that $\mathscr{A}$ implies $\gamma_A^n(\mathscr{A})$ modulo (M), (S). Then, let us denote by $X_p \subset X_n$ the alphabets associated with the substitutions γ_A^p and γ_A^n and let us consider

$$\forall a \in A, \quad M_a = \begin{array}{c} \\ p \\ n-p \end{array} \overset{\begin{array}{cc} p & n-p \end{array}}{\left(\begin{array}{c|c} \gamma_A^p(a) & 0 \\ \hline 0 & 0 \end{array}\right)} \in \mathscr{M}_{n\times n}(\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle X_p\rangle).$$

Then we can obviously define a substitution σ from X_n into X_p such that

$$\forall a \in A, \quad \sigma(\gamma_A^n(a)) = M_a,$$

Let us denote by τ the matrix substitution $\sigma \circ \gamma_A^n$. Since $\gamma_A^n(\mathscr{A})$ is a consequence from $\mathscr{A}$, we obtain immediately applying the usual substitution σ,

$$\mathscr{A} \overset{(M),(S)}{\vdash\!\!\!-\!\!\!-} \sigma(\gamma_A^n(\mathscr{A})) = \tau(\mathscr{A}). \tag{*}$$

But it follows easily from the universal property of the $\mathscr{B}$-*-algebra $\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle$ that τ satisfies the following relation:

$$\forall E \in \mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle, \quad \tau(E) = \begin{array}{c} \\ p \\ n-p \end{array} \overset{\begin{array}{cc} p & n-p \end{array}}{\left(\begin{array}{c|c} \gamma_A^p(E) & 0 \\ \hline 0 & c(E)I_{n-p} \end{array}\right)} \tag{O}$$

According to (*), it follows immediately from (O) that $\mathscr{A}$ implies $\gamma_A^p(\mathscr{A})$. □

The next proposition shows that the generic version of order 2 of a system of identities $\mathscr{A}$ is strong enough to imply all the matrix versions of $\mathscr{A}$.

Proposition 3.12. *Let A be an alphabet and let $\mathscr{A}$ be a system of $\mathscr{B}$-rational identities over A. Then, for every n in $\mathbb{N}$, we have*

$$[\mathscr{A} \overset{(M),(S)}{\longmapsto} \gamma_A^2(\mathscr{A})] \Rightarrow [\mathscr{A} \overset{(M),(S)}{\longmapsto} \gamma_A^n(\mathscr{A})].$$

Proof. To obtain this result, we can restrict ourselves to show by lemma 3.11 that

$$\forall n \geqslant 1, \quad [\mathscr{A} \overset{(M),(S)}{\longmapsto} \gamma_A^2(\mathscr{A})] \Rightarrow [\mathscr{A} \overset{(M),(S)}{\longmapsto} \gamma_A^{2^n}(\mathscr{A})].$$

We will prove it by induction on n. Let us suppose now this result is proved at order $n \geqslant 1$ and let us show it at order $n+1$. We can then always write

$$\forall a \in A, \quad \gamma_A^{2^{n+1}}(a) = \begin{matrix} & 2^n & 2^n \\ 2^n & A_a & B_a \\ 2^n & C_a & D_a \end{matrix} \quad \text{i.e.} \quad \begin{pmatrix} A_a & B_a \\ C_a & D_a \end{pmatrix}.$$

Let us now consider the matrix substitutions $(\tau_{i,j})_{1 \leqslant i,j \leqslant 2}$ defined by

$$\forall a \in A, \qquad \tau_{1,1}(a) = A_a, \quad \tau_{1,2}(a) = B_a, \quad \tau_{2,1}(a) = C_a, \quad \tau_{2,2}(a) = D_a.$$

According to the universal property of $\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle$, we have obviously

$$\forall E \in \mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle, \quad \gamma_A^{2^{n+1}}(E) = \begin{pmatrix} \tau_{1,1}(E) & \tau_{1,2}(E) \\ \tau_{2,1}(E) & \tau_{2,2}(E) \end{pmatrix}. \tag{1}$$

Let us suppose now that $\mathscr{A} \overset{(M),(S)}{\longmapsto} \gamma_A^2(\mathscr{A})$. Therefore, applying the induction hypothesis and Proposition 3.10, we obtain

$$\forall i, j \in [1, 2], \quad \mathscr{A} \overset{(M),(S)}{\longmapsto} \tau_{i,j}(\mathscr{A}).$$

The relation (1) now permits us to conclude immediately that the induction hypothesis holds at order $n+1$. Hence, this ends our proof. □

Note. Consequently, it follows from Proposition 3.9 that if we have

$$\mathscr{A} \overset{(M),(S)}{\longmapsto} \gamma_A^2(\mathscr{A}),$$

then, for every matrix substitution σ, we have

$$\mathscr{A} \vdash E \approx F \Rightarrow \mathscr{A} \vdash \sigma(E) \approx \sigma(F).$$

3.6. Derivations and matrices

We can clearly define, entry by entry, the notion of a derivative with respect to a letter for a matrix. This matrix derivative is $\mathscr{B}$-linear. The following propositions, whose proofs are left to the reader since they can be easily proved by induction on n, show how it transforms products and stars.

Proposition 3.13. *Let A be an alphabet, let n, $m \in \mathbb{N}$ and let M, N be matrices of $\mathcal{M}_{n\times m}(\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle)$ and of $\mathcal{M}_{m\times n}(\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle)$. Then, for every a in A, we have*

$$\partial_a(MN) = \partial_a(M)N + c(M)\partial_a(N).$$

Proposition 3.14. *Let A be an alphabet, let n be an integer and let M be a matrix of $\mathcal{M}_{n\times n}(\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle)$. Then, for every letter a of A, we have*

$$(M) \wedge (S) \vdash \partial_a(M^*) \approx (c(M))^*\partial_a(M)M^*.$$

4. The + operation

4.1. The + operation for rational expressions

For technical reasons that will appear later, some results can be stated and proved more easily with the + operation. This explains why we have devoted this short section to the study of + though it is equivalent to $*$.

Definition 4.1. For every $E \in \mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle$, we denote $E^+ = E.E^*$.

Note. Since we work module (M) and (S), we have

$$E^+ = E.(1+E^*.E) = (1+E.E^*).E = E^*.E.$$

A $\mathcal{B}$-subalgebra of $\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle$, stable by +, will said to be $\mathcal{B}$-+-subalgebra of $\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle$. We also introduce the notion of *non-unitary* $\mathcal{B}$-+-algebra: it is a $\mathcal{B}$-+-algebra which has not necessarily a unit for the product.

Proposition 4.1. *Modulo (M) and (S), the following statements are true:*

(1) *the non-unitary $\mathcal{B}$-+-algebra of the $\mathcal{B}$-rational expressions with zero constant coefficient is generated by A as non-unitary $\mathcal{B}$-+-algebra;*

(2) *$\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle$ is generated as $\mathcal{B}$-+-algebra by A.*

Proof. Let us denote by $K = \mathrm{Ker}\, c$ the $\mathcal{B}$-algebra of the expressions with zero constant coefficient. K is clearly a non-unitary $\mathcal{B}$-+-algebra that contains A. Conversely, let L be a non-unitary $\mathcal{B}$-+-algebra containing A. We shall show by induction on the star height of E that we have for every E in $\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle$,

$$c(E) = 0 \Rightarrow E \in L. \qquad (\mathcal{R})$$

For star height 0, $(\mathcal{R})$ is obvious. Let us suppose now that our result is proved for any star height $< n$ and let E be an expression of star height n. According to proposition 2.11, we can write E modulo (M) and (S) as follows:

$$E = \sum_i E_{i_1}(F_{i_1})^* \ldots E_{i_{n-1}}(F_{i_n})^* E_{i_{n+1}},$$

where E_{i_p} and F_{i_p} are of star height $< n$ and where moreover $c(F_{i_p}) = 0$ for every i_p.

By the induction hypothesis, we obtain

$$\forall p \in [1, n], \quad F_{i_p} \in L \Rightarrow (F_{i_p})^+ \in L.$$

Since $c(E) = 0$, we have for every i at least $c(E_{i_p}) = 0$ for some E_{i_p} which will therefore be in L by our hypothesis. But, we have modulo (M) and (S),

$$E_{i_1}(F_{i_1})^* \dots E_{i_{n-1}}(F_{i_n})^* E_{i_{n+1}} = E_{i_1}(1 + F_{i_1}^+) \dots E_{i_{n-1}}(1 + F_{i_n}^+) E_{i_{n+1}}.$$

By Proposition 2.3, there exists some D_{i_p} with $c(D_{i_p}) = 0$ (and hence in L) such that we have modulo (M) and (S), $E_{i_p} \approx c(E_{i_p}) + D_{i_p}$. Hence, by distributivity, it follows easily that we have for every monomial,

$$E_{i_1}(F_{i_1})^* \dots E_{i_{n-1}}(F_{i_n})^* E_{i_{n+1}} \in L,$$

since we have $c(E_{i_p}) = 0$ for some i_p. Therefore $E \in L$. This ends our induction and proves (1). On the other hand, (2) follows from the fact that for every E in $\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle$, $E^* = 1 + E^+$ since $\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle$ is generated as $*$-algebra by A. □

The distinction that appeared above does not exist with the $*$ operation: indeed, every non-unitary sub-$\mathcal{B}$-$*$-algebra of $\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle$ contains 1 since $0^* = 1$, and, therefore, is a $\mathcal{B}$-$*$-algebra in the usual sense.

Note. The classical identities do not have a very pleasant form if $+$ is the only operation used. For instance, the reader can verify that

$$(S) \overset{(M)}{\longmapsto} (a+b)^+ \approx a^+ + a^+(b + ba^+)^+ + (b + ba^+)^+.$$

4.2. The $+$ operation for matrices

Definition 4.2. We define the $+$ operation for matrices by

$$\forall M \in \mathcal{M}_{n\times n}(\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle), \quad M^+ = M.M^*.$$

Note. By Theorem 3.1 and Corollary 3.2, we have modulo (M) and (S), $M^+ = M^*.M$.

Proposition 4.2. *Let $n \geq 2$ and let M be a matrix of $\mathcal{M}_{n\times n}(\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle)$ given by*

$$M = \begin{matrix} \\ p \\ q \end{matrix} \overset{\begin{matrix} p & q \end{matrix}}{\left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right)}$$

with $p + q = n$. Then the matrix M^+ is equal modulo (M) and (S) to

$$M^+ = \begin{matrix} \\ p \\ q \end{matrix} \overset{\begin{matrix} p & \quad\quad\quad\quad\quad\quad\quad\quad & q \end{matrix}}{\left(\begin{array}{c|c} (A + BC + BD^+C)^+ & (I_p + A^+)B(I_q + (D + CB + CA^+B)^+) \\ \hline (I_q + D^+)C(I_p + (A + BC + BD^+C)^+ & (D + CB + CA^+B)^+ \end{array}\right)}$$

Proof. It is an immediate consequence of Definition 3.2 and Theorem 3.1. □

Remark. The previous proposition gives an inductive definition which allows us to compute M^+ for every matrix. This definition is less pleasant to use than the corresponding one for the star. But, it will be important to know that such a definition exists.

5. Maximal ideals of a semigroup

This section is independent of the previous ones. Its only purpose is to group some classical results concerning maximal ideals of a semigroup that will be needed in the sequel. We refer to [17] for the standard definitions concerning semigroups that will not be recalled here.

5.1. Maximal left and right ideals

Definition 5.1. Let S be a semigroup. Then we call *maximal left* (resp. *right*) *ideal* every non-trivial (i.e. distinct from $\emptyset$ and from S) left (resp. right) ideal I of S such that we have for every left (resp. right) ideal J of S,

$$I \not\subset J \subset S \Rightarrow J = S.$$

Let us recall (see [17, p. 73]) that a semigroup is said to be *left* (resp. *right*) *simple* iff it does not have any non-trivial left (resp. right) ideal. We can now give the following result which the reader can easily prove:

Proposition 5.1. *Let S be a finite semigroup. Then the following statements are equivalent*:

(1) *S has a maximal left (resp. right) ideal*;

(2) *S is not left (resp. right) simple.*

The following proposition is obvious and its proof is left to the reader.

Proposition 5.2. *Let S be a semigroup and let $I \neq S$ be a left (resp. right) ideal of S. Then the following statements are equivalent*:

(1) *I is a maximal left (resp. right) ideal of S*;

(2) $\forall t \in S - I$, $I \cup S^1.t = S$ (resp. $I \cup t.S^1 = S$).

Corollary 5.3. *Let S be a semigroup and let I be a maximal left (resp. right) ideal of S. Then $S - I$ is a $\mathscr{L}$-class (resp. a $\mathscr{R}$-class) of S.*

Proof. We shall work in the left ideal case. Let α, β be elements of $S - I$. By the previous proposition, we have $I \cup S^1.\alpha = S$ and $I \cup S^1.\beta = S$. Therefore, since α and β are not in I; we can write

$$\alpha \in S^1.\beta \text{ and } \beta \in S^1.\alpha \Rightarrow S^1.\alpha = S^1.\beta.$$

Hence, α and β are in the same $\mathcal{L}$-class. But, an element of I and an element of $S-I$ cannot be in the same $\mathcal{L}$-class. From this remark, we can immediately conclude our proposition. □

Note. It is easy to see that all the results above can be generalized to the two-sided ideal case.

5.2. Semigroup generated by the complement of a maximal ideal

We present here a classical result that was introduced by Krohn and Rhodes. It can be found in [15, p. 87] in a slightly different form.

Proposition 5.4. *Let S be a non-left (resp. right) simple finite semigroup and let I be a maximal left (resp. right) ideal of S. Then, only the two following situations can appear:*

(1) *the semigroup generated by $S-I$ is* strictly *included in S;*

(2) *$S-I$ is reduced to a unique element α and $\alpha^2 \in I$.*

Proof. We will do the proof in the left ideal case. Let α be in $S-I$. Since I is a maximal left ideal of S, we are in one of the following situations:

(a) $I \cup S.\alpha = I$, i.e. $S.\alpha \subset I$ or

(b) $I \cup S.\alpha = S$.

At first, we shall study case (a). By Proposition 5.2, we have

$$I \cup S^1.\alpha = I \cup S.\alpha \cup \{\alpha\} = S.$$

It follows that $I \cup \{\alpha\} = S$ and hence that $S-I$ is reduced to a unique element α whose square is in I as $S.\alpha \subset I$. Therefore this ends our study in case (a). Let us suppose now that we are in case (b). Then the previous study allows us to claim that we have

$$\forall \alpha \in S-I, \quad I \cup S.\alpha = S \tag{1}$$

Hence, we deduce from (1) that we have for every $\alpha, \beta \in S-I$,

$$\alpha \in S.\beta \quad \text{and} \quad \beta \in S.\alpha \quad (\text{i.e. } S.\beta = S.\alpha).$$

Let us then denote by L the semigroup defined by $L = S.\alpha$ for every $\alpha \in S-I$. It is clear that $S-I \subset L$. Therefore, if $L \neq S$, the semigroup generated by $S-I$ is included in L and hence is obviously a strict subsemigroup of S. In the other case, $L = S$. Thus, we have $S.\alpha = S$ for every α in $S-I$. Then, it is easy to show that $S-I = \{\alpha \in S, S.\alpha = S\}$. It follows easily that here $S-I$ is a semigroup, strictly included in S. This last case ends our proof. □

Corollary 5.5. *Let S be a non-left (resp. right) simple finite semigroup and let I be a maximal left (resp. right) ideal of S. Then, the semigroup generated by $S-I$ is not*

strictly *included in S if and only if S is isomorphic to* $\mathbb{N}^*_{n,p}$ *and I is isomorphic to* $\mathbb{N}^*_{n,p} - \{1\}$ *for some integers n, p.*

Proof. According to Proposition 5.4, the situation of the corollary can only appear if $S - I = \{\alpha\}$ with $\alpha^2 \in I$. Hence, the semigroup generated by $S - I$ is generated by α and therefore is isomorphic to $\mathbb{N}^*_{n,p}$ for some integers n, p (see [17, p. 19]). The corollary now follows easily. □

6. Semigroup rational identities

6.1. Identities associated with a semigroup morphism

Let A be an alphabet, let S be a finite semigroup, let E be a finite set on which S acts on the right and let ψ be a semigroup morphism from A^+ into S. Let us also consider the matrix of $\mathcal{M}_{E\times E}(\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle)$:

$$C(S, E, \psi) = \left(\sum_{e\psi(a)=f} a \right)_{(e,f)\in E\times E}.$$

Let us finally denote

$$[C(S, E, \psi)]^+ = (E_{e,f})_{(e,f)\in E\times E}.$$

Lemma 6.1. *For every couple* (e, f) *of elements of E, we have*

$$\lambda(E_{e,f}) = \bigcup_{e\psi(w)=f} w. \tag{*}$$

Proof. We can write by Proposition 3.3,

$$\lambda(C(S, E, \psi)^+) = (\lambda(E_{e,f}))_{(e,f)\in E\times E} = \bigcup_{p=1}^{\infty} [\lambda(C(S, E, \psi))]^p. \tag{1}$$

It is also easy to prove by induction on p that we have for every $p \in \mathbb{N}^*$,

$$\lambda(C(S, E, \psi))^p = \left(\sum_{\substack{e\psi(w)=f \\ w\in A^p}} w \right)_{(e,f)\in E\times E}. \tag{2}$$

Our lemma now follows easily from relations (1) and (2). □

The previous lemma shows immediately the validity of the definition:

Definition 6.1. For every e in E, we shall denote by $P(\psi, e)$ the following $\mathscr{B}$-rational identity:

$$P(\psi, e): \quad A^+ \approx \sum_{f\in E} E_{e,f}.$$

Remark. The identity $P(\psi, e)$ can be written under the matrix form

$$P(\psi, e): \quad A^+ \approx u_e[C(S, E, \psi)]^+ u$$

that will be used often in the sequel (see Notation 1.4).

6.2. Identities associated with the action of a semigroup on a set

Let S be a finite semigroup, let E be a finite set on which S acts on the right and let $\rho = \{s_1, \ldots, s_n\}$ be a subset of S. Let us now introduce an alphabet $A_\rho = \{a_s, s \in \rho\}$, indexed by ρ. Then we can consider the natural semigroup morphism φ_ρ from A_ρ^+ into S defined by

$$\forall s \in \rho, \quad \varphi_\rho(a_s) = s.$$

We shall here denote by $C(S, E, \rho)$ the matrix $C(S, E, \varphi_\rho)$. Hence this leads us to the following definition:

Definition 6.2. For every e in E, the identity $P(\varphi_\rho, e)$ over the alphabet A_ρ will be called the *semigroup identity of order e* associated with the action of S on E relatively to ρ and denoted by $P(S, E, \rho, e)$.

Remark. The identity $P(S, E, \rho, e)$ can be written under the matrix form

$$P(S, E, \rho, e): \quad A^+ \approx u_e.[C(S, E, \rho)]^+.u.$$

6.2.1. Identities associated with the action of a semigroup on a set

At first, there is a very important special case of the previous definition which corresponds to the case $\rho = S$. In fact, it will be essentially the only one that we will consider in a first approach. We will denote by $C(S, E)$ the matrix $C(S, E, S)$. This leads us to the definition:

Definition 6.3. When $\rho = S$, the $\mathcal{B}$-rational identity $P(S, E, S, e)$ over A_S will be denoted by $P(S, E, e)$ and will be called the *semigroup identity of order e* associated with the action of S on E.

Note. This definition will provide us with a framework that will permit us to unify several results. But, we are essentially interested in fact by the case where S acts naturally on the right on itself.

6.2.2. Identities associated with a semigroup

There are also two important particular cases of Definition 6.2 that correspond to $E = S$ equipped with its natural action on itself. Thus we shall denote by

$C(S, \rho)$ the matrix $C(S, S, \rho)$ where ρ is a subset of S,

$C(S)$ the matrix $C(S, S, S)$ when $\rho = S$.

This leads us to the two following definitions:

Definition 6.4. When $E = S$, the $\mathcal{B}$-rational identity $P(S, S, \rho, s)$ over the alphabet A_ρ will be called the *semigroup identity of order s* associated with S relatively to ρ and will be denoted by $P(S, \rho, s)$.

Definition 6.5. When $E = S$ and $\rho = S$, the $\mathcal{B}$-rational identity $P(S, S, S, s)$ over the alphabet A_S will be called the *semigroup identity of order s* associated with S and will be denoted by $P(S, s)$.

Notes. (1) The identities $P(S, E, \rho, s)$ and $P(S, E, s)$ are respectively identities over alphabets with $|\rho|$ and $|S|$ letters.

(2) We will study in Section 14 the identities $P(S, \rho, s)$ in the case where ρ is a *generating system* of S.

6.3. Somes properties of semigroup identities

Observe that it follows from the following property applied with $\rho = S$ that the semigroup identities imply their versions relative to any subset. This explains why we will consider only semigroup identities initially.

Proposition 6.2. *Let S be a finite semigroup right acting on a finite set E, let $\rho' \subset \rho$ be two subsets of S and let e be in E. Then we have*

$$P(S, E, \rho, e) \overset{(M),(S)}{\longmapsto} P(S, E, \rho', e).$$

Proof. Let us denote by σ the substitution of A_ρ into $A_{\rho'}$ defined by

$$\forall s \in \rho - \rho',\ \sigma(a_s) = 0 \quad \text{and} \quad \forall r \in \rho',\ \sigma(a_r) = a_r.$$

Therefore we clearly have $\sigma(C(S, E, \rho)) = C(S, E, \rho')$. It follows that

$$\sigma([C(S, E, \rho)]^+) = [C(S, E, \rho')]^+.$$

The proposition is now obtained immediately. □

The following proposition shows that it is not necessary to consider the unit for S, if it exists, in order to study semigroup identities.

Proposition 6.3. *Let S be a monoid, let E be a finite set on which S acts on the right. Then, for every e in E, we have*

$$P(S, E, S - \{\mathrm{Id}\}, e) \overset{(M),(S)}{\longmapsto} P(S, E, e).$$

Proof. According to Proposition 6.2, we can restrict ourselves to proving

$$P(S, E, S-\{\mathrm{Id}\}, e) \overset{(M),(S)}{\vdash\!\!\!-\!\!\!-} P(S, E, e).$$

Let us denote $n = |E|$. Then we have obviously

$$C(S, E) = C(S, E, S-\{\mathrm{Id}\}) + a_{\mathrm{Id}}.I_n.$$

It follows from this relation that

$$(C(S, E))^+ = (C(S, E, S-\{\mathrm{Id}\}) + a_{\mathrm{Id}}.I_n)^+.$$

Therefore we have

$$\begin{aligned}(M)\wedge(S) &\vdash (C(S, E))^* \approx (a_{\mathrm{Id}}I_n)^*(C(S, E, S-\{\mathrm{Id}\})(a_{\mathrm{Id}}\mathrm{I_n})^*)^* \\ &\vdash (C(S, E))^* \approx a_{\mathrm{Id}}^*(C(S, E, S-\{\mathrm{Id}\})a_{\mathrm{Id}}^*)^*. \qquad (1)\end{aligned}$$

Let us denote by σ the substitution from $A_{S-\{\mathrm{Id}\}}$ into A_S defined by

$$\forall s \in S-\{\mathrm{Id}\}, \quad \sigma(a_s) = a_s a_{\mathrm{Id}}^*.$$

Thus relation (1) can be rewritten as

$$\begin{aligned}(M)\wedge(S) &\vdash\!\!\!-\!\!\!- (C(S, E))^* \approx a_{\mathrm{Id}}^*\sigma[(C(S, E, S-\{\mathrm{Id}\}))^*] \\ &\vdash\!\!\!-\!\!\!- u_e(C(S, E))^*u \approx a_{\mathrm{Id}}^*\sigma[u_e(C(S, E, S-\{\mathrm{Id}\}))^*u] \\ &\overset{P(S,E,S-\{\mathrm{Id}\},e)}{\vdash\!\!\!-\!\!\!-} u_e(C(S, E))^*u \approx a_{\mathrm{Id}}^*\sigma[A_{S-\{\mathrm{Id}\}}^*] \\ &\vdash\!\!\!-\!\!\!- u_e(C(S, E))^*u \approx a_{\mathrm{Id}}^*(A_{S-\{\mathrm{Id}\}}a_{\mathrm{Id}}^*)^* \\ &\overset{(S)}{\vdash\!\!\!-\!\!\!-} u_e(C(S, E))^*u \approx (A_{S-\{\mathrm{Id}\}} + a_{\mathrm{Id}})^* = A_S^*.\end{aligned}$$

Using Proposition 6.4 (which is independent of this result), it is now straightforward to finish the proof. □

Remark. It follows from Proposition 6.3 that we have for every semigroup S,

$$P(S, E, e) \overset{(M),(S)}{\vdash\!\!\!\dashv} P(S^1, E, e).$$

6.4. Monoid identities

We will here associate with every monoid another identity equivalent to the one associated by the previous process. Now let M be a finite monoid that acts on the right on a finite set E and let ρ be a subset of M. Then, let us introduce the following two matrices:

$$[C(M, E, \rho)]^* = (F_{e,f})_{(e,f)\in E\times E} \quad \text{and} \quad [C(M, E, \rho)]^+ = (E_{e,f})_{(e,f)\in E\times E}.$$

Then, the following relations hold clearly modulo (M) and (S):

$$\forall e \neq f \in E,\ E_{e,f} = F_{e,f} \quad \text{and} \quad \forall e \in E,\ E_{e,e} = 1 + F_{e,e}.$$

The validity of the following definition follows immediately from these relations and from Definition 6.2.

Definition 6.6. For every $e \in E$, we shall denote by $Q(M, E, \rho, e)$, the identity

$$Q(M, E, \rho, e): \quad A_M^* \approx \sum_{f \in E} F_{e,f},$$

that will be called the *monoid identity of order e* associated with the action of M on E relative to ρ.

Note. As in Section 6.2, we could define the different special cases of Definition 6.6.

Let us now show the equivalence between monoid identities and semigroup identities of the same order.

Proposition 6.4. *For every monoid M, for every subset ρ of M, for every set E on which M acts on the right and for every element e of E, we have*

$$P(M, E, \rho, e) \overset{(M),(S)}{\longmapsto} Q(M, E, \rho, e).$$

Proof. At first, we have for every $e \in E$,

$$\sum_{f \in E} F_{e,f} = 1 + \sum_{f \in E} E_{e,f}.$$

Therefore the deduction

$$P(M, E, \rho, e) \overset{(M),(S)}{\longmapsto} Q(M, E, \rho, e)$$

is obvious. To show the other deduction, let us observe at first that

$$Q(M, E, \rho, e) \overset{(M),(S)}{\longmapsto} A_\rho^+ = A_\rho^* A_\rho \approx \left(\sum_{f \in E} F_{e,f} \right) \left(\sum_{m \in \rho} a_m \right). \tag{1}$$

Now, we have by definition

$$[C(M, E, \rho)]^+ = [C(M, E, \rho)]^* C(M, E, \rho).$$

It follows that we have, for every f in E,

$$\sum_{u \in E} F_{e,u} \left(\sum_{um=f} a_m \right) = E_{e,f}.$$

Therefore this implies

$$\sum_{f \in E} E_{e,f} = \sum_{f \in E} \sum_{u \in E} \sum_{um=f} F_{e,u} a_m = \sum_{u \in E} \sum_{f \in E} \sum_{um=f} F_{e,u} a_m$$

$$= \sum_{u \in E} F_{e,u} \left(\sum_{f \in E} \sum_{um=f} a_m \right) = \sum_{u \in E} F_{e,u} \left(\sum_{m \in \rho} a_m \right).$$

Hence, according to (1), we have proved that

$$Q(M, E, \rho, e) \overset{(M),(S)}{\longmapsto} A_\rho^+ \approx \sum_{f \in E} E_{e,f} \dashv P(M, E, \rho, e).$$

Therefore this ends our proof. □

Note. When we work with monoids, and specially with groups, it will often be easier to use monoid identities rather than semigroup identities in effective computations.

Consequence. For every semigroup S right acting on a set E and for every e in E, we have according to Propositions 6.3 and 6.4,

$$P(S, E, e) \overset{(M),(S)}{\longmapsto} Q(S^1, E, e).$$

Hence, this shows that it is equivalent from the deduction viewpoint to work with the family of the semigroup identities $P(S)$ or with the family of the monoid identities $Q(M)$.

7. Structure of $C(S, E)^+$

The purpose of this section, which is the main part of our study, is to show that the matrix $[C(S, E)]^+$ has in a certain sense the same structure as $C(S, E)$. This result will be essential by its consequences.

7.1. Action matrices of a semigroup on a set

Definition 7.1. Let S be a finite semigroup right acting on a finite set E. Then we call *action matrices of S on E* the matrices $(M_s)_{s \in S}$ defined by

$$\forall s \in S, \quad M_s = (\delta_{e.s,f})_{(e,f) \in E \times E} \in \mathcal{M}_{E \times E}(\mathcal{B}).^4$$

Remarks. (1) The action matrices permit to *represent* the action of S on E in $\mathcal{M}_{E \times E}(\mathcal{B})$; this means that we have

$$\forall s, t \in S, \quad M_s M_t = M_{s.t}.$$

(2) Using the action matrices of S on E, the matrix $C(S, E)$ can be written

$$C(S, E) = \sum_{s \in S} a_s M_s.$$

Definition 7.2. Let S be a finite semigroup right acting on a finite set E. Then we shall denote by $\mathcal{E}[S, E]$ the matrix $\mathcal{B}$-algebra defined by

$$\mathcal{E}[S, E] = \sum_{s \in S} \mathcal{E}_{\mathcal{B}} \mathcal{R}\mathrm{at}\langle A \rangle M_s \subset \mathcal{M}_{E \times E}(\mathcal{E}_{\mathcal{B}} \mathcal{R}\mathrm{at}\langle A \rangle).$$

[4] We recall that $\delta_{e,f}$ denotes the Kronecker symbol which is equal to 1 when $e = f$ and to 0 when $e \neq f$.

Remark. Observe that $\mathscr{E}[S, E]$ is the $\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle$-subalgebra of $\mathscr{M}_{E\times E}(\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle)$ which is generated by the action matrices of S on E.

We can now present the main theorem we want to prove: we shall show that there exist rational expressions $(E_s)_{s\in S}$, independent of E, such that the following rational identity holds:

$$\mathscr{M}(S, E): \quad \left(\sum_{s\in S} a_s M_s\right)^+ \approx \sum_{s\in S} E_s M_s$$

modulo some $\mathscr{B}$-rational identities that we will make precise. This is equivalent to prove that $\mathscr{E}[S, E]$ is $+$-stable, modulo these identities.

Note. We understand here why $+$ was introduced. Indeed, since the unit matrix is not in general an action matrix, $(\mathscr{M}(S, E))$ cannot be stated with $*$.

7.2. Natural action of groups

We shall now prove the above result in the case of groups acting naturally on themselves. Observe that the action in the sense of semigroups is the same as in the usual sense for this natural action.

Definition 7.3. We associate with every finite group G the following matrices that take account of the *left* natural action of G on itself:

$$\forall g\in G, \quad P_g = (\delta_{gu,v})_{(u,v)\in G\times G} \in \mathscr{M}_{G\times G}(\mathscr{B}).$$

Remark. We can easily see that

$$\forall g, h\in G, \quad P_g P_h = P_{hg} \text{ and } P_{1_G} = \mathrm{Id}_G.$$

In particular, every matrix P_g is regular, with P_g^{-1} as inverse.

Notation. Let I be a finite set. Then, for every subset $\mathscr{F}$ of $\mathscr{M}_{I\times I}(\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle)$, we shall denote by $C_I(\mathscr{F})$ the *centralizer* in $\mathscr{M}_{I\times I}(\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle)$ of $\mathscr{F}$:

$$C_I(\mathscr{F}) = \{M\in \mathscr{M}_{I\times I}(\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle), \forall F\in\mathscr{F}, MF = FM\}.$$

The following result shows the connection between the matrices associated with the left action of G on itself and the $\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle$-algebra $\mathscr{E}[G, G]$.

Proposition 7.1. *Let G be a finite group equipped with its right natural action on itself. Then, we have*

$$\mathscr{E}[G, G] = C_G[(P_g)_{g\in G}].$$

Proof. Let M be in $\mathcal{M}_{G\times G}(\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle)$. Then, we can write for every g in G,

$$MP_g = \left(\sum_{w\in G} M(u,w)\delta_{gw,v}\right)_{(u,v)\in G\times G} = (M(u,g^{-1}v))_{(u,v)\in G=G},$$

$$P_gM = \left(\sum_{w\in G} \delta_{gu,w}M(w,v)\right)_{(u,v)\in G\times G} = (M(gu,v))_{(u,v)\in G\times G}.$$

From these two relations, we immediately deduce that

$$\begin{aligned} M\in C_G[(P_g)_{g\in G}] &\Leftrightarrow \forall g\in G, \forall u,v\in G, M(gu,v)=M(u,g^{-1}v)\\ &\Leftrightarrow \forall g\in G, \forall u,v\in G, M(u,v)=M(gu,gv)\\ &\Leftrightarrow \forall u,v\in G, M(u,v)=M(1,u^{-1}v)\\ &\Leftrightarrow \forall u,v\in G, M(u,v)=\sum_{g\in G} M(1,g)\delta_{ug,v}. \end{aligned}$$

This shows that M belongs to the centralizer of the family $(P_g)_{g\in G}$ iff

$$M=\sum_{g\in G} M(1,g)M_g.$$

i.e. iff M belongs to $\mathcal{E}[G,G]$. This was exactly what we wanted to obtain. □

We can now make precise the structure of $[C(G)]^*$ for every finite group G. It is given by the following proposition that generalizes a result of Conway (see [7, p. 111]), proved only in the case $G=\mathbb{Z}/n\mathbb{Z}$.

Proposition 7.2. *Let $(M_g)_{g\in G}$ be the action matrices of a finite group G relative to its natural right action on itself. Then, there exist rational expressions $(E_g)_{g\in G}$ such that we have modulo (M) and (S),*

$$\left[\sum_{g\in G} a_gM_g\right]^* = \sum_{g\in G} E_gM_g.$$

Proof. Let us denote by C the centralizer in $\mathcal{M}_{G\times G}(\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle)$ of the matrices $(P_g)_{g\in G}$ associated with the left natural action of G. Let us define also

$$\mathcal{M}=\sum_{g\in G} a_gM_g. \tag{1}$$

By Proposition 7.1, $\mathcal{M}\in C$. We will show that $\mathcal{M}^*\in C$, modulo (M) and (S). Then our result will follow by Proposition 7.1. Now let $g\in G$. Using (M), we can write

$$\begin{aligned} (P_g\mathcal{M}P_{g^{-1}})^* &= I_{|G|}+P_g\mathcal{M}[P_{g^{-1}}P_g\mathcal{M}]^*P_{g^{-1}} = P_g[I_{|G|}+\mathcal{M}\mathcal{M}^*]P_{g^{-1}}\\ &= P_g\mathcal{M}^*P_{g^{-1}}. \end{aligned}$$

But, since $\mathcal{M}\in C$, we have $\mathcal{M}=P_g\mathcal{M}P_{g^{-1}}$. It follows that we have

$$\mathcal{M}^*=P_g\mathcal{M}^*P_{g^{-1}} \quad (\text{i.e. } \mathcal{M}^*P_g=P_g\mathcal{M}^*).$$

Hence, since this result is true for every g in G, we have proved that $\mathcal{M}^*$ belongs to C. Therefore it ends the proof. □

Corollary 7.3. *Let $(M_g)_{g\in G}$ be the action matrices of a finite group G for its right natural action. Then there exist rational expressions $(E_g)_{g\in G}$ such that we have modulo (M) and (S),*

$$\left[\sum_{g\in G} a_g M_g\right]^+ = \sum_{g\in G} E_g M_g.$$

Proof. It is an obvious consequence of Proposition 7.2. □

Corollary 7.4. *The $\mathcal{B}$-algebra $\mathcal{E}[G, G]$ is $*$ and $+$ stable, modulo (M) and (S).*

Proof. This result follows from the two previous propositions: we just have to use an ordinary substitution in order to map the generic matrix $\mathcal{M}$, defined by relation (1) in the proof of Proposition 7.2, onto any element of $\mathcal{E}[G, G]$. □

Corollary 7.5. *Let G be a finite group and let g, h be in G. Then we have*

$$P(G, g) \overset{(M)\wedge(S)}{\longmapsto} P(G, h).$$

Proof. Let $(E_l)_{l\in G}$ be the expressions given by Corollary 7.3. Then we have

$$P(G, g) \overset{(M)\wedge(S)}{\longmapsto} A_G^+ \approx \sum_{l\in G} E_{g^{-1}l} \overset{(M)\wedge(S)}{\longmapsto} A_G^+ \approx \sum_{l\in G} E_l$$

for every g in G. The corollary now follows clearly. □

This result allows us to give the following definition.

Definition 7.4. Let G be a finite group. Then we shall call the *group identity* associated with G, and denote by $P(G)$, any one of the equivalent identities $(P(G, g))_{g\in G}$ considered modulo (M) and (S).

Note. Owing to Proposition 6.4, we will often use the monoid version of $P(G)$ in order to compute explicitly $P(G)$.

7.3. A generalization of group identities

In this section, we shall prove a result generalizing in a certain sense the definition of the group identity $P(G)$. At first, we shall generalize Corollary 7.4. Therefore,

let us define the matrix $P_g^{(n)}$ of order $[1, n]\times G$ as follows:

$$P_g^{(1)} = P_g \quad \text{and} \quad \forall n \geqslant 2,\ P_g^{(n)} = \left(\begin{array}{c|ccc} P_g & 0 & \dots & 0 \\ \hline 0 & & & \\ \vdots & & P_g^{(n-1)} & \\ 0 & & & \end{array}\right)$$

According to Proposition 7.1, the next result generalizes Corollary 7.4.

Proposition 7.6. *For every $n \geqslant 1$, the $\mathscr{B}$-algebra $C_{[1,n]\times G}[(P_g^{(n)})_{g\in G}]$ is a $\mathscr{B}$-$*$-algebra modulo (M) and (S).*

Proof. We shall use an induction on n. First, let us define for every $n \geqslant 1$,

$$\mathscr{C}_n = C_{[1,n]\times G}((P_g^{(n)})_{g\in G}).$$

The case $n = 1$ is an immediate consequence from Propositions 7.1 and 7.4. Now let $n \geqslant 2$ and let us suppose that the result is proved at every order $\leqslant n-1$. To show it at order n, it suffices to see that $\mathscr{C}_n$ is $*$-stable. Then let M be a matrix of order $[1, n]\times G$ in $\mathscr{C}_n$. We can decompose it as follows:

$$M = \left(\begin{array}{c|ccc} A & B_2 & \dots & B_n \\ \hline C_2 & & & \\ \vdots & & D & \\ C_n & & & \end{array}\right)$$

where A, $(B_i)_{i=2,n}$ and $(C_i)_{i=2,n}$ are square matrices of order G and where D is a square matrix of order $[1, n-1]\times G$. It is easy to see that

$$A \in \mathscr{C}_1,\ D \in \mathscr{C}_{n-1} \quad \text{and} \quad \forall i \in [2, n],\quad B_i \in \mathscr{C}_1,\ C_i \in \mathscr{C}_1 \tag{1}$$

By our induction hypothesis, D^* belongs to $\mathscr{C}_{n-1}$. Then let us decompose D^* in $(n-1)^2$ square blocks of order G as follows:

$$D^* = (\Delta_{i,j})_{(i,j)\in[2,n]} = \left(\begin{array}{ccc} \Delta_{2,2} & \dots & \Delta_{2,n} \\ \vdots & & \vdots \\ \Delta_{2,n} & \dots & \Delta_{n,n} \end{array}\right)$$

As $D^* \in \mathscr{C}_{n-1}$, it follows that we have

$$\Delta_{i,j} \in C_1 \tag{2}$$

for every $i, j \in [2, n]$. Let us introduce the matrix $U = [C_i A^* B_j]_{(i,j)\in[2,n]}$ of order $[1, n-1]\times G$. As $(C_i)_{i\geqslant 2}$, $(B_i)_{i\geqslant 2}$ and A^* are in $\mathscr{C}_1$, it follows that

$$U \in \mathscr{C}_{n-1}. \tag{3}$$

We can now begin proving that $M^* \in \mathscr{C}_n$. According to Definition 3.2, we have

$$M^* = \left(\begin{array}{c|ccc} W^* & X_2 & \dots & X_n \\ \hline Y_2 & & & \\ \vdots & & Z^* & \\ Y_n & & & \end{array}\right)$$

where the matrices W and Z are given by

$$W = A + \sum_{i,j \geqslant 2} B_i \Delta_{i,j} C_j \quad \text{and} \quad Z = D + U.$$

By (1), (2) and (3), we can now claim that $W \in \mathscr{C}_1$ and $Z \in \mathscr{C}_{n-1}$. Therefore, it follows from the induction hypothesis that $W^* \in \mathscr{C}_1$ and $Z^* \in \mathscr{C}_{n-1}$. Hence, we can decompose the matrix Z^* in blocks of order G:

$$Z^* = (\mathscr{Z}_{i,j})_{(i,j)\in[2,n]} = \left(\begin{array}{c|c|c} \mathscr{Z}_{2,2} & \dots & \mathscr{Z}_{2,n} \\ \vdots & & \vdots \\ \hline \mathscr{Z}_{2,n} & \dots & \mathscr{Z}_{n,n} \end{array}\right)$$

where each matrix $\mathscr{Z}_{i,j}$ belongs to $\mathscr{C}_1$. Observe finally that, according to Definition 3.2, the matrices (X_j) and (Y_i) are equal to

$$\forall i, j \in [2, n], \quad X_j = A^*\left(\sum_{i=2}^{n} B_i \mathscr{Z}_{i,j}\right) \text{ and } Y_i = \left(\sum_{j=2}^{n} \Delta_{i,j} C_j\right) W^*.$$

It follows immediately from the previous results that these matrices belong to $\mathscr{C}_1$. Hence we have proved that M^* belongs to $\mathscr{C}_n$. This ends our proof. □

Let us introduce some further new notations. At first, we associate with every finite group G, the matrix

$$J = (1)_{(u,v)\in G\times G} \in \mathscr{M}_{G\times G}(\mathscr{B})$$

and the matrices $J^{(n)}$ of order $[1, n] \times G$ which are defined by

$$J^{(1)} = J \quad \text{and} \quad \forall n \geqslant 2, J^{(n)} = \left(\begin{array}{c|c|c} J & 0 & \dots & 0 \\ \hline 0 & & & \\ \vdots & & J^{(n-1)} & \\ 0 & & & \end{array}\right)$$

To express $P(G)$ in a new form, we shall need the following lemma that the reader will easily prove with Proposition 4.2 by induction on the order of J.

Lemma 7.7. *For every $a \in A$, we have*

$$(M) \wedge (S) \vdash (a.J)^+ \approx a^+.J.$$

Proposition 7.8. *Let G be a finite group equipped with its right natural action. Then, every matrix M of $\mathscr{E}[G, G]$ commutes with J and we have*

$$P(G) \vdash^{(M),(S)} (M.J)^+ \approx M^+.J.$$

Proof. Indeed, let us consider the generic matrix of $\mathcal{C}[G, G]$:

$$\mathcal{M} = \sum_{g \in G} a_g M_g \in \mathcal{M}_{G \times G}(\mathcal{C}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A \rangle).$$

By Corollary 7.3, there exist $\mathcal{B}$-rational expressions $(E_g)_{g \in G}$ such that we have

$$\mathcal{M}^+ = \sum_{g \in G} E_g M_g$$

modulo (M), (S). On the other hand, we have

$$J.\mathcal{M} = \mathcal{M}.J = \left(\sum_{g \in G} a_g \right) J.$$

Therefore $\mathcal{M}$ does commute with J. Using a substitution, it follows easily that every matrix of $\mathcal{C}[G, G]$ does commute with J. Then, we obtain by Lemma 7.7

$$(\mathcal{M}.J)^+ = \left(\left(\sum_{g \in G} a_g \right) J \right)^+ = \left(\sum_{g \in G} a_g \right)^+ J$$

modulo (M) and (S). Thus, we have the equivalence modulo (M) and (S),

$$(\mathcal{M}.J)^+ \approx \mathcal{M}^+.J \vdash\!\dashv \left(\sum_{g \in G} a_g \right)^+ \approx \sum_{g \in G} E_g \vdash\!\dashv P(G).$$

In particular, we have

$$P(G) \xrightarrow{(M),(S)} (\mathcal{M}.J)^+ \approx \mathcal{M}^+.J.$$

The same result for a general matrix of $\mathcal{C}[G, G]$ now follows clearly. □

Remark. Conversely, if we have for every M in $\mathcal{C}[G, G]$, $(M.J)^+ \approx M^+.J$, the identity $P(G)$ will follow by taking $M = C(G)$.

We can now give the main result of this section; according to Proposition 7.1, it does appear as a generalization of Proposition 7.8.

Theorem 7.9. *Let G be a finite group and let $n \geq 1$. Then, every matrix M of order $[1, n] \times G$ which belongs to the centralizer in $\mathcal{M}_{[1,n] \times G}(\mathcal{C}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A \rangle)$ of the matrices $(P_g^{(n)})_{g \in G}$ commutes with $\mathcal{J}_n$. Moreover we have*

$$P(G) \xrightarrow{(M),(S)} (M.\mathcal{J}_n)^+ \approx M^+.\mathcal{J}_n^+.$$

Proof. At first, let us define for every $n \geq 1$,

$$\mathcal{C}_n = C_{[1,n] \times G}((P_g^{(n)})_{g \in G}).$$

We shall do the proof by induction on n exactly as for Proposition 7.6. For $n = 1$, the result comes from Proposition 7.8. Let $n \geq 2$ and let us suppose that our result

is proved at any order $<n$. Then let M be a matrix in $\mathscr{C}_n$:

$$M = \begin{array}{c} \\ G \\ G \\ \vdots \\ G \end{array} \begin{array}{c} \begin{array}{cccc} G & G & \dots & G \end{array} \\ \left(\begin{array}{c|c|c|c} A & B_2 & \dots & B_n \\ \hline C_2 & \multicolumn{3}{c}{\multirow{3}{*}{D}} \\ \vdots & & & \\ C_n & & & \end{array}\right) \end{array} = \left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right)$$

where B and C denote the matrices formed with the blocks $(B_i)_{i\geqslant 2}$ and $(C_i)_{i\geqslant 2}$, respectively. It is easily checked that

$$A\in\mathscr{C}_1,\ D\in\mathscr{C}_{n-1} \quad \text{and} \quad \forall i\in[2,n],\ B_i\in\mathscr{C}_1, C_i\in\mathscr{C}_1.$$

By our induction hypothesis, A, $(B_i)_{i\geqslant 2}$ and $(C_i)_{i\geqslant 2}$ do commute with J and D commutes with $\mathscr{J}_{n-1}$. It follows that M commutes with $\mathscr{J}_n$. Observe now that we can write modulo (M) and (S),

$$M.\mathscr{J}_n = \left(\begin{array}{c|c|c|c} AJ & B_2J & \dots & B_nJ \\ \hline C_2J & \multicolumn{3}{c}{\multirow{3}{*}{$D.\mathscr{J}_{n-1}$}} \\ \vdots & & & \\ C_nJ & & & \end{array}\right)$$

$$\Rightarrow (M.\mathscr{J}_n)^+ = \left(\begin{array}{c|c|c|c} \mathscr{E}^+ & \mathscr{F}_2 & \dots & \mathscr{F}_n \\ \hline \mathscr{G}_2 & \multicolumn{3}{c}{\multirow{3}{*}{$\mathscr{H}^+$}} \\ \vdots & & & \\ \mathscr{G}_n & & & \end{array}\right)$$

where the different matrices $\mathscr{E}$, $\mathscr{H}$, $(\mathscr{F}_i)_{i=2,n}$ and $(\mathscr{G}_i)_{i=2,n}$ are given by Proposition 4.2. We shall now define them. First, we have modulo (M) and (S),

$$\mathscr{E} = A.J + \sum_{2\leqslant i\leqslant n} (B_iJ)(C_iJ) + (J.B)(D.\mathscr{J}_{n-1})^+(C.J).$$

Therefore, since J is idempotent and since B_i and C_i commute with J, it follows from our induction hypothesis applied to D that

$$P(G) \xrightarrow{(M),(S)} \mathscr{E} \approx \left[A + \sum_{2\leqslant i\leqslant n} B_iC_i\right].J + (JB)(D^+\mathscr{J}_{n-1})(CJ). \tag{1}$$

By Proposition 7.6, $D^+\in\mathscr{C}_{n-1}$. Let us decompose D^+ in square blocks of order G:

$$D^+ = (\Delta_{i,j})_{(i,j)\in[2,n]}.$$

Thus each of these blocks will belong to $\mathscr{C}_1$ and commute with J by Propositions 7.1 and 7.8. Then it follows that

$$(JB)(D^+\mathscr{J}_n)(CJ) = \sum_{i,j\geqslant 2} (B_iJ)(\Delta_{i,j}J)(C_iJ) = \left(\sum_{i,j\geqslant 2} B_i\Delta_{i,j}C_i\right)J.$$

Therefore, using (1), we can write

$$P(G) \overset{(M),(S)}{\vdash\!\!\!-\!\!\!-} \mathscr{E} \approx (A + BC + BD^+C).J.$$

But, according to the previous results, the matrix

$$A + BC + BD^+C = A + \sum_{2 \leqslant i \leqslant n} B_i C_i + \sum_{2 \leqslant i,j \leqslant n} B_i \Delta_{i,j} C_j$$

belongs to $\mathscr{C}_1$. Therefore, by Propositions 7.1 and 7.8, we have

$$P(G) \overset{(M),(S)}{\vdash\!\!\!-\!\!\!-} \mathscr{E}^+ \approx (A + BC + BD^+C)^+.J. \tag{2}$$

Let us now study $\mathscr{H}$. We have

$$\mathscr{H} = D.\mathscr{J}_{n-1} + U + V, \tag{*}$$

where U and V denote the two matrices of order $[2, n] \times G$ given by

$$U = [(C_iJ)(B_jJ)]_{(i,j) \in [2,n]} \quad \text{and} \quad V = [(C_iJ)(A.J)^+(B_iJ)]_{(i,j) \in [2,n]}.$$

By Propositions 7.1 and 7.8 applied to A, Since $A^+ \in \mathscr{C}_1$ and since the matrices $(C_i)_{i=2,n}$, $(B_i)_{i=2,n}$ and A^+ commute with J, we obtain

$$U = [C_iB_jJ]_{i,j \geqslant 2} = CB.\mathscr{J}_{n-1},$$

$$P(G) \overset{(M),(S)}{\vdash\!\!\!-\!\!\!-} V \approx [C_i(A)^+B_jJ]_{i,j \geqslant 2} = CA^+B.\mathscr{J}_{n-1}.$$

By (*), it follows that

$$P(G) \overset{(M),(S)}{\vdash\!\!\!-\!\!\!-} \mathscr{H} \approx (D + CB + CA^+B).\mathscr{J}_{n-1}.$$

But, by the induction hypotheses and by Propositions 7.1 and 7.8, $D + CB + CA^+B$ clearly belongs to $\mathscr{C}_{n-1}$. Then, applying the induction hypothesis, we obtain

$$P(G) \overset{(M),(S)}{\vdash\!\!\!-\!\!\!-} \mathscr{H}^+ \approx (D + CB + CA^+B)^+.\mathscr{J}_{n-1}. \tag{3}$$

Finally let us study the case of $\mathscr{F}$ and $\mathscr{G}$. We can write

$$\mathscr{F} = (I_G + (A.J)^+)(JB)(I_{[2,n] \times G} + \mathscr{H}^+)$$

modulo (M) and (S). According to the above results, it follows that

$$P(G) \overset{(M),(S)}{\vdash\!\!\!-\!\!\!-} \mathscr{F} \approx (I_G + A^+J)(JB) \times (I_{[2,N] \times G} + (D + CB + CA^+B)^+.\mathscr{J}_{n-1}).$$

By our induction hypothesis and with the +-stability of $\mathscr{C}_{n-1}$, we obtain

$$P(G) \overset{(M),(S)}{\vdash\!\!\!-\!\!\!-} \mathscr{F} \approx J.(I_G + A^+) \times B(I_{[2,n] \times G} + (D + CB + CA^+B)^+). \tag{4}$$

In the same way, we can show that we also have

$$P(G) \vdash^{(M),(S)} \mathcal{G} \approx (I_{[2,n]\times G} + D^+) \times C(I_G + (A + BC + BD^+C)^+).J. \tag{5}$$

Observe now that the identities (2) to (5) mean exactly that

$$P(G) \vdash^{(M),(S)} (M.\mathcal{J}_n)^+ \approx M^+.\mathcal{J}_n.$$

Therefore this ends our induction and proves the proposition. □

7.4. Action of a group on a set

We shall now study the case when a group acts on the right on a finite set. Therefore, we shall first give a result concerning the right action of a group on its left cosets relative to a subgroup.

Lemma 7.10. *Let A be an alphabet, let J be the square matrix of order n whose entries are all 1 and let σ be the matrix substitution defined by*

$$\forall a \in A, \quad \sigma(a) = aJ.$$

Then, for every $E \in \mathscr{E}\mathscr{R}\mathrm{at}\langle A\rangle$ with zero constant coefficient, we have

$$(M) \wedge (S) \vdash \sigma(E) \approx EJ.^5$$

Proof. Let us consider the following set:

$$\mathcal{N} = \{E \in \mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle, (M) \wedge (S) \vdash \sigma(E) \approx EJ\}.$$

It is clear that $A \subset \mathcal{N}$ and that $\mathcal{N}$ is a non-unitary $\mathscr{B}$-algebra. But Lemma 7.7 ensures that $\mathcal{N}$ is a $\mathscr{B}$-+-algebra: therefore $\mathcal{N}$ contains the non-unitary $\mathscr{B}$-+-algebra generated by A. The lemma now follows by Proposition 4.1. □

For every group G and for every subgroup H of G, we denote by $(G/H)_\ell$ the set of the left cosets of G relative to H:

$$(G/H)_\ell = \{H.g, g \in G\}.$$

It is clear that G acts *naturally* on the right on $(G/H)_\ell$ by the action

$$(G/H)_\ell \times G \to (G/H)_\ell,$$

$$(H.u, v) \to H.uv.$$

Note that this action will always be the right action of G on $(G/H)_\ell$ to which we will refer in the sequel.

Proposition 7.11. *Let $(M_g)_{g\in G}$ be the matrices associated with the right natural action of a finite group G on itself and let $(E_g)_{g\in G}$ be the rational expressions given by*

[5] More generally, we can prove that we have $(M) \wedge (S) \vdash \sigma(E) \approx c(E) + E.J$ for every E in $\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle$.

Proposition 7.3. *Let H be a subgroup of G and let $(N_g)_{g\in G}$ be the action matrices of G on $(G/H)_\ell$ for the above action. Then, we have*

$$(P(H))\wedge(M)\wedge(S)\vdash\left(\sum_{g\in G}a_gN_g\right)^+\approx\sum_{g\in G}E_gN_g.$$

Proof. We shall consider here $\mathcal{H}=(G/H)_\ell$ and π the canonical projection of G onto $\mathcal{H}$. Let us also introduce the generic matrices

$$\mathcal{M}=\sum_{g\in G}a_gM_g\quad\text{and}\quad\mathcal{N}=\sum_{g\in G}a_gN_g=\left(\sum_{\alpha g=\beta}a_g\right)_{(\alpha,\beta)\in\mathcal{H}\times\mathcal{H}}.$$

Let us consider now, for every $h\in H$, the matrices

$$\mathcal{P}_h=(\delta_{h,u,v})_{(u,v)\in G\times G}.$$

At first, observe that $\mathcal{M}$ belongs to the centralizer of these matrices since for every $h\in H$ and for every pair $(u,v)\in G\times G$, we clearly have

$$(\mathcal{M}\mathcal{P}_h)_{(u,v)}=\sum_{w\in G}a_{u^{-1}w}\delta_{hw,v}=a_{u^{-1}h^{-1}v}=a_{(hu)^{-1}v},$$

$$(\mathcal{P}_h\mathcal{M})_{(u,v)}=\sum_{w\in G}\delta_{hu,w}a_{w^{-1}v}=a_{(hu)^{-1}v}.$$

Let us finally introduce the matrices $\mathcal{J}$ and J defined by

$$\mathcal{J}=(\delta_{\pi(g),\pi(h)})_{(g,h)\in G\times G}\in\mathcal{M}_{G\times G}(\mathcal{B})\quad\text{and}\quad J=(1)_{(\alpha,\beta)\in H\times H}\in\mathcal{M}_{H\times H}(\mathcal{B}).$$

Let us now compute $\mathcal{M}.\mathcal{J}$. For every pair (g,h) in $G\times G$, we have

$$(\mathcal{M}.\mathcal{J})_{(g,h)}=\sum_{u\in G}a_{g^{-1}u}\delta_{\pi(u),\pi(h)}=\sum_{\pi(g)l=\pi(h)}a_l=\mathcal{N}_{\pi(g),\pi(l)}.$$

Let σ denote the matrix substitution defined by

$$\forall g\in G,\quad\sigma(a_g)=a_gJ.$$

We can now express the previous result by $\mathcal{M}.\mathcal{J}=\sigma(\mathcal{N})$. As σ is a $+$-morphism, we have $(\mathcal{M}.\mathcal{J})^+=\sigma(\mathcal{N}^+)$. But, since $\mathcal{M}$ belongs to the centralizer of the family $(\mathcal{P}_h)_{h\in H}$, it follows by Theorem 7.9 that

$$P(H)\overset{(M),(S)}{\vdash}(\mathcal{M}.\mathcal{J})^+\approx\mathcal{M}^+.\mathcal{J},\quad\text{i.e.}$$

$$P(H)\overset{(M),(S)}{\vdash}\sigma(\mathcal{N}^+)\approx\mathcal{M}^+.\mathcal{J}.\qquad(*)$$

Since $c(\mathcal{N}^+)=c(\mathcal{N})^+=0$, every expression $(\mathcal{N}^+)_{\alpha,\beta}$ has a constant coefficient equal to 0. Then, Lemma 7.10 implies that we have modulo (M) and (S),

$$\sigma(\mathcal{N}^+)\approx((\mathcal{N}^+)_{\alpha,\beta}.J)_{(\alpha,\beta)\in\mathcal{H}\times\mathcal{H}}.$$

Identifying now the two parts of $(*)$, we obtain for every $\alpha,\beta\in\mathcal{H}$,

$$P(H)\overset{(M),(S)}{\vdash}(\mathcal{N})^+_{\alpha,\beta}\approx\sum_{\alpha l=\beta}E_l=\sum_{g\in G}E_g\delta_{\alpha g,\beta}$$

It now follows immediately that

$$P(H) \overset{(M),(S)}{\vdash\!\!\!-\!\!\!-} \mathcal{N}^+ \approx \sum_{g \in G} E_g N_g.$$

Therefore this ends our proof. □

This result being proved, we can now consider general group actions. We will need the following lemma that the reader will easily prove.

Lemma 7.12. *Let G be a finite group that acts on the right on a finite set E, let e be in E and let G_e be the following subgroup of G:*

$$G_e = \{g \in G,\ e.g = e.1_G\}.$$

Then, if we equip $e.G$ with the action of G obtained by restriction of the action of G on E, the following sets are isomorphic for the action of G:

$$e.G \simeq (G/G_e)_\ell.$$

Definition 7.5. Let G be a finite group that acts on the right on a finite set E and let $(G_e)_{e \in E}$ be the subgroups of G defined by Lemma 7.12. Then we associate with the action of G on E the following *set* of subgroups of G:

$$\mathcal{A}(G, E) = \bigcup_{e \in E} \{G_e\}$$

where the isomorphic groups are identified.

Example. When G right acts naturally on itself, we have $\mathcal{A}(G, G) = \{1_G\}$.

Proposition 7.13. *Let H be a subgroup of a finite group G. Then, we have*

$$(P(U))_{U \in \mathcal{A}(G,E)} \vdash (P(V))_{V \in \mathcal{A}(H,E)}.$$

Proof. Indeed, we clearly have for every $e \in E$, $H_e \subset G_e$. Therefore, by Proposition 12.1, which is completely independent of the sequel, and by Corollary 7.5, we have $P(G_e) \vdash P(H_e)$ for every $e \in E$. The proposition follows. □

Note. The above proof also shows that, if we are only interested in the identities $P(U)$ for $U \in \mathcal{A}(G, E)$, we can suppress in $\mathcal{A}(G, E)$ the subgroups of the groups that appear in it.

Proposition 7.1.4 (Action of a group on a set). *Let G be a finite group that acts on the right on a finite set E and let $(M_g)_{g \in G}$ denote the action matrices of G on E. Then, there exists $\mathcal{B}$-rational expressions $(E_g)_{g \in G}$ which* depend only *on S, such that*

$$(P(H))_{H \in \mathcal{A}(G,E)} \overset{(M),(S)}{\vdash\!\!\!-\!\!\!-} \left[\sum_{g \in G} a_g M_g\right]^+ \approx \sum_{g \in G} E_g M_g.$$

Proof. Let us denote $Q = E - E.G$. We can decompose $E.G$,

$$E.G = \bigcup_{i=1}^{n} e_i.G,$$

in a partition of distinct classes for the right action of G on E. Let us also introduce the generic matrix

$$\mathcal{M} = \sum_{g \in G} a_g M_g.$$

We can decompose each matrix M_g as follows:

$$M_g = \begin{array}{c} \\ E.G \\ Q \end{array} \begin{array}{c} \begin{array}{cc} E.G & Q \end{array} \\ \left(\begin{array}{c|c} P_g & 0 \\ \hline Q_g & 0 \end{array}\right) \end{array}$$

Since $M_g M_h = M_{gh}$, we clearly have

$$Q_g P_h = Q_{gh} \tag{0}$$

for every g, h in G. Let us now write $\mathcal{M}$ as follows:

$$\mathcal{M} = \begin{array}{c} \\ e_1.G \\ \vdots \\ e_n.G \\ Q \end{array} \begin{array}{c} \begin{array}{ccc} e_1.G & \cdots & e_n.G \end{array} \\ \left(\begin{array}{c|c|c} \mathcal{M}_1 & \cdots & 0 \\ \vdots & & \vdots \\ \hline 0 & \cdots & \mathcal{M}_n \\ \hline \mathcal{Q}_1 & \cdots & \mathcal{Q}_n \end{array} \right. \end{array} \begin{array}{c} Q \\ \left.\begin{array}{c} 0 \\ \vdots \\ 0 \\ \hline 0 \end{array}\right) \end{array} = \begin{array}{c} \\ E.G \\ Q \end{array} \begin{array}{c} \begin{array}{cc} E.G & Q \end{array} \\ \left(\begin{array}{c|c} \mathcal{P} & 0 \\ \hline \mathcal{Q} & 0 \end{array}\right) \end{array}$$

Then, using Definition 3.2, we can easily compute $\mathcal{M}^+$:

$$\mathcal{M}^+ = \begin{array}{c} \\ e_1.G \\ \vdots \\ e_n.G \\ Q \end{array} \begin{array}{c} \begin{array}{ccc} e_1.G & \cdots & e_n.G \end{array} \\ \left(\begin{array}{c|c|c} \mathcal{M}_1^+ & \cdots & 0 \\ \vdots & & \vdots \\ \hline 0 & \cdots & \mathcal{M}_n^+ \\ \hline \mathcal{Q}_1\mathcal{M}_1^* & \cdots & \mathcal{Q}_n\mathcal{M}_n^* \end{array} \right. \end{array} \begin{array}{c} Q \\ \left.\begin{array}{c} 0 \\ \vdots \\ 0 \\ \hline 0 \end{array}\right) \end{array} = \begin{array}{c} \\ E.G \\ Q \end{array} \begin{array}{c} \begin{array}{cc} E.G & Q \end{array} \\ \left(\begin{array}{c|c} \mathcal{P}^+ & 0 \\ \hline \mathcal{Q}\mathcal{P}^* & 0 \end{array}\right) \end{array}$$

Let $(A_g)_{g \in G}$ be the action matrices associated with the natural action of G on itself. By Corollary 7.3, there exist expressions $(E_g)_{g \in G}$ such that

$$\left(\sum_{g \in G} a_g A_g\right)^+ \approx \sum_{g \in G} E_g A_g.$$

Observe that it follows from Theorem 3.1 that we have modulo (M) and (S),

$$\left[\sum_{g \in G} a_g A_g\right]^+ \approx \sum_{g \in G} a_g A_g + \left[\sum_{g \in G} a_g A_g\right]\left[\sum_{g \in G} a_g A_g\right]^+.$$

Looking at this identity on the row associated with 1_G, we obtain

$$\forall g \in G, \quad E_g \approx a_g + \sum_{u \in G} a_u E_{u^{-1}g}. \tag{1}$$

But, Proposition 7.11 and Lemma 7.12 show that

$$(P(H))_{H\in\mathscr{A}(G,E)} \vdash \mathscr{P}^+ \approx \sum_{g\in G} E_g P_g. \tag{2}$$

Hence it follows that

$$\begin{aligned}(P(H))_{H\in\mathscr{A}(G,E)} &\vdash \mathscr{Q}\mathscr{P}^* = \mathscr{Q} + \mathscr{Q}\mathscr{P}^+ \approx \sum_{g\in G} a_g Q_g + \left(\sum_{g\in G} a_g Q_g\right)\left(\sum_{g\in G} E_g P_g\right)\\ &\vdash \mathscr{Q}\mathscr{P}^* \approx \sum_{g\in G} a_g Q_g + \sum_{g,h\in G} a_g E_h Q_{gh}.\end{aligned}$$

by (0). But, we can write, according to (1),

$$\begin{aligned}\sum_{g\in G} a_g Q_g + \sum_{g,h\in G} a_g E_h Q_{gh} &= \sum_{g\in G}\left(a_g + \left(\sum_{u\in G} a_u E_{u^{-1}g}\right)\right) Q_g\\ &= \sum_{g\in G} E_g Q_g.\end{aligned}$$

Therefore we showed that

$$(P(H))_{H\in\mathscr{A}(G,E)} \vdash \mathscr{Q}\mathscr{P}^* \approx \sum_{g\in G} E_g Q_g. \tag{3}$$

Then it follows immediately from (2) and (3) that we have

$$(P(H))_{H\in\mathscr{A}(G,E)} \vdash \mathscr{M}^+ \approx \sum_{g\in G} E_g M_g.$$

Since it is clear that the expressions $(E_g)_{g\in G}$ depend only on the natural action of G on itself, this ends our proof. □

Note. The above proof shows that the expressions $(E_g)_{g\in G}$ which occur in it are in fact those defined in Corollary 7.3; hence they depend only on G.

7.5. Action of a monogenic semigroup on a set

The aim of this section is to prove a result similar to Proposition 7.14, but for monogenic semigroups. Hence, since these semigroups are closely related to cyclic groups, it is not surprising that these last groups appear here.

Lemma 7.15. *For every $k \geqslant 0$, we have*

$$(M) \vdash a^k (a^p)^* \approx (a^p)^* a^k.$$

Proof. It clearly suffices to show the lemma for $k = 1$. Since we have

$$a(a^p)^* = a(1 + a^{p-1}(a^p)^* a) = (1 + a^p (a^p)^*) a = (a^p)^* a$$

modulo (M), the lemma follows. □

Lemma 7.16. *Let $p \in \mathbb{N}$ and let us denote by N the matrix $C(\mathbb{Z}/p\mathbb{Z}, \{1\})$. Then, we have modulo (M) and (S),*

$$(aN)^* \approx (a^p)^* \left(\sum_{i=0}^{p-1} a^i N^i \right).$$

Proof. Indeed, we can write the matrix $a.N$ as follows:

$$aN = \begin{array}{c} \\ 0 \\ \vdots \\ p-2 \\ p-1 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & \dots & p-1 \end{array} \\ \left(\begin{array}{ccc|c} 0 & a & \dots & 0 \\ \vdots & & & \vdots \\ 0 & \dots & 0 & 0 \\ 0 & \dots & 0 & a \\ \hline a & \dots & 0 & 0 \end{array} \right) \end{array} = \left(\begin{array}{c|c} A & B \\ \hline C & 0 \end{array} \right)$$

and compute its star with Definition 3.2:

$$(aN)^* = \left(\begin{array}{c|c} (A+BC)^* & A^*B(CA^*B)^* \\ \hline C(A+BC)^* & (CA^*B)^* \end{array} \right).$$

Since A is a nilpotent matrix of order $p-2$, the computation of A^* is easy. Indeed, we obtain by iterated use of (M):

$$A^* = I + A + \cdots + A^{p-2} + A^{p-1}A^* = \sum_{i=0}^{p-2} A^i.$$

It follows easily that $CA^*B = a^p$. With the previous formulas, we obtain easily by elementary computations

$$(aN)^* = \begin{array}{c} \\ 0 \\ \vdots \\ p-2 \\ p-1 \end{array} \begin{array}{c} \begin{array}{ccc} 0 & \dots & p-2 \end{array} \quad \begin{array}{c} p-1 \end{array} \\ \left(\begin{array}{ccc|c} & & & a^{p-1}(a^p)^* \\ & (A+BC)^* & & \vdots \\ & & & a(a^p)^* \\ \hline C(A+BC)^* & & & (a^p)^* \end{array} \right) \end{array}$$

Since we know the last column of $(aN)^*$, our result follows from Proposition 7.2 which described, modulo a substitution, the structure of this matrix. □

Note. This lemma also shows that the classical identity $P(n)$ is equivalent, modulo (M), (S), to the identity $P(\mathbb{Z}/n\mathbb{Z}, \{1\})$. This justifies our denotation of classical cyclic identity for $P(n)$.

Proposition 7.17. *Let N be a monogenic semigroup, isomorphic to $\mathbb{N}^*_{n,p}$ and let N_1 be the action matrix associated with N that corresponds to 1. Then, we have modulo (M) and (S),*

$$\forall k \geqslant n-1, \quad (aN_1)^* \approx \sum_{i=0}^{k-1} a^i N_1^i + (a^p)^* \left(\sum_{i=0}^{p-1} a^{k+i} N_1^{k+i} \right).$$

Proof. It is easy to check that we have

$$N_1 = \begin{array}{c} \\ 1 \\ \vdots \\ n-1 \\ n \\ \vdots \\ n+p-1 \end{array} \begin{array}{c} \begin{array}{cccccccc} 1 & 2 & \dots & n-1 & n & & \dots & n+p-1 \end{array} \\ \left(\begin{array}{cccc|cccc} 0 & 1 & \dots & 0 & 0 & & \dots & 0 \\ \vdots & & \ddots & \vdots & \vdots & & & \vdots \\ & & & 1 & 0 & & & 0 \\ 0 & 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ \hline & & & & 0 & 1 & \dots & 0 \\ & & 0 & & \vdots & & \ddots & \vdots \\ & & & & & & & 1 \\ & & & & 1 & 0 & \dots & 0 \end{array}\right) \end{array}$$

For every $k \geqslant 1$, let us denote

$$N_1^k = \begin{array}{c} \\ 1 \\ \vdots \\ n-1 \\ n \\ \vdots \\ n+p-1 \end{array} \begin{array}{c} \begin{array}{cc} 1 \dots n-1 & n \dots n-p-1 \end{array} \\ \left(\begin{array}{c|c} A_k & B_k \\ \hline 0 & C_k \end{array}\right) \end{array}$$

Since the matrix A_1 is nilpotent of order $n-1$, we immediately have $A_k = 0$ for every $k \geqslant n-1$. Let us also denote

$$(aN_1)^* = \begin{array}{c} \\ 1 \\ \vdots \\ n-1 \\ n \\ \vdots \\ n+p-1 \end{array} \begin{array}{c} \begin{array}{cc} 1 \dots n-1 & n \dots n-p-1 \end{array} \\ \left(\begin{array}{c|c} A & B \\ \hline 0 & C \end{array}\right) \end{array}$$

Using (M), we obtain for every $k \geqslant n-1$,

$$(aN_1)^* = \sum_{i=0}^{k-1} a^i N_1^i + a^k N_1^k (aN_1)^*.$$

But, since $k \geqslant n-1$, we have

$$N_1^k (aN_1)^* = \left(\begin{array}{c|c} 0 & B_k C \\ \hline 0 & C_k C \end{array}\right).$$

Now, Lemma 7.16 shows that

$$C = (aC_1)^* = (a^p)^* \left(\sum_{i=0}^{p-1} a^i C_i \right).$$

It follows that

$$C_k C = (a^p)^* \left(\sum_{i=0}^{p-1} a^i C_k C_i \right) \quad \text{and} \quad B_k C = (a^p)^* \left(\sum_{i=0}^{p-1} a^i B_k C_i \right).$$

But, since $A_k = 0$ and since $(N_1)^k (N_1)^i = N_1^{i+k}$, we obtain immediately that

$$C_k C_i = C_{i+k} \quad \text{and} \quad B_k C_i = B_{i+k}.$$

Then this allows us to write

$$C_k C = (a^p)^* \left(\sum_{i=0}^{p-1} a^i C_{i+k} \right) \quad \text{and} \quad B_k C = (a^p)^* \left(\sum_{i=0}^{p-1} a^i B_{k+i} \right).$$

Hence, we find finally that

$$N_1^k (aN_1) = \left(\begin{array}{c|c} 0 & B_k C \\ \hline 0 & C_k C \end{array} \right) = (a^p)^* \left(\sum_{i=0}^{p-1} a^i \left(\begin{array}{c|c} 0 & B_{i+k} C \\ \hline 0 & C_{i+k} C \end{array} \right) \right)$$

$$= (a^p)^* \left(\sum_{i=0}^{p-1} a^i (N_1)^{i+k} \right).$$

It follows that we have modulo (M) and (S),

$$(aN_1)^* = \sum_{i=0}^{k-1} a^i N_1^i + a^k (a^p)^* \left(\sum_{i=0}^{p-1} a^i (N_1)^{i+k} \right)$$

$$= \sum_{i=0}^{k-1} a^i N_1^i + (a^p)^* \left(\sum_{i=0}^{p-1} (aN_1)^{i+k} \right)$$

according to Lemma 7.15. Thus this ends our proof. □

Corollary 7.18. *Let N be a monogenic semigroup, isomorphic to $\mathbb{N}_{n,p}^*$ and let N_1 be the action matrix associated with N that corresponds to 1. Then, for every $k \geqslant n$, we have modulo (M) and (S),*

$$(aN_1)^+ \approx \sum_{i=1}^{k-1} a^i N_1^i + (a^p)^* \left(\sum_{i=0}^{p-1} a^{k+i} N_1^{k+i} \right).$$

Proof. It follows easily from Proposition 7.17, Definition 4.1 and Lemma 7.15. □

Corollary 7.19. *Let $q|p \in \mathbb{N}$ and let $r = p/q$. Let N, M be monogenic semigroups isomorphic to $\mathbb{N}_{n,p}^*$ and $\mathbb{N}_{m,q}^*$, respectively. Let us denote by M_1 the action matrix associated with M that corresponds to 1. Then, for every $k \geqslant m$, we have*

$$P(\mathbb{Z}/r\mathbb{Z}) \vdash (aM_1)^+ \approx \sum_{i=1}^{k-1} a^i M_1^i + (a^p)^* \left(\sum_{i=0}^{p-1} a^{k+i} M_1^{k+i} \right).$$

Proof. Indeed, according to the previous corollary, we have for every $k \geqslant m$,

$$(M_1)^+ \approx \sum_{i=1}^{k-1} a^i M_1^i + (a^q)^* \left(\sum_{i=0}^{q-1} a^{k+i} M_1^{k+i} \right) \tag{0}$$

modulo (M) and (S). But, according to the note following Lemma 7.16 and to

Proposition 6.2, it follows from $P(\mathbb{Z}/r\mathbb{Z})$ that

$$(a^q)^* \approx (a^{qr})^* \left(\sum_{i=0}^{r-1} a^{qi} \right) = (a^p)^* \left(\sum_{i=0}^{r-1} a^{qi} \right). \tag{1}$$

Therefore the following identity is a $P(\mathbb{Z}/r\mathbb{Z})$ consequence:

$$(a^q)^* \left(\sum_{i=0}^{q-1} a^{k+i} M_1^{k+i} \right) \approx (a^p)^* \left(\sum_{i=0}^{r-1} a^{qi} \right) \left(\sum_{i=0}^{q-1} a^{k+i} M_1^{k+i} \right)$$

$$\approx (ap)^* \left(\sum_{i=0}^{r-1} \sum_{j=0}^{q-1} a^{k+j+qi} M_1^{k+j} \right).$$

But, we clearly have $M_1^{k+j} = M_1^{k+j+qi}$ for every $i \in \mathbb{N}$ since $k \geqslant m$. Hence the following deduction holds:

$$P(\mathbb{Z}/r\mathbb{Z}) \vdash (a^q)^* \left(\sum_{i=0}^{q-1} a^{k+i} M_1^{k+i} \right) \approx (a^p)^* \left(\sum_{j=0}^{p-1} a^{k+j} M_1^{k+j} \right).$$

The proposition now follows according to relation (0). □

We can clearly define an action of $\mathbb{N}_{n,p}^*$ on $\mathbb{N}_{m,q}^*$ when $q|p$ and $n \leqslant m$ by

$$\forall [a] \in \mathbb{N}_{n,p}^*, \forall [b] \in \mathbb{N}_{m,q}^*, \quad [a]_{n,p} . [b]_{m,q} = [a+b]_{m,q}.$$

We will equip $\mathbb{N}_{m,q}^*$ with this action in the following lemma that will be easily proved by the reader.

Lemma 7.20. *Let N be a monogenic semigroup, isomorphic to $\mathbb{N}_{n,p}^*$ that acts on the right on a finite set E and let e be in E. Then, if we equip $e.N$ with the action of N obtained by restriction of the action of N on E, there exist m,q in $\mathbb{N}$ with $m \leqslant n$ and $q|p$ such that the sets $e.N \simeq \mathbb{N}_{m,q}^*$ are isomorphic for the action of N on them.*

Note. Let $\mathscr{Z}$ be the unique subsemigroup of N isomorphic to $\mathbb{Z}/p\mathbb{Z}$. Then, we clearly have $G_e \simeq \mathbb{Z}/r\mathbb{Z}$ for the action of $\mathscr{Z}$ on E.

Proposition 7.21. *Let S be a semigroup that acts on the right on a finite set E, let $s \in S$ and let M_s be the action matrix of S on E corresponding to s. Let $\mathbb{N}_{n,p}^*$ be the monogenic semigroup generated by s. Then, for $k \geqslant n$, we have*

$$(P(H))_{H \in \mathscr{A}(\mathbb{Z}/p\mathbb{Z},E)} \vdash (aM_s)^* \approx \sum_{i=1}^{k-1} a^i (M_s)^i + (a^p)^* \left(\sum_{i=0}^{p-1} a^{k+i} (M_s)^{k+i} \right).$$

Proof. The proof is exactly the same as for Proposition 7.14 up to some easy modifications: we just have to replace the propositions that are used in the proof of Proposition 7.14, by Corollary 7.19, Lemma 7.20 and the above note. □

Proposition 7.22 (Action of a monogenic semigroup on a set). *Let M be a semigroup isomorphic to $\mathbb{N}_{n,p}^*$ that acts on the right of a finite set E and let $(M_m)_{m \in M}$ be the*

action matrices of M on E. Then, there exist rational expressions $(E_m)_{m\in M}$ that depend only *on M such that*

$$(P(H))_{H\in\mathcal{A}(\mathbb{Z}/p\mathbb{Z},E)} \xrightarrow{(M),(S)} \left[\sum_{m\in M} a_m M_m\right]^+ \approx \sum_{m\in M} E_m M_m.$$

Proof. We can identify M to $\mathbb{N}^*_{n,p}$ and write $M=\{1,\dots,n+p-1\}$. We shall denote by $\mathcal{Z}=\{n,\dots,n+p-1\}$ the unique subsemigroup of N isomorphic to $\mathbb{Z}/p\mathbb{Z}$. Let us now introduce the matrix

$$\mathcal{P}=\sum_{i\in\mathcal{Z}} a_i M_i.$$

We shall prove by induction on k that there exist for every k in $[1,n]$ some rational expressions $(E_i)_{i\in[k,n+p-1]}$, independent of E, such that

$$(P(H))_{H\in\mathcal{A}(\mathbb{Z}/p\mathbb{Z},E)} \xrightarrow{(M),(S)} \left[\sum_{i=k}^{n-1} a_i M_i+\mathcal{P}\right]^+ \approx \sum_{i=k}^{n+p-1} E_i M_i.$$

For $k=n$, this result follows from Proposition 7.14 applied to $\mathcal{Z}$. Let $k\leqslant n$ and suppose our result is true at order k. We shall show it now at order $k-1$. Let us introduce the following matrices for every $k\leqslant n$:

$$\mathcal{M}_k=\sum_{i=k}^{n-1} a_i M_i+\mathcal{P}.$$

Then, using (S), we have

$$\mathcal{M}_{k-1}^*=(\mathcal{M}_k+a_{k-1}M_{k-1})^*=(a_{k-1}M_{k-1})^*(\mathcal{M}_k(a_{k-1}M_{k-1})^*)^* \tag{1}$$

The element $(k-1)$ generates a monogenic semigroup isomorphic to $\mathbb{N}^*_{m,q}$ for some $q|p$. According to Proposition 7.21, we have

$$(P(H))_{H\in\mathcal{A}(\mathbb{Z}/q\mathbb{Z},E)} \vdash (a_{k-1}M_{k-1})^* \approx I+\sum_{i=k-1}^{n+p-1} F_i M_i$$

with $\mathcal{B}$-rational expressions (F_i) which are independent of E. By Proposition 7.13, it follows that

$$(P(H))_{H\in\mathcal{A}(\mathbb{Z}/p\mathbb{Z},E)} \vdash (a_{k-1}M_{k-1})^* \approx I+\sum_{i=k-1}^{n+p-1} F_i M_i.$$

It follows from this identity and from (1) that

$$(P(H))_{H\in\mathcal{A}(\mathbb{Z}/p\mathbb{Z},E)} \vdash \mathcal{M}_{k-1}^* \approx \left(I+\sum_{i=k-1}^{n+p-1} F_i M_i\right)\left(\mathcal{M}_k\left(I+\sum_{i=k-1}^{n+p-1} F_i M_i\right)\right)^*.$$

It is easy to introduce adapted $\mathcal{B}$-rational expressions $(G_i)_{i\geqslant k}$, which will be independent of E by construction, such that

$$(P(H))_{H\in\mathcal{A}(\mathbb{Z}/p\mathbb{Z},E)} \vdash \mathcal{M}_{k-1}^* \approx \left(I+\sum_{i=k-1}^{n+p-1} F_i M_i\right)\left(\sum_{i=k}^{n+p-1} G_i M_i\right)^*. \tag{2}$$

By our induction hypothesis, it follows that there exist rational expressions $(H_i)_{i \geqslant k}$, depending only on M, such that

$$(P(H))_{H \in \mathscr{A}(\mathbb{Z}/p\mathbb{Z}, E)} \vdash \left(\sum_{i=k}^{n+p-1} G_i M_i \right)^* \approx \sum_{i=k}^{n+p-1} H_i M_i. \tag{3}$$

With (2) and (3), it is now easy to see that the induction hypothesis is true at order $k-1$. Therefore this ends our proof. □

Note. When we speak of "rational expressions *independent* of E", we mean expressions that are the same for any set E on which S acts. Consequently, we can obtain them in particular with the natural right action of S on itself.

7.6. Action of a simple semigroup on a set

We shall now study the case of the simple semigroups right acting on a set. First, let us give the following definition that extends Definition 7.5.

Definition 7.6. Let S be a finite semigroup right acting on a finite set E and let $\mathscr{G}$ denote the set of the groups included in S. Then we define

$$\mathscr{A}(S, E) = \bigcup_{G \in \mathscr{G}} \mathscr{A}(G, E) \subset \mathscr{G},$$

where the isomorphic groups are identified.

Notes. (1) Observe that $\mathscr{G}$ cannot be empty since the finite semigroup S has always an idempotent which forms clearly a trivial group.

(2) If S right acts naturally on itself, we note $\mathscr{A}(S)$ instead of $\mathscr{A}(S, S)$.

Example. If S is an aperiodic semigroup, $\mathscr{A}(S, E) = \{\{1_G\}\}$ for every set E.

Proposition 7.23. (Action of a simple semigroup on a set). *Let S be a finite left (resp. right) simple semigroup right acting on a finite set E and let $(M_s)_{s \in S}$ be the action matrices of S on E. Then, there exist rational expressions $(E_s)_{s \in S}$ which are* independent *of E such that*

$$(P(H))_{H \in \mathscr{A}(S,E)} \xvdash{(M),(S)} \left[\sum_{s \in S} a_s M_s \right]^+ \approx \sum_{s \in S} E_s M_s.$$

Proof. By symmetry, we can suppose that S is left simple. Then, there exist a finite group G and a part $P = (p_i)_{1 \leqslant i \leqslant n}$ of G such that S is isomorphic to the semigroup $M(n, G, P)$ (cf. [17, Chap. 3, Section 3.3] or [15, Chap. 3, Section 2]) which is constructed on the set $[1, n] \times G$ and whose law is defined by

$$(i, g).(l, h) = (i, g.p_l.h). \tag{1}$$

We shall prove the proposition by induction on n. If $n=1$, S is isomorphic to a group and our result follows from Proposition 7.14. Now let $n \geqslant 2$ and let us suppose our result is proved for every $M(n, G, P)$ with $k<n$. Then let S be a left simple semigroup isomorphic to $M(n, G, P)$ and let us introduce the matrix

$$\mathcal{S}=\sum_{s\in S} a_s M_s=\sum_{1\leqslant i\leqslant n, g\in G} a_{(i,g)}M_{(i,g)}.$$

Then, we have modulo (M) and (S),

$$\mathcal{S}^*=\left(\sum_{g\in G} a_{(n,g)}M_{(n,g)}\right)^*\left(\left(\sum_{1\leqslant i\leqslant n-1}^{g\in G} a_{(i,g)}M_{(i,g)}\right)\left(\sum_{g\in G} a_{(n,g)}M_{(n,g)}\right)^*\right)^*.$$

But it follows clearly from (1) that $\{n\}\times G$ is a group which consequently acts on E. Hence, according to Proposition 7.14, there exist $\mathcal{B}$-rational expressions $(E_{(n,g)})_{g\in G}$, independent of E, such that we have modulo (M) and (S),

$$(P(H))_{H\in\mathcal{A}(\{n\}\times G,E)} \vdash \Big(\sum_{g\in G} a_{(n,g)}.M_{(n,g)}\Big)^+ \approx \sum_{g\in G} E_{(n,g)}.M_{(n,g)}.$$

It follows that we have, modulo (M), (S) and the group identities associated with the groups of $\mathcal{A}(\{n\}\times G, E)$,

$$\begin{aligned}\mathcal{S}^* &= \left(I+\sum_{g\in G} E_{(n,g)}M_{(n,g)}\right)\\ &\quad\times\left(\left(\sum_{1\leqslant i\leqslant n-1}^{g\in G} a_{(i,g)}M_{(i,g)}\right)\left(I+\sum_{g\in G} E_{(n,g)}.M_{(n,g)}\right)\right)^*\\ &= \left(I+\sum_{g\in G} E_{(n,g)}M_{(n,g)}\right)\\ &\quad\times\left(\sum_{1\leqslant i\leqslant n-1}^{g,h\in G} a_{(i,g)}E_{(n,h)}M_{(i,gp_nh)}+\sum_{1\leqslant i\leqslant n-1}^{g\in G} a_{(i,g)}M_{(i,g)}\right)^*.\end{aligned}$$

We can obviously introduce a family $(F_{(i,l)})$ of $\mathcal{B}$-rational expressions, which will be by construction independent of E, such that

$$\sum_{1\leqslant i\leqslant n-1}^{g,h\in G} a_{(i,g)}E_{(n,h)}M_{(i,gp_nh)}+\sum_{1\leqslant i\leqslant n-1}^{g\in G} a_{(i,g)}M_{(i,g)}=\sum_{1\leqslant i\leqslant n-1}^{l\in G} F_{(i,l)}M_{(i,l)}$$

Since $\mathcal{A}(\{n\}\times G, E)\subset\mathcal{A}(S, E)$, we obtain

$$(P(H))_{H\in\mathcal{A}(S,E)} \vdash \mathcal{S}^*\approx\left(I+\sum_{g\in G} E_{(n,g)}M_{(n,g)}\right)\left(\sum_{1\leqslant i\leqslant n-1}^{l\in G} F_{(i,l)}M_{(i,l)}\right)^*.$$

Let us consider $\mathcal{U}=[1, n-1]\times G$ which is a left simple subsemigroup of S. Then, applying the induction hypothesis to $\mathcal{U}$ and substituting the expressions $F_{(i,l)}$ to the letters $a_{(i,l)}$ for each $(i,l)\in\mathcal{U}$, we easily obtain that there exist expressions $(A_{(i,l)})_{(i,l)\in\mathcal{U}}$, which will not depend on E, such that

$$(P(H))_{H\in\mathcal{A}(S,E)} \vdash \left(\sum_{1\leqslant i\leqslant n-1}^{l\in G} F_{(i,l)}M_{(i,l)}\right)^+ \approx \sum_{1\leqslant i\leqslant n-1}^{l\in G} A_{(i,l)}M_{(i,l)}$$

It follows easily that we have modulo (M) and (S),

$$(P(H))_{H\in\mathscr{A}(S,E)} \vdash \mathscr{S}^* \approx \left(I + \sum_{g\in G} E_{(n,g)}M_{(n,g)}\right)\left(I + \sum_{1\leqslant i\leqslant n-1}^{l\in G} A_{(i,l)}M_{(i,l)}\right).$$

Therefore, using (1), we can write

$$(P(H))_{H\in\mathscr{A}(S,E)} \vdash \mathscr{S}^* \approx I + \sum_{1\leqslant i\leqslant n}^{l\in G} B_{(i,l)}M_{(i,l)}$$

with some rational expressions $(B_{(i,l)})$ which are obviously independent of E. Hence it follows easily that the matrix $\mathscr{S}^+$ has the required form, modulo (M), (S) and the identities associated with the groups of $\mathscr{A}(S, E)$. This ends our induction and proves our proposition. □

Note. We can easily adapt the previous proof for simple semigroups.

7.7. The general structure theorem for $C(S, E)^+$

Finally we can prove the main result of this chapter.

Theorem 7.24 (Structure of $C(S, E)^+$). *Let S be a finite semigroup which acts on the right on a finite set E and let $(M_s)_{s\in S}$ be the action matrices of S on E. Then, there exist $\mathscr{B}$-rational expressions $(E_s)_{s\in S}$, which are* independent *of E, such that*

$$(P(H))_{H\in\mathscr{A}(S,E)} \xvdash{(M),(S)} \left[\sum_{s\in S} a_s M_s\right]^+ \approx \sum_{s\in S} E_s M_s.$$

Proof. We shall argue by induction on $|S|$. If $|S| = 1$, our result is obvious. Now let $n \geqslant 2$ and let us suppose that our result is proved for $|S| < n$. Then let S be a semigroup such that $|S| = n$. If S is left simple, the result follows from Proposition 7.23. In the same way, our theorem follows from Proposition 7.22 when S is a monogenic semigroup. Then we can suppose that S is neither left simple, nor isomorphic to a semigroup $\mathbb{N}^*_{n,p}$. Let us now consider a maximal left ideal I of S: then the subsemigroup U of S generated by $S - I$ is strictly included in S by Corollary 5.5. Thus, we can apply the induction hypothesis to U: hence, there exist $\mathscr{B}$-rational expressions $(E_u)_{u\in U}$, independent of E, such that

$$(P(H))_{H\in\mathscr{A}(U,E)} \vdash \left[\sum_{u\in U} a_u M_u\right]^+ \approx \sum_{u\in U} E_u M_u$$

modulo (M) and (S). Since $S - I \subset U$, it follows that there exist $\mathscr{B}$-rational expressions $(F_u)_{u\in U}$, independent of E, such that we have modulo (M) and (S),

$$(P(H))_{H\in\mathscr{A}(U,E)} \vdash \left[\sum_{u\in S-I} a_u M_u\right]^+ \approx \sum_{u\in U} F_u M_u.$$

Applying (S), we obtain

$$\left[\sum_{s\in S} a_s M_s\right]^* \approx \left[\sum_{u\in S-I} a_u M_u\right]^* \left(\left(\sum_{i\in I} a_i M_i\right)\left[\sum_{u\in S-I} a_u M_u\right]^*\right)^*.$$

Therefore it follows that we have modulo (M), (S) and $(P(H))_{H\in\mathcal{A}(U,E)}$,

$$\left[\sum_{s\in S} a_s M_s\right]^* \approx \left(I + \sum_{u\in U} F_u M_u\right)\left[\left(\sum_{i\in I} a_i M_i\right)\left(I + \sum_{u\in U} F_u M_u\right)\right]^*$$

$$\approx \left(I + \sum_{u\in U} F_u M_u\right)\left[\sum_{i\in I} a_i M_i + \sum_{i\in I, u\in U} a_i F_u M_{iu}\right]^*.$$

But, since I is a left ideal, we can clearly define $\mathcal{B}$-rational expressions $(A_i)_{i\in I}$, which are independent of E by construction, as follows:

$$\sum_{i\in I} a_i M_i + \sum_{i\in I, u\in U} a_i F_u M_{iu} = \sum_{i\in I} A_i M_i.$$

It now follows that

$$(P(H))_{H\in\mathcal{A}(U,E)} \vdash \left[\sum_{s\in S} a_s M_s\right]^* \approx \left(I + \sum_{u\in U} F_u M_u\right)\left(\sum_{i\in I} A_i M_i\right)^*.$$

But, I is also a strict subsemigroup of S. Hence, we can also apply the induction hypothesis to I. Using substitutions, it follows easily that there exist $\mathcal{B}$-rational expressions $(B_i)_{i\in I}$, independent of E, such that

$$(P(H))_{H\in\mathcal{A}(I,E)} \vdash \left[\sum_{i\in I} A_i M_i\right]^+ \approx \sum_{i\in I} B_i M_i.$$

Since $\mathcal{A}(I, E)$ and $\mathcal{A}(U, E)$ are subsets of $\mathcal{A}(S, E)$, we have

$$(P(H))_{H\in\mathcal{A}(S,E)} \vdash \left[\sum_{s\in S} a_s M_s\right]^* \approx \left(I + \sum_{u\in U} F_u M_u\right)\left(I + \sum_{i\in I} B_i M_i\right).$$

Grouping some terms, we can write

$$(P(H))_{H\in\mathcal{A}(S,E)} \xvdash{(M),(S)} \left[\sum_{s\in S} a_s M_s\right]^* \approx I + \sum_{s\in S} C_s M_s,$$

where $(C_s)_{s\in S}$ is a family of $\mathcal{B}$-rational expressions, which are independent of E by construction. It is now easy to conclude our induction. □

Remark. At the interpretation level, the identity given by Theorem 7.24 is quite easy to understand. Indeed, we have

$$\lambda\left(\sum_{s\in S} a_s M_s\right)^* = \sum_{k=0}^{\infty} \sum_{s_i\in S} a_{s_1} \dots a_{s_k} M_{s_1} \dots M_{s_k}$$

$$= \sum_{s\in S}\left(\sum_{k=0}^{\infty} \sum_{s_1 \dots s_k = s} a_{s_1} \dots a_{s_k}\right) M_s.$$

We also understand here why the expressions $(E_s)_{s\in S}$ do not depend on E.

From Theorem 7.24, we can now easily obtain the following results.

Corollary 7.25. *Let S be a finite semigroup which acts on the right on a finite set E and let $(M_s)_{s\in S}$ be the action matrices of S on E. Then, there exist $\mathcal{B}$-rational expressions $(E_s)_{s\in S}$,* independent *of E, such that*

$$(P(H))_{H\in\mathcal{A}(S,E)} \xrightarrow{(M),(S)} [C(S,E)]^+ \approx \left(\sum_{es=f} E_s\right)_{(e,f)\in E\times E} = \sum_{s\in S} E_s M_s.$$

Corollary 7.26. *Let S be a finite semigroup which acts naturally on the right on itself and let $(M_s)_{s\in S}$ be the associated action matrices. Then, there exist $\mathcal{B}$-rational expressions $(E_s)_{s\in S}$ such that*

$$(P(H))_{H\in\mathcal{A}(S)} \vdash [C(S)]^+ \approx \left(\sum_{us=v} E_s\right)_{(u,v)\in S\times S} = \sum_{s\in S} E_s M_s.$$

Note. The expressions $(E_s)_{s\in S}$ of Corollary 7.26 are also those of Corollary 7.25.

Corollary 7.27. *Let M be a monoid that acts on the right naturally on itself and let $(M_m)_{m\in M}$ be the associated action matrices. Then, there exist $\mathcal{B}$-rational expressions $(E_m)_{m\in M}$ such that*

$$(P(H))_{H\in\mathcal{A}(M)} \vdash [C(M)]^* \approx \left(\sum_{um=v} E_m\right)_{(u,v)\in M\times M} = \sum_{m\in M} E_m M_m.$$

Note. More generally, if M is a monoid and if 1_M induces the identity on E, Corollary 7.25 extends immediately to $C(M,E)^*$.

Corollary 7.28. *Let S be a finite semigroup which acts on the right on a finite set E. Then, the $\mathcal{B}$-algebra $\mathcal{E}[S,E]$ is $+$-stable modulo (M), (S) and the group identities associated with the groups of $\mathcal{A}(S,E)$.*

8. Consequences of the structure theorem

8.1. Semigroup identities equivalence

We study here the equivalence between the different semigroup identities that were introduced previously. Therefore we will need the following lemma.

Lemma 8.1. *Let S be a finite semigroup that acts on the right on a finite set E. Then, we have*

$$(P(H))_{H\in\mathcal{A}(S,E)} \vdash (P(H))_{H\in\mathcal{A}(S)}.$$

Proof. For every group $G\subset S$, for every $s\in S$ and for every $e\in E$, we clearly have the inclusion $G_s\subset G_{e.s}$. The lemma follows from Proposition 7.13. □

The following example shows that there are no inclusions between the *sets* $\mathcal{A}(S, E)$ and $\mathcal{A}(S)$ in general.

Example. Let us consider the semigroup $S = \mathbb{Z}/6\mathbb{Z} \cup \mathbb{Z}/2\mathbb{Z}$ equipped with the law $\oplus$, whose restriction to $\mathbb{Z}/6\mathbb{Z}$ and to $\mathbb{Z}/2\mathbb{Z}$ is the usual addition on these two groups and which relates the two parts of S by

$$\forall x \in \mathbb{Z}/6\mathbb{Z}, \forall y \in \mathbb{Z}/2\mathbb{Z}, \quad x \oplus y = x + y \ [2].$$

One can check that $\mathcal{A}(S) = \{\mathbb{Z}/3\mathbb{Z}\}$. But, if S acts on the right on the set $E = \{e\}$ by the trivial law $e.s = e$ for every $s \in S$, we have $\mathcal{A}(S, E) = \{\mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}\}$. Here, there are no inclusions between $\mathcal{A}(S)$ and $\mathcal{A}(S, E)$. This example shows also that the converse deduction of Lemma 8.1 is false since by Theorem 2.5, by Lemma 7.16 and by Theorem 14.5, $P(\mathbb{Z}/3\mathbb{Z})$ is independent of $P(\mathbb{Z}/2\mathbb{Z})$.

The following result says that the semigroup identities for the action of S on E relative to any element of E are all equivalent modulo the identities associated with the groups of $\mathcal{A}(S, E)$:

Proposition 8.2. *Let S be a semigroup that acts on the right on E and let $\rho \subset S$. Then, for every $e, f \in E$, we have modulo (M), (S) and $(P(H))_{H \in \mathcal{A}(S,E)}$,*

$$P(S, E, \rho, e) \vdash\!\dashv P(S, E, \rho, f) \vdash\!\dashv P(S, \rho, e) \vdash\!\dashv P(S, \rho, f).$$

Proof. It follows easily from Theorem 7.24 that we can write for every $e \in E$,

$$(P(H))_{H \in \mathcal{A}(S,E)} \overset{(M),(S)}{\vdash\!\dashv} u_e.[C(S, E, \rho)]^+.u \approx \sum_{v \in E} \left(\sum_{e.s = v} E_s \right) = \sum_{s \in S} E_s$$

with rational expressions $(E_s)_{s \in S}$ independent of E. Hence, we have modulo the group identities $(P(H))_{H \in \mathcal{A}(S,E)}$,

$$P(S, E, \rho, e) \overset{(M),(S)}{\vdash\!\dashv} A_\rho^+ \approx \sum_{s \in S} E_s.$$

Since the second member of the previous identity is independent of e and of E, the proposition follows with Lemma 8.1. □

The previous proposition allows us to give the following definitions:

Definition 8.1. Let S be a finite semigroup right acting on a finite set E and let $\rho \subset S$. Then we call *semigroup identity associated with the action of S on E relative to ρ*, and we denote by $P(S, E, \rho)$, any one of the equivalent identities $P(S, E, \rho, e)$, considered modulo (M), (S) and $(P(H))_{H \in \mathcal{A}(S,E)}$.

Definition 8.2. Let S be a finite semigroup and let ρ be a part of S. Then, we call *semigroup identity associated with S relative to ρ*, and we denote by $P(S, \rho)$, any one

of the equivalent identities $P(S, \rho, e)$, considered modulo (M), (S) and $(P(H))_{H \in \mathscr{A}(S)}$.

Notation. When $\rho = S$, we denote by $P(S, E)$ and $P(S)$ the identities that are introduced by Definitions 8.1 and 8.2.

Remarks. (1) In a semigroup S, there is not generally a distinguished element s that allows us to define the identity associated with S only relative to s. This is not the case in a monoid where the unit can play such a role. However we could have defined the identity associated with S as $P(S^1, 1)$ for instance (this choice was used by Conway (see [7, p. 116]). But, this would just give another presentation of the same results.

(2) When S is aperiodic, it follows from Proposition 8.2 that the semigroup identity $P(S)$ associated with S can be defined only modulo (M) and (S).

We can now obviously express Proposition 8.2 as follows:

Corollary 8.3. *Let S be a finite semigroup that acts on the right on a finite set E and let $\rho \subset S$. Then, we have modulo $(P(H))_{H \in \mathscr{A}(S,E)}$,*

$$P(S, \rho) \overset{(M),(S)}{\longmapsto} P(S, E, \rho).$$

Note. This corollary explains why we will progressively work only with the semigroup identities $P(S, \rho)$ or $P(S)$ in the sequel.

Example. Let G be a group and let $S = G \cup \{\infty\}$ be the semigroup obtained by adding an absorbing element ∞ to G. Then we have

$$C(S) = \begin{matrix} \\ G \\ \infty \end{matrix} \overset{\begin{matrix} G & \infty \end{matrix}}{\left(\begin{array}{c|c} C(G) & a_\infty u \\ \hline 0 & A_s \end{array}\right)}$$

Using Definition 3.2, we obtain immediately for every $g \in G$,

$$P(S, g) = [A_S^+ \approx u_g C(G)^+ u + u_g C(G)^* a_\infty A_S^* u]$$
$$\longmapsto A_S^* \approx u_g C(G)^* u (1 + a_\infty A_S^*)$$

when $P(S, \infty)$ is the tautology $A_S^+ \approx A_S^+$. Therefore, the different identities associated with S are not equivalent here. Moreover, for every $g \in G$, we have

$$P(S, g) \overset{P(G)}{\longmapsto} A_S^* \approx A_G^*(1 + a_\infty(A_G + a_\infty)^*)$$
$$\overset{(S)}{\longmapsto} A_S^* \approx A_G^* + A_G^* a_\infty (A_G^* a_\infty)^* A_G^*$$
$$\longmapsto A_S^* \approx (1 + A_G^* a_\infty (A_G^* a_\infty)^*) A_G^*$$

$$\vdash\!\!\xrightarrow{(M)}\!\!\dashv\ A_S^* \approx (A_G^* a_\infty)^* A_G^*$$

$$\vdash\!\!\xrightarrow{(S)}\!\!\dashv\ A_S^* \approx (A_G + a_\infty)^* = A_S^*.$$

This illustrates Proposition 8.2 since $\mathscr{A}(S) = \{G\}$. Observe also that this example shows that trivial identities can be obtained when we work modulo the group identities of $\mathscr{A}(S)$. Hence, it is not always possible to associate with a finite semigroup a non-trivial canonical identity as for a group.

8.2. *Matrix identities associated with semigroups*

Another main consequence of the $C(S, E)^+$ structure theorem is that the identity $P(S, E)$ implies its matrix versions. According to Proposition 3.9, this will allow us to use matrix substitutions in our deductions.

Theorem 8.4. *Let S be a finite semigroup right acting on a finite set E. Then, for every matrix substitution σ from A_S into $\mathscr{M}_{n\times n}(\mathscr{C}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle)$, we have*

$$(P(H))_{H\in\mathscr{A}(S,E)} \wedge P(S, E) \vdash\!\!\xrightarrow{(M),(S)}\!\!\dashv\ \sigma(P(S, E)).$$

Proof. According to Proposition 3.10, we may just prove this result for generic substitutions. First, we shall begin proving our result for $n = 2$. Let α_S, β_S, γ_S and δ_S be four copies of A_S and let σ be the generic matrix substitution of order 2 from A_S into $\mathscr{M}_{2\times 2}(\mathscr{C}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle\alpha_S, \beta_S, \gamma_S, \delta_S\rangle)$ which is defined by

$$\forall s \in S, \quad \sigma(a_s) = \begin{pmatrix} \alpha_s & \beta_s \\ \gamma_s & \delta_s \end{pmatrix} = X_s.$$

Then $\sigma(C(S, E))$ is a square matrix of order $E\times\{1, 2\}$:

$$\sigma(C(S, E)) = \begin{array}{c} \\ E\times\{1\} \\ E\times\{2\} \end{array} \begin{array}{c} \begin{array}{cc} E\times\{1\} & E\times\{2\} \end{array} \\ \left(\begin{array}{c|c} \sigma_\alpha(C(S, E)) & \sigma_\beta(C(S, E)) \\ \hline \sigma_\gamma(C(S, E)) & \sigma_\delta(C(S, E)) \end{array}\right) \end{array}$$

$$= \begin{array}{c} \\ E\times\{1\} \\ E\times\{2\} \end{array} \begin{array}{c} \begin{array}{cc} E\times\{1\} & E\times\{2\} \end{array} \\ \left(\begin{array}{c|c} C_\alpha & C_\beta \\ \hline C_\gamma & C_\delta \end{array}\right) \end{array}$$

where σ_α, σ_β, σ_γ and σ_δ denote the substitutions defined by

$$\forall s \in S, \qquad \sigma_\alpha(a_s) = \alpha_s, \quad \sigma_\beta(a_s) = \beta_s, \quad \sigma_\gamma(a_s) = \gamma, \quad \sigma_\delta(a_s) = \delta_s.$$

Now let e be in E. Then the identity $\sigma(P(S, E, e))$ can be written

$$\sigma(P(S, E, e)): \quad \left(\sum_{s\in S} X_s\right)^+ \approx U_e[\sigma(C(S, E))]^+ U,$$

where the matrices U_e and U are given by

$$U = \begin{matrix} \\ E\times\{1\} \\ \\ \\ E\times\{2\} \\ \\ \end{matrix} \overset{\begin{matrix} 1 & 2 \end{matrix}}{\begin{pmatrix} 1 & 0 \\ \vdots & \vdots \\ 1 & 0 \\ 0 & 1 \\ \vdots & \vdots \\ 0 & 1 \end{pmatrix}} \quad \text{and}$$

$$U_e = \begin{matrix} 1 \\ 2 \end{matrix} \begin{pmatrix} 0 & \dots & 0 & \overset{e}{1} & 0 & \dots & 0 & 0 & \dots & 0 & \overset{e}{0} & 0 & \dots & 0 \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & \dots & 0 & 1 & 0 & \dots & 0 \end{pmatrix}.$$
$$\qquad E = \{1\} \qquad\qquad\qquad E\times\{2\}$$

Using four square matrices of order E that will be made precise in the sequel, we can write $(\sigma[C(S,E)])^+$ as follows:

$$[\sigma(S,E)]^+ = \begin{matrix} E\times\{1\} \\ E\times\{2\} \end{matrix} \overset{\begin{matrix} E\times\{1\} & E\times\{2\} \end{matrix}}{\left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right)}.$$

Then the second member of the identity $\sigma(P(S,E,e))$ is given by

$$U_e.[\sigma(C(S,E))]^+.U = \begin{matrix} 1 \\ 2 \end{matrix} \overset{\begin{matrix} 1 & 2 \end{matrix}}{\left(\begin{array}{c|c} u_eAu & u_eBu \\ \hline u_eCu & u_eDu \end{array}\right)}.$$

We shall prove that $\sigma(P(S,E,e))$ is a consequence of $P(S,E,e)$ modulo (M), (S) and $(P(H))_{H\in\mathscr{A}(S,E)}$. To this end, let us now make explicit A:

$$A = \mathscr{A}^+ \quad \text{with } \mathscr{A} = C_\alpha + C_\beta C_\gamma + C_\beta C_\delta^+ C_\gamma.$$

We have for every $(e,f)\in E\times E$,

$$[C_\alpha + C_\beta C_\gamma]_{(e,f)} = \sum_{e.s=f} \alpha_s + \sum_{d\in E} \left(\sum_{e.u=d} \beta_u\right)\left(\sum_{d.v=f} \gamma_v\right)$$
$$= \sum_{e.s=f} \left(\alpha_s + \sum_{uv=s} \beta_u\gamma_v\right). \qquad (1)$$

But, by Theorem 7.24, there are also rational expressions $(E_s)_{s\in S}$ such that

$$(P(H))_{H\in\mathscr{A}(S,E)} \overset{(M),(S)}{\vdash\!\!\!-\!\!\!-} [C(S,E)]^+ \approx \left[\sum_{e.s=f} E_s\right]_{(e,f)\in E\times E}.$$

Hence, for every $(e,f)\in E\times E$, we have modulo the previous identities

$$[C_\beta C_\delta^+ C_\gamma]_{(e,f)} = \sum_{c,d\in E} \left(\sum_{e.u=c} \beta_u\right)\left(\sum_{c.v=d} \sigma_\delta(E_v)\right)\left(\sum_{d.w=f} \gamma_w\right)$$
$$= \sum_{e.s=f} \left(\sum_{uvw=s} \beta_u\sigma_\delta(E_v)\gamma_w\right). \qquad (2)$$

Let us now define for every s in S,

$$\mathcal{A}_s = \alpha_s + \sum_{uv=s} \beta_u \gamma_v + \sum_{uvw=s} \beta_u \sigma_\delta(E_v)\gamma_w.$$

Then it follows from (1) and (2) that the matrix $\mathcal{A}$ can be written

$$\mathcal{A} = \left[\sum_{e.s=f} \mathcal{A}_s\right]_{(e,f)\in E\times E}.$$

Hence let us introduce the substitution τ defined by $\tau(a_s) = \mathcal{A}_s$ for every s in S. Then we have $\mathcal{A} = \tau(C(S, E))$. It follows that

$$P(S, E, e) \vdash u_e.A.u = u_e.\mathcal{A}^+.u = \tau(u_e.[C(S, E)]^+.u) \approx \tau(A_S^+)$$

$$\vdash u_e.A.u \approx \left(\sum_{s\in S} \mathcal{A}_s\right)^+.$$

But, it is easy to see that

$$\sum_{s\in S} \mathcal{A}_s = \alpha_S + \beta_S\gamma_S + \beta_S\sigma_\delta\left(\sum_{s\in S} E_s\right)\gamma_S.$$

By a new application of $P(S, E, e)$, it follows that

$$P(S, E, e) \vdash \sum_{s\in S} \mathcal{A}_s \approx \alpha_S + \beta_S\gamma_S + \beta_S\delta_S^+\gamma_S.$$

Finally, it follows that we have modulo (M), (S) and $(P(H))_{H\in\mathcal{A}(S,E)}$,

$$P(S, E, e) \vdash u_e.A.u \approx (\alpha_S + \beta_S\gamma_S + \beta_S\delta_S^+\gamma_S)^+. \qquad (*)$$

Using exactly the same method, we can prove that we have modulo the above identities,

$$P(S, E, e) \vdash u_e.D.u \approx (\delta_S + \gamma_S\beta_S + \gamma_S\alpha_S^+\beta_S)^+.$$

Let us consider now the matrix C which is given by

$$C = (I_E + C_\alpha^+)C_\gamma(I_E + A).$$

By Proposition 8.2, the identities $P(S, E, e)$ are all equivalent modulo (M), (S) and $(P(H))_{H\in\mathcal{A}(S,E)}$. It follows from this result and from $(*)$ that

$$P(S, E) \vdash A.u \approx (\alpha_S + \beta_S\gamma_S + \beta_S\delta_S^+\gamma_S)^+u$$

$$\vdash u_eCu \approx u_e(I_E + C_\alpha^+)C_\gamma u(\alpha_S + \beta_S\gamma_S + \beta_S\delta_S^+\gamma_S)^*.$$

Since we clearly have $C_\gamma u = \gamma_S u = u\gamma_S$, we obtain

$$u_e(I_E + C_\alpha^+)C_\gamma u = u_e(I_e + C_\alpha^+)u\gamma_S = \gamma_S + u_eC_\alpha^+u\gamma_S$$

$$= \gamma_S + \sigma_\alpha(u_e[C(S, E)]^+u)\gamma_S.$$

Using $P(S, E, e)$, it follows that

$$P(S, E, e) \vdash u_e(I_E + C_\alpha^+)C_\gamma u \approx \gamma_S + \alpha_S^+\gamma_S.$$

Thus we have modulo (M), (S) and $(P(H))_{H\in\mathscr{A}(S,E)}$,

$$P(S,E) \vdash u_e.C.u \approx \alpha_S^* \gamma_S(\alpha_S+\beta_S\gamma_S+\beta_S\delta_S^+\gamma_S)^*.$$

A similar proof would also show that we have

$$P(S,E) \vdash u_e.B.u \approx \delta_S^*\beta_S(\delta_S+\gamma_S\beta_S+\gamma_S\alpha_S^+\beta_S)^*.$$

Hence, grouping all our results, we proved that we have modulo (M), (S) and $(P(H)_{H\in\mathscr{A}(S,E)}$,

$$P(S,E) \vdash U_e[\sigma(C(S,E))]^+U \approx \left(\begin{array}{c|c} (\alpha_S+\beta_S\gamma_S+\beta_S\delta_S^+\gamma_S)^+ & \delta_S^*\beta_S(\delta_S+\gamma_S\beta_S+\gamma_S\alpha_S^+\delta_S)^* \\ \hline \alpha_S^*\gamma_S(\alpha_S+\beta_S\gamma_S+\beta_S\delta_S^+\gamma_S)^* & (\delta_S+\gamma_S\beta_S+\gamma_S\alpha_S^+\beta_S)^+ \end{array}\right).$$

This means exactly that

$$(P(H)_{H\in\mathscr{A}(S,E)} \wedge P(S,E) \xvdash{(M),(S)} U_e[\sigma(C(S,E))]^+U \approx \left(\begin{array}{c|c} \alpha_S & \beta_S \\ \hline \gamma_S & \delta_S \end{array}\right)^+,$$

$$(P(H))_{H\in\mathscr{A}(S,E)} \wedge P(S,E) \xvdash{(M),(S)} U_e[\sigma(C(S,E))]^+U \approx \left(\sum_{s\in S} X_s\right)^+ = \sigma(A_S^+).$$

Thus we have proved the theorem for $n=2$. Since $\mathscr{A}(G,G)=\{1\}$ for any group G, it follows that the group identities imply their matrix versions of order 2, modulo (M), (S). Hence, according to Proposition 3.12, the identities $P(G)$ imply all their matrix versions. This being proved, our theorem follows from Proposition 3.12 applied with $P(S,E)$ and $(P(H))_{H\in\mathscr{A}(S,E)}$ since our proof and the above remark show that this system implies its matrix version of order 2. □

Note. The previous proof does not work for $P(S,E,\rho)$ with $\rho \neq S$. The problem of the matrix version of $P(S,E,\rho)$ will be considered in Section 14.

The two following results are immediate consequences of Theorem 8.4.

Corollary 8.5 (Matrix identities for groups). *Let G be a group and let $n\geq 2$. Then, for every matrix substitution σ from A_G into $\mathscr{M}_{n\times n}(\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle)$, we have*

$$P(G) \xvdash{(M),(S)} \sigma(P(G)).$$

Corollary 8.6 (Matrix identities for aperiodic semigroups). *Let S be an aperiodic semigroup right acting on a finite set E and let $n\geq 2$. Then, for every matrix substitution σ from A_G into $\mathscr{M}_{n\times n}(\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle)$, we have*

$$P(S,E) \xvdash{(M),(S)} \sigma(P(S,E)).$$

8.3. Derivatives of semigroup identities

Let S be a finite semigroup right acting on a finite set E and let $\rho \subset S$. For every e in E, we denote here by $A(S, E, \rho, e)$ the second member of the semigroup identity $P(S, E, \rho, e)$. Therefore, we can write with this notation,

$$P(S, E, \rho, e): \quad A_\rho^+ \approx A(S, E, \rho, e).$$

Proposition 8.7. *Let S be a semigroup that acts on the right on a set E, let ρ be a subset of S, let $e \in E$ and let $r \in \rho$. Then we have*

$$(M) \wedge (S) \vdash \partial_{a_r}(A(S, E, \rho, e)) \approx 1 + A(S, E, \rho, e.r).$$

Proof. By Proposition 3.13, we have modulo (M) and (S),

$$\begin{aligned}\partial_{a_r}([C(S, E, \rho)]^+) &= \partial_{a_r}(C(S, E, \rho)[C(S, E, \rho)]^*) \\ &= \partial_{a_r}(C(S, E, \rho)).[C(S, E, \rho)]^*.\end{aligned}$$

But, we also clearly have

$$\partial_{a_r}(C(S, E, \rho)) = \Delta_r = (\delta_{e.r,f})_{(e,f)\in E\times E} \in \mathcal{M}_{E\times E}(\mathcal{B}).$$

It follows immediately that

$$\partial_{a_r}(A(S, E, \rho, e)) = u_e.\Delta_r.[C(S, E, \rho)]^*.u = u_{e.r}.[C(S, E, \rho)]^*.u.$$

It is now straightforward to obtain our result. □

Note. Let M be a monoid that acts on the right on a set E. Let us denote by $B(M, E, \rho, e)$ the second member of the monoid identity

$$Q(M, E, \rho, e): \quad A_\rho^* \approx B(M, E, \rho, e).$$

Therefore, the same computation as above will show that

$$(M) \wedge (S) \vdash \partial_{a_r}(B(S, E, \rho, e)) \approx B(S, E, \rho, e.r),$$

for every $r \in \rho$ and $e \in E$. Thus monoid identities have a better behaviour relative to derivations than semigroup identities.

Corollary 8.8. *Let S be a semigroup that acts on the right on a set E,* let $\rho \subset S$ *and let $r \in \rho$. Then we have modulo (M), (S) and $(P(H))_{H\in\mathcal{A}(S,E)}$,*

$$P(S, E, \rho) \vdash\!\dashv \partial_{a_r}(P(S, E, \rho)).$$

Proof. This follows immediately from Propositions 8.7 and 8.2 and from the proof of Proposition 6.4 which remains valid for a semigroup. □

Note. The same result also holds for monoid identities.

8.4. The identity associated with U_2

We study here the monoid identities associated with U_2 (cf. Notation 1.2). We will show that these identities are all consequences of (M) and (S). This result will permit us to show that every identity associated with an aperiodic semigroup is a consequence of (M) and (S) (see Section 13).

Proposition 8.9. *We have the deduction* $(M) \wedge (S) \vdash P(U_2)$.

Proof. Since U_2 is aperiodic, the identity $P(U_2)$ is just defined modulo (M) and (S) according to Proposition 8.2. We can now easily compute

$$C(U_2, \{\sigma, \tau\}) = \begin{matrix} \\ \sigma \\ \tau \end{matrix} \overset{\begin{matrix} \sigma & \tau \end{matrix}}{\begin{pmatrix} a_\sigma & a_\tau \\ a_\sigma & a_\tau \end{pmatrix}}.$$

We immediately obtain by Definition 3.2,

$$[C(U_2, \{\sigma, \tau\})]^* = \begin{pmatrix} (a_\sigma + a_\tau a_\tau^* a_\sigma)^* & a_\sigma^* a_\tau (a_\tau + a_\sigma a_\sigma^* a_\tau)^* \\ a_\tau^* a_\sigma (a_\sigma + a_\tau a_\tau^* a_\sigma)^* & (a_\tau + a_\sigma a_\sigma^* a_\tau)^* \end{pmatrix}.$$

This shows that we have

$$Q(U_2, \{\sigma, \tau\}, \sigma): \quad (a_\sigma + a_\tau)^* \approx ((1 + a_\tau a_\tau^*) a_\sigma)^* + a_\sigma^* a_\tau ((1 + a_\sigma a_\sigma^*) a_\tau)^*.$$

Let us now introduce

$$D = ((1 + a_\tau a_\tau^*) a_\sigma)^* + a_\sigma^* a_\tau ((1 + a_\sigma a_\sigma^*) a_\tau)^*.$$

Therefore we clearly have

$$(M) \longmapsto D \approx (a_\tau^* a_\sigma)^* + a_\sigma^* a_\tau (a_\sigma^* a_\tau)^*$$

$$\overset{(M)}{\longmapsto} D \approx a_\tau^* (a_\sigma a_\tau^*)^* a_\sigma + 1 + a_\sigma^* a_\tau (a_\sigma^* a_\tau)^*$$

$$\overset{(M)}{\longmapsto} D \approx a_\tau^* (a_\sigma a_\tau^*)^* a_\sigma + (a_\sigma^* a_\tau)^*$$

$$\overset{(M)}{\longmapsto} D \approx a_\tau^* (a_\sigma a_\tau^*)^* a_\sigma + a_\sigma^* (a_\tau a_\sigma^*)^* a_\tau + 1$$

$$\overset{(S)}{\longmapsto} D \approx (a_\sigma + a_\tau)^* (a_\sigma + a_\tau) + 1 \overset{(M)}{\longmapsto} D \approx (a_\sigma + a_\tau)^*.$$

This proves that the identity $P(U_2, \{\sigma, \tau\}, \sigma)$ is a consequence of (M) and (S). Our result now follows easily from Propositions 6.3, 6.4 and 8.2. □

9. Universal rational expressions

This section is devoted to the proof of a result that will be the last step towards the completeness of the system of semigroup identities. Therefore, we will need to

study some properties of the $\mathcal{B}$-rational expressions $(E_s)_{s\in S}$ that are associated with a finite semigroup S by the Theorem 7.24.

9.1. Universal rational expressions associated with a semigroup

Let S be a finite semigroup right acting on a finite set E and let $(M_s)_{s\in S}$ be the action matrices of S on E. According to Theorem 7.24, there exists a family $(E_s)_{s\in S}$ of rational expressions, *independent of* E, such that

$$(P(H))_{H\in\mathcal{A}(S,E)} \xrightarrow{(M),(S)} \left(\sum_{s\in S} a_s M_s\right)^+ \approx \sum_{s\in S} E_s M_s \qquad (*)$$

Hence this leads us naturally to the following definition:

Definition 9.1. Let S be a finite semigroup. Then, we shall call *universal $\mathcal{B}$-rational expressions associated with* S the family $(E_s)_{s\in S}$ of $\mathcal{B}$-rational expressions which is constructed by the proof of Theorem 7.24.

Theorem 7.24 claims just that the expressions $(E_s)_{s\in S}$ associated with S are independent from E. But the relation $(*)$ does not characterize this family. Indeed, every family deduced from the previous one by (M) and (S) for instance, also satisfies $(*)$. Nevertheless, we have the following proposition.

Proposition 9.1. *Let S be a finite semigroup equipped with its natural action on S^1 and let $(M_s)_{s\in S}$ be the action matrices of S on S^1.*[6] *Then, the family $(E_s)_{s\in S}$ of the universal $\mathcal{B}$-rational expressions associated with S is* characterized, *modulo (M), (S) and $(P(H))_{H\in\mathcal{A}(S)}$ by*

$$\left(\sum_{s\in S} a_s M_s\right)^+ \approx \sum_{s\in S} E_s M_s. \qquad (**)$$

Proof. Since $\mathcal{A}(S, S^1) = \mathcal{A}(S)$, it follows from Theorem 7.24 that the universal $\mathcal{B}$-rational expressions associated with S satisfy $(**)$, modulo (M), (S) and $(P(H))_{H\in\mathcal{A}(S)}$. Thus, we just have to show that $(**)$ characterizes the family $(E_s)_{s\in S}$. This follows immediately from the fact that we have for every $s\in S$,

$$E_s = \left[\sum_{s\in S} E_s M_s\right]_{1,s}. \qquad (\mathscr{C})$$

Therefore this ends our proof. □

Note. Observe that the above relation $(\mathscr{C})$ clearly permits us to compute modulo (M), (S) and $(P(H))_{H\in\mathcal{A}(S)}$ the universal expressions associated with S.

[6] This family is exactly the family of the action matrices of the semigroup S^1 for its right natural action on itself, with the exception of I_{S^1}.

We shall now investigate the interpretation of the universal expressions which are associated with a given finite semigroup S. First, let us consider the alphabet $A_S = \{a_s, s \in S\}$ and let us denote by φ_S the semigroup morphism

$$\varphi_S : A_S^+ \to S,$$
$$a_s \to s.$$

Then, the interpretation of E_s is given by the following proposition

Proposition 9.2. *Let $(E_s)_{s\in S}$ denote the universal $\mathcal{B}$-rational expressions associated with a finite semigroup S. Then, we have $\lambda(E_s) = \varphi_S^{-1}(s)$.*

Proof. Let us consider the action matrices $(M_s)_{s\in S}$ associated with the right natural action of S on S^1. Since the matrix interpretation λ is a $*$-morphism by Proposition 3.3, it follows from Proposition 9.1 that

$$\lambda\left(\sum_{s\in S} a_s M_s\right)^+ = \left(\lambda\left(\sum_{s\in S} a_s M_s\right)\right)^+ = \left(\bigcup_{s\in S} a_s M_s\right)^+ = \bigcup_{s\in S} \lambda(E_s) M_s. \tag{1}$$

This relation stands in the $\mathcal{B}$-$*$-bound-algebra $\mathcal{M}_{S\times S}(\mathcal{P}(A_S^+))$. Using a classical technique, (cf. [2, p. 25] for instance) we can easily show that

$$\left(\bigcup_{s\in S} a_s M_s\right)^+ = \bigcup_{n\geqslant 1}\left(\bigcup_{w\in A_S^n} w M_{\varphi_S(w)}\right) = \bigcup_{w\in A_S^+} w M_{\varphi_S(w)}. \tag{2}$$

Relations (1) and (2) now imply that

$$\bigcup_{w\in A_S^+} w M_{\varphi_S(w)} = \bigcup_{s\in S} \lambda(E_s) M_s.$$

Identifying the languages in the $(1, s)$-entries of these matrices, we obtain

$$\lambda(E_s) = \bigcup_{\varphi_S(w)=s} w = \varphi_S^{-1}(s).$$

This ends our proof. □

Note. Hence, according to Theorem 7.24, we proved that the interpretation of the semigroup identity $P(S)$ is exactly $\lambda(A_S^+) = \sum_{s\in S} \varphi_S^{-1}(s)$.

Definition 9.2. Let S be a finite semigroup and let $n \in \mathbb{N}$. Then, we shall call *$\mathcal{B}$-linear representation* of order n of S any semigroup morphism μ from S into the matrix semigroup $\mathcal{M}_{n\times n}(\mathcal{B})$.

Notation. For every finite semigroup S and for every $\mathcal{B}$-linear representation μ of order n of S, we will denote by $\bar{\mu}$ the $\mathcal{B}$-$*$-morphism defined by

$$\bar{\mu} : \mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A_S\rangle \to \mathcal{M}_{n\times n}(\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A_S\rangle)$$
$$a_s \to a_s \mu(s).$$

We can now present the main result of this section: we shall show that, if $(E_s)_{s\in S}$ denote the universal expressions associated with a semigroup S, then we have for every $\mathcal{B}$-linear representation μ of S and for every s in S,

$$(M)\wedge(S) \vdash \bar{\mu}(E_s)\approx E_s\mu(s) \quad (\mathcal{M}(S,s)).$$

At the language level, this result is clear. Indeed, Proposition 3.7 shows that there is a $\mathcal{B}$-$*$-morphism $\hat{\mu}$ making the following diagram commutative:

$$\begin{array}{ccc} \mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A_S\rangle & \xrightarrow{\bar{\mu}} & \mathcal{M}_{n\times n}(\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A_S\rangle) \\ \lambda\downarrow & & \downarrow\lambda \\ \mathrm{Rat}(A_s^*) & \xrightarrow{\hat{\mu}} & \mathcal{M}_{n\times n}(\mathrm{Rat}(A_S^*)) \end{array}$$

It follows from this diagram and from Proposition 9.2 that we have

$$\lambda(\bar{\mu}(E_s)) = \hat{\mu}(\lambda(E_s)) = \hat{\mu}\left(\bigcup_{\varphi_S(w)=s} w\right).$$

We can easily check with the previous commutative diagram that, for every w in A_S^*, we have $\hat{\mu}(w) = w.\mu(\varphi(w))$. Thus, it follows from the above relation that

$$\lambda(\bar{\mu}(E_s)) = \bigcup_{\varphi_S(w)=s} w\mu(\varphi(w)) = \left(\bigcup_{\varphi_S(w)=s} w\right)\mu(s) = \lambda(E_s)\mu(s).$$

This ends our proof that $(\mathcal{M}(S,s))$ is really a $\mathcal{B}$-rational identity. Note finally that we will prove the identities $\mathcal{M}(S,s)$with the same method as in Section 7, beginning with groups before coming to general semigroups.

9.2 Structure of boolean idempotent matrices

We shall study in this section the structure of the idempotent matrices of $\mathcal{M}_{n\times n}(\mathcal{B})$. Observe that these matrices are exactly the images of the units by all $\mathcal{B}$-linear monoid representations.

Let us now give some definitions. We shall say that a matrix P of $\mathcal{M}_{n\times n}(\mathcal{B})$ is a *permutation* matrix iff there exist $\sigma\in\mathfrak{S}_n$ such that

$$\forall i,j\in[1,n], \quad P_{i,j} = \delta_{\sigma(i),j}$$

and we will denote this matrix by P_σ. Then it is easy to see that permutation matrices satisfy the following properties:

$$P_{\sigma^{-1}} = {}^tP_\sigma \quad \text{and} \quad \forall\sigma,\tau\in\mathfrak{S}_n, \quad P_\sigma P_\tau = P_{\tau\circ\sigma}.$$

Hence P_σ is invertible in $\mathcal{M}_{n\times n}(\mathcal{B})$ with $P_\sigma{}^{-1} = {}^tP_\sigma$ as inverse.[7] Observe also that multiplying a matrix M on the right (resp. on the left) by P_σ amounts to doing the permutation σ (resp. σ^{-1}) on the columns (resp. the rows) of M.

[7] The permutation matrices are in fact here the only boolean invertible matrices.

Then, we shall say that a matrix M of $\mathcal{M}_{n\times n}(\mathcal{B})$ is *reducible* iff there is a permutation matrix P_σ and an integer $p>0$ such that

$$P_\sigma M P_\sigma^{-1} = (M_{\sigma(i),\sigma(j)})_{(i,j)\in[1,n]} = \begin{array}{c} \\ p \\ n-p \end{array} \begin{array}{c} \begin{array}{cc} p & n-p \end{array} \\ \left(\begin{array}{c|c} A & B \\ \hline 0 & C \end{array}\right) \end{array}.$$

A matrix will be called *irreducible* iff it is not reducible. One can find several characterizations of real reducible or irreducible matrices in the literature (see [27] for example). It is not very difficult to show that they can in general be extended to our case. For instance, we have the following proposition.

Proposition 9.3. *A matrix $M \in \mathcal{M}_{n\times n}(\mathcal{B})$ is reducible iff there is a partition (I, J) of $[1, n]$ such that*

$$\forall i \in I, \forall j \in J, \quad M_{i,j} = 0.$$

In this section, we shall denote by J_n the matrix of $\mathcal{M}_{n\times n}(\mathcal{B})$ whose entries are all 1. We can now give:

Proposition 9.4. *The only idempotent and irreducible matrix in $\mathcal{M}_{n\times n}(\mathcal{B})$ is the matrix J_n.*

Proof. First, J_n is clearly irreducible and idempotent. Let us suppose now that there exist an idempotent and irreducible matrix M in $\mathcal{M}_{n\times n}(\mathcal{B})$ which is different from J_n. This means that there are at least two integers i, j such that $M_{i,j} = 0$. Then the set $I = \{k, M_{i,k} = 0\}$ is not empty. Let us consider $k \in I$. Since M is idempotent, we have

$$M_{i,k} = (M^2)_{i,k} = \sum_{l=1}^{n} M_{i,l} M_{l,k} = 0.$$

It now follows immediately by definition of I that

$$\sum_{l=1}^{n} M_{i,l} M_{l,k} = \sum_{l\in I} M_{i,l} M_{l,k} + \sum_{l\notin I} M_{i,l} M_{l,k} = \sum_{l\notin I} M_{l,k} = 0.$$

Since this equality holds in $\mathcal{B}$, it follows that $M_{l,k} = 0$ for every $l \notin I$. Thus, we have proved that $M_{l,k} = 0$ for every $k \in I$ and $l \notin I$. Since M is irreducible, it follows immediately from Proposition 9.3 that $I = [1, n]$. Hence, we have shown that

$$\forall k \in [1, n], \quad M_{i,k} = 0.$$

If now follows obviously from Proposition 9.3 that M is reducible which is not the case. Hence, this contradiction ends our proof. □

We can now study the structure of a general boolean idempotent matrix.

Theorem 9.5 (Boolean idempotent matrices' structure). *Let n be an integer and let M be an idempotent matrix in $\mathcal{M}_{n\times n}(\mathcal{B})$. Then, only two cases can occur:*

- *M is equal to the matrix J_n or to the zero matrix;*
- *there exists a permutation matrix $P_\sigma \in \mathcal{M}_{n\times n}(\mathcal{B})$, an integer $p \in [1, n[$ and an idempotent matrix N in $\mathcal{M}_{p\times p}(\mathcal{B})$ such that M can be written under one of the two following forms:*

$$M = P_\sigma^{-1}\left(\begin{array}{c|c} J_{n-p} & L \\ \hline 0 & N \end{array}\right) P_\sigma \quad \text{or} \quad M = P_\sigma^{-1}\left(\begin{array}{c|c} 0_{n-p} & L \\ \hline 0 & N \end{array}\right) P_\sigma.$$

Proof. Let $M \neq 0$ be an idempotent matrix in $\mathcal{M}_{n\times n}(\mathcal{B})$. Two cases can occur: if M is irreducible, Proposition 9.4 shows that $M = J_n$; on the other hand, if $M \neq 0$ is reducible, there will exist $p \in [1, n[$ and a permutation matrix P_σ such that

$$M = P_\sigma^{-1} \mathcal{M} P_\sigma \quad \text{with } \mathcal{M} = \begin{array}{c} \begin{matrix} n-p & p \end{matrix} \\ \left(\begin{array}{c|c} K & L \\ \hline 0 & N \end{array}\right) \begin{matrix} n-p \\ p \end{matrix} \end{array}.$$

We can clearly suppose that either $K = 0$ or K is irreducible. Indeed, if it were not the case, it would suffice to increase p. We can also easily check that $\mathcal{M}$ is idempotent. It follows that K and N are also idempotent. If $K = 0$, we immediately obtain one of the desired forms. If K is irreducible, we just have to use Proposition 9.4 in order to conclude. Hence this ends our proof. □

Note. The two above forms are not equivalent by row or column permutations as shown easily by the two following examples:

$$M = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad N = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}.$$

Note. In fact, starting from this theorem, one can continue the study and give the complete structure of a boolean idempotent matrix. One can show that such a matrix is formed of blocks of 0 and of 1, mixed with row and column permutations. We do not give this result here since the recursive structure given by Theorem 9.5 will suffice in the sequel.

9.3. A rational identity related to boolean idempotent matrices

The purpose of the previous study was to permit us to prove Proposition 9.7 which generalizes Lemma 7.7. We will need the following lemma:

Lemma 9.6 (Conway [7, p. 35]). *We have the following deduction:*

$$(M) \wedge (S) \vdash a^* a^* \approx a^*.$$

Proof. According to Proposition 2.2, we can write

$$(M)\wedge(S) \vdash\!\!\!- \; a^*a^* \approx a^*a^{**} = a^*(1a^*)^* \overset{(S)}{\vdash\!\!\!-} a^*a^* \approx (1+a)^*$$

$$\overset{(S)}{\vdash\!\!\!-} a^*a^* \approx 1^*(a1^*)^* = a^*.$$

This ends the proof of this lemma. □

Proposition 9.7. *Let M be an idempotent matrix of $\mathcal{M}_{n\times n}(\mathcal{B})$. Then, we have*

$$(M)\wedge(S) \vdash (aM)^+ \approx a^+M.$$

Proof. We shall do an induction on the order n of M. The case $n=1$ is clear. Suppose now that $n\geqslant 2$ and let us suppose that our result is proved at any order $<n$, Let M be an idempotent matrix of order n. By Proposition 9.5, we are in one of the four following cases:

Case 1: $M=0$: the result is obvious.

Case 2: $M=J_n$: the proposition follows from Lemma 7.7.

Case 3: there is an integer $p\in[1, n[$, a permutation matrix P_σ and an idempotent matrix N of order p such that

$$M = P_\sigma^{-1}\mathcal{M}P_\sigma \quad \text{with } \mathcal{M} = \left(\begin{array}{c|c} J_q & L \\ \hline 0 & N \end{array}\right).$$

where we denote $q=n-p$. Therefore, we can write

$$(M)\wedge(S) \vdash\!\!\!- \; (aM)^+ = (P_\sigma^{-1}a\mathcal{M}P_\sigma)^+ = (P_\sigma^{-1}a\mathcal{M}P_\sigma)^*(P_\sigma^{-1}a\mathcal{M}P_\sigma)$$

$$\overset{(M)}{\vdash\!\!\!-} (aM)^+ \approx (I + P_\sigma^{-1}a\mathcal{M}(a\mathcal{M})^*P_\sigma)(P_\sigma^{-1}a\mathcal{M}P_\sigma)$$

$$\vdash\!\!\!- (aM)^+ \approx P_\sigma^{-1}a\mathcal{M}(I+(a\mathcal{M})^+)P_\sigma. \tag{1}$$

This relation shows that we can reduce the problem to prove that

$$(M)\wedge(S) \vdash (a\mathcal{M})^+ \approx a^+\mathcal{M} \tag{2}$$

Indeed, if this deduction was true, since $\mathcal{M}$ is clearly idempotent, we would obtain with (1)

$$(M)\wedge(S) \vdash\!\!\!- \; (aM)^+ \approx P_\sigma^{-1}a\mathcal{M}(I+a^+\mathcal{M})P_\sigma = P_\sigma^{-1}(a\mathcal{M}+aa^+\mathcal{M}^2)P_\sigma$$

$$\vdash\!\!\!- (aM)^+ \approx P_\sigma^{-1}a(1+aa^*)\mathcal{M}P_\sigma$$

$$\overset{(M)}{\vdash\!\!\!-} (aM)^+ \approx P_\sigma^{-1}aa^*\mathcal{M}P_\sigma = a^+P_\sigma^{-1}\mathcal{M}P_\sigma = a^+M.$$

Thus, we may only prove (2). First, let us compute $(a\mathcal{M})^+$. According to Propositions 4.2 and 3.2, we have modulo (M) and (S),

$$(a\mathcal{M})^+ = \left(\begin{array}{c|c} aJ_q & aL \\ \hline 0 & aN \end{array}\right)^+ = \left(\begin{array}{c|c} (aJ_q)^+ & (aJ_q)^*aL(aN)^* \\ \hline 0 & (aN)^+ \end{array}\right).$$

Since $p < n$, we can apply the induction hypothesis to N:

$$(M) \wedge (S) \vdash (aN)^+ \approx a^+ N \tag{3}$$

Note that Lemma 7.7. gives the corresponding result for J_q. We can now look at how to reduce the last block:

$$\begin{aligned}
(M) \wedge (S) \;&\vdash\!\!\!\!-\!\!\!- \; (aJ_q)^* aL(aN)^* \approx (I + (aJ_q)^+) aL(I + (aN)^+) \\
&\vdash\!\!\!\!-\!\!\!-^{(M),(S)} \; (aJ_q)^* aL(aN)^* \approx (I + a^+ J_q) aL(I + a^+ N) \\
&\vdash\!\!\!\!-\!\!\!- \; (aJ_q)^* aL(aN)^* \\
&\qquad \approx aL + a^+ aJ_q L + aa^+ LN + a^+ aa^+ J_q LN \\
&\vdash\!\!\!\!-\!\!\!-^{(M),(S)} \; (aJ_q)^* aL(aN)^* \\
&\qquad \approx a[L + a^+ J_q L + a^+ LN + a^+ a^+ J_q LN].
\end{aligned} \tag{4}$$

Observe now that the relation

$$J_q L + LN = L \tag{5}$$

follows easily from the idempotency of $\mathcal{M}$. This relation, together with Lemma 9.6, shows that

$$\begin{aligned}
(M) \wedge (S) \;&\vdash\!\!\!\!-\!\!\!- \; a^+ J_q L + a^+ a^+ J_q LN \approx a^+ J_q L + aa^+ J_q LN \\
&\vdash\!\!\!\!-\!\!\!-^{(M)} \; a^+ J_q L + a^+ a^+ J_q LN \approx (a + aa^+) J_q L + aa^+ J_q LN \\
&\vdash\!\!\!\!-\!\!\!- \; a^+ J_q L + a^+ a^+ J_q LN \approx aJ_q L + aa^+ J_q L = (a + aa^+) J_q L \\
&\vdash\!\!\!\!-\!\!\!-^{(M)} \; a^+ J_q L + a^+ a^+ J_q LN \approx a^+ J_q L.
\end{aligned} \tag{6}$$

But, it follows now from (4), (5) and (6) that

$$\begin{aligned}
(M) \wedge (S) \;&\vdash\!\!\!\!-\!\!\!- \; (aJ_q)^* aL(aN)^* \approx a(L + a^+ (J_q L + LN)) \\
&\vdash\!\!\!\!-\!\!\!- \; (aJ_q)^* aL(aN)^* \approx a(L + a^+ L) = (a + aa^+) L \\
&\vdash\!\!\!\!-\!\!\!-^{(M)} \; (aJ_q)^* aL(aN)^* \approx a^+ L.
\end{aligned}$$

Thus, these different results give us

$$(M) \wedge (S) \vdash (a\mathcal{M})^+ \approx \left(\begin{array}{c|c} a^+ J_q & a^+ L \\ \hline 0 & a^+ N \end{array}\right) = a^+ \mathcal{M}.$$

Therefore this ends the proof of the proposition in this case.

Case 4: There exists an integer $p \in [1, n[$, a permutation matrix P_σ and an idempotent matrix N of order p such that

$$M = P_\sigma^{-1} \mathcal{M} P_\sigma \quad \text{with } \mathcal{M} = \left(\begin{array}{c|c} 0 & L \\ \hline 0 & N \end{array}\right).$$

Using the same argument as above, we can reduce the problem to proving

$$(M) \wedge (S) \vdash (a\mathcal{M})^+ \approx a^+ \mathcal{M}.$$

With Propositions 4.2 and 3.2, we can now compute $(a\mathcal{M})^+$ modulo (M) and (S),

$$(a\mathcal{M})^+ = \left(\begin{array}{c|c} 0 & aL \\ \hline 0 & aN \end{array}\right)^+ = \left(\begin{array}{c|c} 0 & aL(aN)^* \\ \hline 0 & (aN)^+ \end{array}\right).$$

The induction hypothesis applied to N gives us

$$(M) \wedge (S) \vdash (aN)^+ \approx a^+ N. \tag{7}$$

Since $\mathcal{M}$ is clearly idempotent, we obtain $LN = L$. It follows now from (7) that

$$(M) \wedge (S) \vdash\!\!\!\!- \; aL(aN)^* \approx aL(I + (aN)^+) \approx aL + aLa^+ N = (a + aa^+)L$$

$$\overset{(M)}{\vdash\!\!\!\!-} \; aL(aN)^* \approx a^+ L. \tag{8}$$

The two deductions (7) and (8) show that

$$(M) \wedge (S) \vdash (a\mathcal{M})^+ \approx \left(\begin{array}{c|c} 0 & a^+ L \\ \hline 0 & a^+ N \end{array}\right) = a^+ \mathcal{M}.$$

Hence it follows that the desired result is true in this case. Thus this ends our induction and our proof. □

Corollary 9.8. *Let M be an idempotent matrix of $\mathcal{M}_{n\times n}(\mathcal{B})$. Then, we have*

$$(M) \wedge (S) \vdash (aM)^* M \approx M(aM)^* \approx a^* M.$$

Proof. By symmetry, we can restrict ourselves to showing that

$$(M) \wedge (S) \vdash (aM)^* M \approx a^* M.$$

Then it follows from Proposition 9.7 that we have

$$\begin{aligned} (M) \wedge (S) &\vdash (aM)^* M \approx (I + (aM)^+) M \\ &\vdash (aM)^* M \approx M + a^+ M^2 = (1 + a^+) M \\ &\vdash (aM)^* M \approx a^* M. \end{aligned}$$

Hence this ends the proof of our corollary. □

Note. The identities given in Propositions 9.7 and 9.8 are clearly equivalent.

9.4. The identity $\mathcal{M}(G, g)$ for groups

We shall now prove that the deduction $\mathcal{M}(G, g)$ holds for every finite group G and for every $g \in G$. First, let us introduce the following notation.

Definition 9.3. Let μ be a $\mathscr{B}$-linear representation of order m of a finite group G and let $M \in \mathscr{M}_{G\times G}(\mathscr{C}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle)$. Then, we will denote by $M\otimes\mu$ the square matrix of order $G\times[1,n]$ with entries in $\mathscr{C}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle$ which is defined by

$$M\otimes\mu=[M_{g,h}\mu(g^{-1}h)]_{(g,h)\in G\times G}.$$

Proposition 9.9. *Let G be a finite group, let $X=\{x_{g,h},(g,h)\in G\times G\}$ be an alphabet indexed by $G\times G$ and let μ be a $\mathscr{B}$-linear representation of G. Let us now denote by $\mathscr{X}$ the* generic *matrix of order G defined by*

$$\mathscr{X}=(x_{g,h})_{(g,h)\in G\times G}.$$

Then, the following matrix identity holds:

$$(M)\wedge(S)\vdash(\mathscr{X}\otimes\mu)^{+}\approx\mathscr{X}^{+}\otimes\mu.$$

Proof. We shall prove by induction on $|H|$ that we have for every $H\subset G$,

$$(M)\wedge(S)\ \vdash\ (\mathscr{X}_H\otimes\mu)^{+}\approx\mathscr{X}_H^{+}\otimes\mu\quad(\mathscr{H}(H))$$

where $\mathscr{X}_H=(x_{g,h})_{(g,h)\in H\times H}$. When $|H|=1$, $\mathscr{H}(H)$ is given by

$$(M)\wedge(S)\ \vdash\ (a\mu(1_G))^{+}\approx a^{+}\mu(1_G)$$

and hence follows from Proposition 9.7 since $\mu(1_G)$ is idempotent. Let us suppose now that $\mathscr{H}(H)$ is proved for every $|H|<p$ with $p\geqslant 2$. Then let $H\subset G$ with $|H|=p$, let $k\in H$ and let $K=H-\{k\}$. Therefore we can write

$$\mathscr{X}_H=\begin{matrix}k\\K\end{matrix}\left(\begin{array}{c|c}x_{k,k} & B_{k,K}\\ \hline C_{K,k} & \mathscr{X}_K\end{array}\right)\begin{matrix}k & K\end{matrix}\quad\text{and}\quad(\mathscr{X}_H\otimes\mu)^{+}=\begin{matrix}k\\K\end{matrix}\left(\begin{array}{c|c}\mathscr{A} & \mathscr{B}\\ \hline \mathscr{C} & \mathscr{D}\end{array}\right)\begin{matrix}k & K\end{matrix}.\tag{1}$$

Let us now study each block that appears in (1). First, we have

$$\mathscr{A}=\left(x_{k,k}\mu(1)+\sum_{p,q\in K}x_{k,p}\mu(k^{-1}p)[(\mathscr{X}_K\otimes\mu)^{*}]_{(p,q)}x_{q,k}\mu(q^{-1}k)\right)^{+}.$$

But, according to the induction hypothesis applied to K, we have

$$(M)\wedge(S)\ \vdash\ (\mathscr{X}_K\otimes\mu)^{*}\approx I+\mathscr{X}_K^{+}\otimes\mu.$$

It follows immediately that we have modulo (M) and (S),

$$\mathscr{A}\approx\left((x_{k,k}+\sum_{h\in K}x_{k,h}x_{h,k})\mu(1)+\sum_{p,q\in K}x_{k,p}\mu(k^{-1}p)[\mathscr{X}_K^{+}\otimes\mu]_{(p,q)}x_{q,k}\mu(q^{-1}k)\right)^{+}.$$

Using both the fact that μ is a morphism and Proposition 9.7 with $\mu(1)$, it follows

easily from this last identity that

$$(M)\wedge(S) \longmapsto \mathscr{A} \approx \left((x_{k,k} + \sum_{h\in K} x_{k,h}x_{h,k} + \sum_{p,q\in K} x_{k,p}[\mathscr{X}_K^+]_{(p,q)}x_{q,k})\mu(1)\right)^+$$

$$\vdash^{(M),(S)} \mathscr{A} \approx \left(x_{k,k} + \sum_{h\in K} x_{k,h}x_{h,k} + \sum_{p,q\in K} x_{k,p}[\mathscr{X}_K^+]_{(p,q)}x_{q,k}\right)^+ \mu(1)$$

$$\vdash^{(M)} \mathscr{A} \approx \left(x_{k,k} + \sum_{p,q\in K} x_{k,p}[\mathscr{X}_K^*]_{(p,q)}x_{q,k}\right)^+ \mu(1)$$

$$\vdash \mathscr{A} \approx (x_{k,k} + B_{k,K}\mathscr{X}_K^* C_{K,k})^+\mu(1). \tag{2}$$

This will end our study of $\mathscr{A}$. Let us consider now $\mathscr{C}$. According to Propositions 3.2 and 4.2, we can write modulo (M) and (S),

$$\mathscr{C} = (I + (\mathscr{X}_K \otimes \mu)^+)C_{K,k}(I + \mathscr{A}).$$

The induction hypothesis applied to K and relation (2) show that

$$(M)\wedge(S) \vdash \mathscr{C} \approx (I + \mathscr{X}_K^+ \otimes \mu)C_{K,k}(x_{k,k} + B_{k,K}\mathscr{X}_K^* C_{K,k})^+\mu(1) \tag{3}$$

Then we can compute easily that

$$\begin{aligned}(I + \mathscr{X}_K^+ \otimes \mu)C_{K,k} &= \left[x_{h,k}\mu(h^{-1}k) + \sum_{l\in K} (\mathscr{X}_K^+)_{h,l}\mu(h^{-1}l)x_{l,k}\mu(l^{-1}k)\right]_{h\in K} \\ &= \left[\left(x_{h,k} + \sum_{l\in K} (\mathscr{X}_K^+)_{h,l}x_{l,k}\right)\mu(h^{-1}k)\right]_{h\in K} \\ &= [(C_{K,k} + \mathscr{X}_K^+ C_{K,k})_h\mu(h^{-1}k)]_{h\in K} \\ &= [((I + \mathscr{X}_K^+)C_{K,k})_h\mu(h^{-1}k)]_{h\in K}.\end{aligned}$$

This relation together with (3) allows us to write the deduction

$$\begin{aligned}(M)\wedge(S) &\vdash \mathscr{C} \approx [((I + \mathscr{X}_K^+)C_{K,k}(x_{k,k} + B_{k,K}\mathscr{X}_K^* C_{K,k})^+)_h\mu(h^{-1}k)]_{h\in K} \\ &\vdash^{(M)} \mathscr{C} \approx [(\mathscr{X}_K^* C_{K,k}(x_{k,k} + B_{k,K}\mathscr{X}_K^* C_{K,k})^+)_h\mu(h^{-1}k)]_{h\in K}.\end{aligned} \tag{4}$$

This will end our study of $\mathscr{C}$. Let us consider now the block $\mathscr{D}$. According to Proposition 4.2, we can write modulo (M) and (S),

$$\mathscr{D} = \left((\mathscr{X}_K)_{h,l}\mu(h^{-1}l) + x_{h,k}\mu(h^{-1}k)(I + (x_{k,k}\mu(1))^+)x_{k,l}\mu(k^{-1}l)\right)^+_{(h,l)\in K^2}.$$

Using Proposition 9.7, we can write modulo (M) and (S),

$$\begin{aligned}\mathscr{D} &\approx [(\mathscr{X}_K)_{h,l}\mu(h^{-1}l) + x_{h,k}\mu(h^{-1}k)(I + x_{k,k}^+\mu(1))x_{k,l}\mu(k^{-1}l)]^+_{(h,l)\in K^2} \\ &\approx [(\mathscr{X}_K)_{h,l}\mu(h^{-1}l) + x_{h,k}\mu(h^{-1}k)(1 + x_{k,k}^+)x_{k,l}\mu(k^{-1}l)]^+_{(h,l)\in K^2}.\end{aligned}$$

Then it follows obviously that

$$\begin{aligned}(M)\wedge(S) &\vdash \mathscr{D} \approx [((\mathscr{X}_K)_{h,l} + x_{h,k}x_{k,k}^* x_{k,l})\mu(h^{-1}l)]^+_{(h,l)\in K^2} \\ &\vdash \mathscr{D} \approx [(\mathscr{X}_K + C_{K,k}x_{k,k}^* B_{k,K})\otimes\mu]^+.\end{aligned}$$

Let us consider now the substitution σ defined by

$$\forall h, l \in K, \quad \sigma(x_{h,l}) = x_{h,l} + x_{h,k} x_{k,k}^* x_{k,l}.$$

Then, if we apply σ to the deduction obtained from the induction hypothesis applied to $\mathcal{X}_K$, we obtain the following identity:

$$(M) \wedge (S) \vdash \mathcal{D} \approx [\mathcal{X}_K + C_{K,k} x_{k,k}^* B_{k,K}]^+ \otimes \mu. \tag{5}$$

This ends our study of $\mathcal{D}$. Let us finally come to $\mathcal{B}$. According to Proposition 4.2, we have modulo (M) and (S),

$$\mathcal{B} = (I + (x_{k,k}\mu(1))^+) B_{k,K} (I + \mathcal{D}).$$

But, we have by (5) modulo (M) and (S),

$$\begin{aligned} B_{k,K}(I+\mathcal{D}) \approx \Big(& x_{k,h}\mu(k^{-1}h) \\ & + \sum_{l \in K} x_{k,l}\mu(k^{-1}l)[(\mathcal{X}_K + C_{K,k}x_{k,k}^* B_{k,K})^+]_{(l,h)}\mu(l^{-1}h) \Big)_{h \in K} \\ \approx & \Big((x_{k,h} + \sum_{l \in K} x_{k,l}[(\mathcal{X}_K + C_{K,k}x_{k,k}^* B_{k,K})^+]_{(l,h)}\mu(l^{-1}h) \Big)_{h \in K} \\ \approx & ((B_{K,k}(I + (\mathcal{X}_K + C_{K,k}x_{k,k}^* B_{k,K})^+)_h \mu(l^{-1}h))_{h \in K}. \end{aligned}$$

It follows easily from Proposition 9.7 and from previous relations that

$$\begin{aligned} (M) \wedge (S) \vdash & \quad \mathcal{B} \approx (I + x_{k,k}^+ \mu(1)) \\ & \qquad \times [(B_{K,k}(\mathcal{X}_K + C_{K,k}x_{k,k}^* B_{k,K})^*)_h \mu(l^{-1}h)]_{h \in K} \\ \vdash & \quad \mathcal{B} \approx (1 + x_{k,k}^+)[(B_{K,k}(\mathcal{X}_K + C_{K,k}x_{k,k}^* B_{k,K})^*)_h \mu(l^{-1}h)]_{h \in K} \\ \overset{(M)}{\vdash} & \quad \mathcal{B} \approx x_{k,k}^* [(B_{K,k}(\mathcal{X}_K + C_{K,k}x_{k,k}^* B_{k,K})^*)_h \mu(l^{-1}h)]_{h \in K}. \end{aligned} \tag{6}$$

It is now straightforward to see that the identities (2), (4), (5) and (6) mean exactly that $\mathcal{H}(H)$ is satisfied. The proposition now follows immediately. □

The previous result now gives us easily the following proposition:

Proposition 9.10. *Let μ be a $\mathcal{B}$-linear representation of order n of a group G, let $\bar{\mu}$ be its associated $\mathcal{B}$-$*$-morphism from $\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A_G\rangle$ into $\mathcal{M}_{n\times n}(\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A_G\rangle)$ and let $(E_g)_{g\in G}$ be the universal expressions associated with G. Then, for every $g \in G$, we have*

$$(M) \wedge (S) \vdash \bar{\mu}(E_g) \approx E_g \mu(g). \quad (\mathcal{M}(G, g))$$

Proof. It follows immediately from Proposition 9.9 that we have

$$(M) \wedge (S) \vdash (C(G) \otimes \mu)^+ \approx C(G)^+ \otimes \mu.$$

But, we clearly have $C(G)\otimes\mu = \bar{\mu}(C(G))$. Hence, this shows that

$$(M)\wedge(S) \vdash [\bar{\mu}(C(G))]^+ \approx C(G)^+\otimes\mu \vdash \bar{\mu}(C(G)^+) \approx C(G)^+\otimes\mu$$

since $\bar{\mu}$ is a $*$-morphism. Writing this identity on each entry, we now obtain all the identities $\mathcal{M}(G, g)$. □

9.5. The identity $\mathcal{M}(S, s)$ for monogenic semigroups

We shall now prove $\mathcal{M}(S, s)$ in the case of finite monogenic semigroups.

Proposition 9.11. *Let μ be a $\mathcal{B}$-linear representation of order n of a monogenic semigroup $S \simeq \mathbb{N}^*_{n,p}$, let $\bar{\mu}$ denote its associated $\mathcal{B}$-$*$-morphism from $\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A_S\rangle$ into $\mathcal{M}_{n\times n}(\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A_S\rangle)$ and let $(E_s)_{s\in S}$ be the universal expressions associated with S. Then, for every s in S, we have*

$$(M)\wedge(S) \vdash \bar{\mu}(E_s) \approx E_s\mu(s). \quad (\mathcal{M}(S, s))$$

Proof. We will use in the sequel the identification $S \simeq [1, n+p-1]$ and we will also denote by $S(k)$ the subsemigroup $[k, n+p-1]$ of S. According to Definition 9.1, the proof of Proposition 7.22 shows us that the family $(E_s)_{s\in S}$ is obtained by an inductive process which builds a sequence $(\mathcal{E}_k)_{k=n,1}$ of rational expression families: it starts with the family $\mathcal{E}_n$ of the universal rational expressions associated with the group $S(n) \simeq \mathbb{Z}/p\mathbb{Z}$ and it ends with the family $\mathcal{E}_1 = (E_s)_{s\in S}$. To describe it, let us now define the relation between $\mathcal{E}_k$ and $\mathcal{E}_{k-1}$.

Let us suppose that the family $\mathcal{E}_k = (E^k_i)_{i\in[k,n+p-1]}$ of $\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A_{S(k)}\rangle$ is constructed and let us denote

$$A_j = \sum_{(k-1)i=j}^{1\leqslant i\leqslant n-1} a^i_{k-1} + \left[\sum_{(k-1)i=j}^{n\leqslant i\leqslant n+p-1} a^i_{k-1}\right](a^p_{k-1})^*, \tag{1}$$

for every j in $[1, n+p-1]$. Let us also introduce the substitution σ from $A_{S(k)}$ into $A_{S(k-1)}$ defined by

$$\forall a_m \in A_{S(k)}, \quad \sigma(a_m) = a_m + \sum_{i+j=m}^{i\geqslant k} a_i A_j. \tag{2}$$

Then every element of the family $\mathcal{E}_{k-1}$ is obtained as follows:

$$\forall m \geqslant k-1, \quad E^{(k-1)}_m = \sigma(E^{(k)}_m) + A_m + \sum_{i+j=m}^{i\geqslant k} A_j\sigma(E^{(k)}_i). \tag{3}$$

The reader should refer to the proof of Proposition 7.22 in order to see that the method we used there, really satisfies modulo (M) and (S) to our description. Let us now prove our proposition. Thus, let μ be a $\mathcal{B}$-linear representation of S. We shall show by descending induction on k that

$$(M)\wedge(S) \vdash \bar{\mu}(E^{(k)}_i) \approx E^{(k)}_i\mu(i), \tag{*}$$

for every $i \in [k, n+p-1]$. Note that in this identity, μ can be considered as a representation of the semigroup $S(k)$. First, the identities $(*)$ are true for $k=n$ as follows immediately from Proposition 9.10 applied to $S(n) \simeq \mathbb{Z}/p\mathbb{Z}$. Let us suppose now that $(*)$ is proved at order k. Then let $m \geqslant k-1$. By (3), we have

$$\bar{\mu}(E_m^{(k-1)}) = \bar{\mu}(\sigma(E_m^{(k)})) + \bar{\mu}(A_m) + \sum_{\substack{i+j=m \\ i \geqslant k}} \bar{\mu}(A_j)\bar{\mu}(\sigma(E_i^{(k)})). \tag{4}$$

It follows from Proposition 9.7 applied to the idempotent matrix $\mu((k-1)p) = \mu(p)$ and from (1) that we have for every $j \geqslant k-1$

$$(M) \wedge (S) \vdash \bar{\mu}(A_j) \approx A_j \mu(j). \tag{5}$$

But, we check easily with definition (2) that

$$\bar{\mu}(\sigma(a_i)) = \sigma(a_i)\mu(i), \tag{6}$$

for every $i \geqslant k$. Let denote by $\bar{\sigma}$ the $\mathcal{B}$-$*$-endomorphism of $\mathcal{M}_{n\times n}(\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A_{S(k)}\rangle)$ which acts like σ on each entry. Hence, it follows from the universal property of $\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A_{S(k)}\rangle$ that (6) means exactly that the following diagram commutes:

$$\begin{array}{ccc} \mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A_{S(k)}\rangle & \xrightarrow{\ \sigma\ } & \mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A_{S(k-1)}\rangle \\ \downarrow{\scriptstyle \bar{\mu}} & & \downarrow{\scriptstyle \bar{\mu}} \\ \mathcal{M}_{n\times n}(\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A_{S(k)}\rangle) & \xrightarrow{\ \bar{\sigma}\ } & \mathcal{M}_{n\times n}(\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A_{S(k-1)}\rangle) \end{array}$$

The induction hypothesis at order k with $\bar{\sigma}$ applied to $(*)$ gives us

$$(M) \wedge (S) \vdash \bar{\sigma}(\bar{\mu}(E_i^{(k)})) \approx \bar{\sigma}(E_i^{(k)}\mu(i))$$

For every $i \geqslant k$. Therefore, since the previous diagram is commutative, we obtain by definition of $\bar{\sigma}$,

$$(M) \wedge (S) \vdash \bar{\mu}(\sigma(E_i^{(k)})) \approx \sigma(E_i^{(k)})\mu(i). \tag{7}$$

According to relations (5) and (7), it follows immediately from (4) that

$$(M) \wedge (S) \vdash \bar{\mu}(E_m^{(k-1)}) \approx E_m^{(k-1)}\mu(m).$$

Hence, since this is true for any $m \geqslant k-1$, we have proved $(*)$ at the order $k-1$. Therefore, this ends our induction and consequently our proof. □

9.6. The identity $\mathcal{M}(S, s)$ for simple semigroups

The next step of our study is to prove $\mathcal{M}(S, s)$ for simple semigroups.

Proposition 9.12. *Let μ be a $\mathcal{B}$-linear representation of order n of a finite left (resp. right) simple semigroup, let $\bar{\mu}$ be its associated $\mathcal{B}$-$*$-morphism from $\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A_S\rangle$ into $\mathcal{M}_{n\times n}(\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A_S\rangle)$ and let $(E_s)_{s\in S}$ be the universal rational expressions associated*

with S. Then, for every s in S, we have

$$(M) \wedge (S) \vdash \bar{\mu}(E_s) \approx E_s \mu(s) \quad (\mathcal{M}(S, s)).$$

Proof. We can clearly consider only the left simple case. We will also take here the notations of Proposition 7.23. Thus S is isomorphic to the Rees semigroup $M(n, G, P)$ of support $[1, n] \times G$, where G is a finite group and $P = (p_i)_{i=1,n}$ is a subset of G. According to Definition 9.1, the proof of Proposition 7.23 shows that the universal expressions $(E_{(i,l)})_{(i,l) \in [1,n] \times G}$ associated with S are built with the universal expressions associated with the subsemigroup $U = [1, n-1] \times G$ of S by the following process.

At first, let us introduce the subsemigroup $V = \{n\} \times G$ of S which is in fact isomorphic to a group and let $(V_{(n,g)})_{(n,g) \in V}$ be the universal expressions on the alphabet A_V associated with V. Let us also consider the substitution σ from A_U into A_S defined by

$$\forall (i, g) \in U, \quad \sigma(a_{(i,g)}) = a_{(i,g)} + \sum_{\substack{1 \leqslant j \leqslant n-1 \\ (j,h).(n,l) = (i,g)}} a_{(j,h)} V_{(n,l)} \tag{1}$$

Finally, let $(U_{(i,l)})_{(i,l) \in U}$ be the universal expressions on the alphabet A_U associated with the subsemigroup U of S. Then, for every $i \leqslant n-1$ and for every g in G, we have

$$E_{(i,g)} = \sigma(U_{(i,g)}) \quad \text{and} \quad E_{(n,g)} = V_{(n,g)} + \sum_{\substack{1 \leqslant j \leqslant n-1 \\ (n,h).(i,l) = (n,g)}} V_{(n,h)} \sigma(U_{(i,l)}) \tag{2}$$

The reader can refer to the proof of Proposition 7.23 in order to check that the above definitions are true, modulo (M) and (S).

We can now prove $\mathcal{M}(S, s)$ by induction on n. If $n = 1$, S is a group and our result follows from Proposition 9.10. If $n \geqslant 2$, let us suppose that $\mathcal{M}(S, s)$ is proved at order $n-1$. Then let μ be a $\mathcal{B}$-linear representation of S and let us denote by $\bar{\mu}$ the associated $\mathcal{B}$-$*$-morphism from $\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A_S \rangle$ in $\mathcal{M}_{n \times n}(\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A_S \rangle)$. Therefore, by the induction hypothesis applied to U and by Proposition 9.7 applied to V, we easily obtain, arguing as in the proof of Proposition 9.11 but using (1) and (2) here, the desired identity:

$$(M) \wedge (S) \vdash \bar{\mu}(E_{(i,g)}) \approx E_{(i,g)} \mu((i, g))$$

for every $(i, g) \in [1, n] \times G$. Hence this ends our proof. □

9.7. The identity $\mathcal{M}(S, s)$

We can now prove $\mathcal{M}(S, s)$ without any restriction on the structure of S.

Theorem 9.13. *Let μ be a $\mathcal{B}$-linear representation of order n of a semigroup S, let $\bar{\mu}$ be its associated $\mathcal{B}$-$*$-morphism from $\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A_S \rangle$ into $\mathcal{M}_{n \times n}(\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A_S \rangle)$ and let $(E_s)_{s \in S}$ be the universal expressions associated with S. Therefore, for every s in S, we have*

$$(M) \wedge (S) \vdash \bar{\mu}(E_s) \approx E_s \mu(s). \quad (\mathcal{M}(S, s))$$

Proof. As in the proof of Theorem 7.24, we shall use here an induction on $|S|$. First, if $|S|=1$, our theorem follows clearly from Proposition 9.7. Now let $n \geqslant 2$ and let us suppose that our result is proved for $|S|<n$. Then, let S be a semigroup with $|s|=n$. If S is left simple or monogenic, our theorem follows from Proposition 9.11 or 9.12, respectively. If this is not the case, we can consider the left maximal ideal I of S that was chosen in the proof of Theorem 7.24. As in this proof, let us also denote here by $U \not\subset S$ the semigroup generated by $S-I$. Then the proof of Theorem 7.24 shows that the universal expressions $(E_s)_{s\in S}$ associated with S are constructed as follows.

First, let $(V_u)_{u\in U}$ and $(J_i)_{i\in I}$ be the universal rational expressions on the alphabets A_U and A_I associated with U and V, respectively. Then, let σ and φ denote respectively the two substitutions from A_U into A_U and from A_I into A_S defined by

$$\forall u \in U, \quad \varphi(a_u)=\begin{cases} a_u & \text{if } u \notin I \\ 0 & \text{otherwise} \end{cases}$$

and

$$\forall i \in I, \quad \sigma(a_i)=a_i+\sum_{j\in I, v\in U}^{jv=i} a_j\varphi(V_v).$$

The proof of Proposition 7.24 now shows that the universal expressions $(E_s)_{s\in S}$ associated with S are obtained modulo (M) and (S) by

$$\forall i \in I \cap U, \quad E_i=\sigma(J_i)+\varphi(V_i)+\sum_{vj=i}\varphi(V_v)\sigma(J_j),$$

$$\forall u \in U-I, \quad E_u=\varphi(V_i)+\sum_{vj=u}\varphi(V_v)\sigma(J_j),$$

$$\forall i \in I-U, \quad E_i=\sigma(J_i)+\sum_{vj=i}\varphi(V_v)\sigma(J_j).$$

Using, with φ and σ, the same method as in the proof of Proposition 9.11, it now follows easily from the induction hypothesis applied to I and to U that

$$(M)\wedge(S) \vdash \bar{\mu}(E_s)\approx E_s\mu(s)$$

for every s in S and for every $\mathcal{B}$-linear representation μ of S. Therefore this ends our induction and our proof. □

10. Consequences of the identity $\mathcal{M}(S, s)$

10.1. Action of a semigroup on a free $\mathcal{B}$-module

Let M be a finitely generated free $\mathcal{B}$-module and let E be its basis. Hence, every element m of M can be written in a unique way as follows:

$$m=\sum_{e\in E}\Delta_{m,e}e \quad \text{with } \Delta_{m,e}\in\mathcal{B} \text{ for every } e \text{ in } E.^{8}$$

[8] $\Delta_{m,e}$ will always be used in this sense in the sequel. Therefore, up to the isomorphism $\mathcal{B}\langle E\rangle \simeq \mathcal{P}(E)$, we have $\Delta_{m,e}=1$ iff $e\in m$.

We will denote $M = \mathcal{B}\langle E\rangle$. Let S be a semigroup which acts on the right on M. Then, the action of S on M is completely given by its action on E. Thus, we can write for every s of S and for every e in E,

$$e.s = \sum_{f \in S} \Delta_{e.s,f} f.$$

This leads us now to the following definition.

Definition 10.1. Let $M = \mathcal{B}\langle E\rangle$ be a free $\mathcal{B}$-module with a finite basis E and let S be a finite semigroup that acts on the right on M. Therefore we shall call *reduced action matrices of S on M* the matrices $(R_s)_{s \in S}$ defined by

$$\forall s \in S, \quad R_s = [\Delta_{e.s,f}]_{(e,f) \in E \times E} \in \mathcal{M}_{E \times E}(\mathcal{B}).$$

Remark. It is easy to see that $R_s R_t = R_{st}$ for every s, t in S. Therefore, the mapping ρ which maps every s of S on R_s is a $\mathcal{B}$-linear representation of order $|E|$ of S. Conversely, if μ is a given $\mathcal{B}$-linear representation of order n of S, it is easy to build an action of S on $\mathcal{B}\langle[1, n]\rangle$ such that the matrices $(\mu(s))_{s \in S}$ are the associated reduced action matrices of S on $\mathcal{B}\langle[1, n]\rangle$.

Theorem 10.1. *Let S be a finite semigroup that acts on the right on a free $\mathcal{B}$-module $M = \mathcal{B}\langle E\rangle$ of finite basis E, let $(E_s)_{s \in S}$ be the universal expressions associated with S and let $(R_s)_{s \in S}$ be the reduced action matrices of S on M. Then, we have*

$$(P(H))_{H \in \mathcal{A}(S)} \wedge (M) \wedge (S) \xrightarrow{P(S)} \left(\sum_{s \in S} a_s R_s\right)^+ \approx \sum_{s \in S} E_s R_s.$$

Proof. Let ρ be the $\mathcal{B}$-linear representation of order $|E|$ defined by $\rho(s) = R_s$ for every s in $\mathcal{S}$. According to Proposition 8.2, the identity $P(S)$ is given by

$$A_S^+ \approx \sum_{s \in S} E_s, \tag{1}$$

modulo (M), (S) and $(P(H))_{H \in \mathcal{A}(S)}$. Let $\bar{\rho}$ denote the morphism associated with ρ as defined in Section 9.1. Then, applying $\bar{\rho}$ to (1), we obtain

$$(P(H))_{H \in \mathcal{A}(S)} \wedge (M) \wedge (S) \xrightarrow{P(S)} \bar{\rho}(A_S^+) = \left(\sum_{s \in S} a_s \rho(s)\right)^+ \approx \sum_{s \in S} \bar{\rho}(E_s),$$

according to Proposition 3.9 and Theorem 8.4. It now follows from Theorem 9.13 that

$$(P(H))_{H \in \mathcal{A}(S)} \wedge (M) \wedge (S) \xrightarrow{(S)} \left(\sum_{s \in S} a_s \rho(s)\right)^+ \approx \sum_{s \in S} E_s \rho(s).$$

Therefore this ends our proof. □

Note. Observe that we need the identity $P(S)$ for proving Theorem 10.1. This situation is quite different from Theorem 7.24, which also deals with the same problem, but with non-reduced action matrices.

The following corollary will be essential in the proof of the completeness of the system of semigroup identities.

Corollary 10.2. *Let A be a finite alphabet and let $(M_a)_{a\in A}$ be a family of matrices of $\mathcal{M}_{n\times n}(\mathcal{B})$. For every $w = a_1 \dots a_n \in A^*$, let us define M_w by*

$$M_1 = I_n, \text{ if } n = 0 \quad \text{and} \quad M_w = M_{a_1} \dots M_{a_n}, \text{ if } n \geqslant 1.$$

Let S denote the finite semigroup generated by the family $(M_a)_{a\in A}$. Then there exist a finite part W of A^* and $\mathcal{B}$-rational expressions $(F_w)_{w\in W}$ such that

$$(P(H))_{H\in\mathcal{A}(S)} \wedge (M) \wedge (S) \vdash^{P(S)} \left(\sum_{a\in A} aM_a\right)^* \approx \sum_{w\in W} F_w M_w.$$

Proof. There exists clearly a finite part $V \subset A^*$ which contains A, such that we can write $S = \{M_v, v \in V\}$. Of course, we can also suppose that $M_u \neq M_v$ for every $u \neq v$ in V. Therefore we can identify V and S. Let us now consider the action of S on $\mathcal{B}\langle[1, n]\rangle$ defined by

$$\forall v \in V, \forall P \in \mathcal{B}\langle[1, n]\rangle, \quad P.M_v = \sum_{i=1}^{n} \Delta_{P,i}\left(\sum_{j=1}^{n} (M_v)_{i,j} j\right).$$

The matrices $(M_v)_{v\in V}$ are clearly the reduced action matrices of S on $\mathcal{B}\langle[1, n]\rangle$ for this action. Hence it follows immediately from Theorem 10.1 that

$$(P(H))_{H\in\mathcal{A}(S)} \wedge (M) \wedge (S) \vdash^{P(S)} \left(\sum_{v\in V} a_v M_v\right)^+ \approx \sum_{v\in V} E_v M_v,$$

where $(E_v)_{v\in V}$ are the universal $\mathcal{B}$-rational expressions associated with S. Let us also denote by σ the substitution from A_v into A defined by

$$\forall v \in V, \quad \sigma(a_v) = \begin{cases} 0 & \text{if } v \notin A, \\ a & \text{if } v = a \in A. \end{cases}$$

Applying σ to the previous identity, we obtain

$$(P(H))_{H\in\mathcal{A}(S)} \wedge (M) \wedge (S) \vdash^{P(S)} \left(\sum_{a\in A} aM_a\right)^+ \approx \sum_{v\in V} F_v M_v,$$

where $F_v = \sigma(E_v)$ for every $v \in V$. It follows that we have

$$(P(H))_{H\in\mathcal{A}(S)} \wedge (M) \wedge (S) \vdash^{P(S)} \left(\sum_{a\in A} aM_a\right)^* \approx I + \sum_{v\in V} F_v M_v.$$

To conclude, it suffices to define $W = V$ if $I \in S$ or $W = V \cup \{1\}$ if $I \notin S$ and consequently to modify the family $(F_v)_{v\in V}$. □

Notes. (1) The above proof shows that, for every family of matrices of order n, there exist a semigroup S and an action of S on $\mathcal{B}\langle[1, n]\rangle$, such that this family is only composed of reduced actions matrices for this action.

(2) If every matrix M_a has at most one 1 in each row, it is easy to show, using a completion process, that we can suppose that they have modulo (M) and (S) exactly one 1 in each row. In this case, we can use in the previous proof Theorem 7.24 instead of Theorem 10.1, since the matrices $(M_a)_{a\in A}$ are now a subfamily of the action matrices of S on $[1, n]$ for a naturally constructed action. Therefore we can in this case avoid the use of $P(S)$.

10.2. A determination process

We associate with every free $\mathcal{B}$-module $M = \mathcal{B}\langle E\rangle$ of finite basis E, the matrices

$$\delta = [\delta_{e,m}]_{(e,m)\in E\times M} \quad \text{and} \quad \Delta = [\Delta_{m,e}]_{(m,e)\in M\times E}.$$

Remark. An easy computation shows that $\delta\Delta = I_E$.

Lemma 10.3. *Let S be a semigroup that acts on the right on a free $\mathcal{B}$-module M of finite basis E, let $(R_s)_{s\in S}$ be the reduced action matrices of S on M and let $(M_s)_{s\in S}$ be the action matrices of S on M. Then, for every $s\in S$, we have $\delta M_s\Delta = R_s$.*

Proof. Indeed, let $s\in S$ and $(e,f)\in E\times E$. Then we have

$$(\delta M_s\Delta)_{(e,f)} = \sum_{n,m\in M} \delta_{e,m}\delta_{m.s,n}\Delta_{n,f} = \sum_{n\in M} \delta_{e.s,n}\Delta_{n,f}$$

$$= \Delta_{e.s,f} = (R_s)_{(e,f)}.$$

Hence this ends the proof. □

The following result shows how, from the viewpoint of rational identities, a finite automaton and the automaton obtained by the classical determination process are related.

Proposition 10.4. *Let S be a finite semigroup which acts on the right on a free $\mathcal{B}$-module M of finite basis E, let $(R_s)_{s\in S}$ be the reduced action matrices of S on M and let $(M_s)_{s\in S}$ be the action matrices of S on M. Then, we have*

$$P(H))_{H\in\mathcal{A}(S)} \wedge (M) \wedge (S) \xrightarrow{P(S)} \delta\left(\sum_{s\in S} a_sM_s\right)^*\Delta \approx \left(\sum_{s\in S} a_sR_s\right)^*.$$

Proof. Let $(E_s)_{s\in S}$ be the universal rational expressions associated with S. Then, it follows from Theorem 7.24 and from Lemma 10.3 that

$$(P(H))_{H\in\mathcal{A}(S)} \wedge (M) \wedge (S) \vdash \left(\sum_{s\in S} a_sM_s\right)^* \approx I + \sum_{s\in S} E_sM_s$$

$$\vdash \delta\left(\sum_{s\in S} a_sM_s\right)^*\Delta \approx \delta\Delta + \sum_{s\in S} E_s\delta M_s\Delta$$

$$\vdash \delta\left(\sum_{s\in S} a_sM_s\right)^*\Delta \approx I + \sum_{s\in S} E_sR_s.$$

But, it follows also from Theorem 10.1 that

$$(P(H))_{H\in\mathscr{A}(S)} \wedge (M) \wedge (S) \overset{P(S)}{\vdash} \left(\sum_{s\in S} a_s R_s\right)^* \approx I + \sum_{s\in S} E_s R_s.$$

It is now straightforward to conclude with these two last identities. □

Remark. We think that it should be possible to prove the above identity with less axioms. But this problem remains open.

Note. We can also study from our viewpoint, other methods used in automata theory. For instance, it can be easily proved that the classical completion process is (M)-(S) stable.

11. Completeness of semigroup identities

We shall prove in this chapter that the system, composed of the identities (M), (S) and $(P(S))$ for all finite semigroups, is complete. This result was conjectured by Conway (see [7, p. 116]).

11.1. Automaton recognizing a $\mathscr{B}$-rational expression

A *finite automaton* $\mathscr{A}$ of order n on the alphabet A is a triple (I, M, T) where $I \in \mathscr{M}_{1\times n}(\mathscr{B})$ and $T \in \mathscr{M}_{n\times 1}(\mathscr{B})$ are called *initial* and *final state vectors* and where M is called the *transition matrix* of $\mathscr{A}$ and is defined by

$$M = \sum_{a\in A} a.M_a,$$

where $(M_a)_{a\in A}$ is a family of matrices in $\mathscr{M}_{n\times n}(\mathscr{B})$ almost all equal to 0. Then, any rational expression equivalent modulo (M) and (S) to $I.M^*.T$ will said to be a *rational expression recognized* by $\mathscr{A}$ modulo (M) and (S).

The following proposition is just a new formulation of a classical result in terms of $\mathscr{B}$-rational expressions.

Proposition 11.1 Conway ([7, p. 31]). *Let A be an alphabet and let E be in $\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle$. Then, there exists an automaton (I, M, T) such that*

$$(S) \wedge (M) \vdash E \approx I.M^*.T.$$

Proof. Let us denote by $\mathscr{E}$ the set of the $\mathscr{B}$-rational expressions that are recognized modulo (M) and (S) by some finite automaton. First, let us show that $\mathscr{E}$ is a semiring. Now let E and F be two rational expressions recognized modulo (S) and (M) by the automata (I_1, M_1, T_1) and (I_2, M_2, T_2) of order n and m, respectively. Then, $E + F$ is clearly recognized by the automaton (I, M, T) of order $n + m$ defined

by

$$I=(I_1\ I_2),\qquad M=\left(\begin{array}{c|c} M_1 & 0 \\ \hline 0 & M_2 \end{array}\right),\qquad T=\begin{pmatrix} T_1 \\ T_2 \end{pmatrix}.$$

In order to study the product $E.F$, let us now consider the matrices

$$I=(I_1\ 0),\qquad M=\left(\begin{array}{c|c} M_1 & T_1 I_2 \\ \hline 0 & M_2 \end{array}\right),\qquad T=\begin{pmatrix} 0 \\ T_2 \end{pmatrix}$$

Using Definition 3.2, it is easy to see that

$$(M)\wedge(S)\ \vdash\ E.F\approx I.M^*.T. \tag{1}$$

Let us introduce the two matrices

$$Q=\left(\begin{array}{c|c} 0 & T_1 I_2 \\ \hline 0 & 0 \end{array}\right)\quad\text{and}\quad P=\left(\begin{array}{c|c} M_1 & 0 \\ \hline 0 & M_2 \end{array}\right).$$

Then, according to (1), we have

$$(M)\wedge(S)\ \vdash\ E.F\approx I.(Q^*.P)^*.Q^*T.$$

Hence, since Q^* is a boolean matrix, $E.F$ is recognized modulo (M) and (S) by the automaton (I, Q^*P, Q^*T). Finally, it is easy to see that 1 and 0 are in $\mathscr{E}$. Thus $\mathscr{E}$ is a semiring. Let us now prove that $\mathscr{E}$ is a $\mathscr{B}$-$*$-algebra: therefore, let $E\in\mathscr{E}$. Then, E is recognized modulo (M) and (S) by some automaton (I, M, T) of order n. Let us introduce now the matrices of order $n+1$:

$$e=(1\quad 0\quad \ldots\quad 0),\qquad N=\left(\begin{array}{c|c} 0 & I \\ \hline T & M \end{array}\right),\qquad f=\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Using Definition 3.2, we easily obtain

$$(M)\wedge(S)\vdash E^*\approx e.N^*.f. \tag{2}$$

Let us also consider the two matrices

$$P=\left(\begin{array}{c|c} 0 & I \\ \hline T & 0 \end{array}\right)\quad\text{and}\quad Q=\left(\begin{array}{c|c} 0 & 0 \\ \hline 0 & M \end{array}\right).$$

According to (2), we can write

$$(M)\wedge(S)\ \vdash\ E^*\approx e.(P+Q)^*.f\ \overset{(S)}{\vdash}\ E^*\approx e.(P^*Q)^*.P^*f.$$

Since P^* is in $\mathscr{M}_{n+1}(\mathscr{B})$, this means that E^* is recognized modulo (M) and (S) by the automaton (e, P^*Q, P^*f). It follows immediately that $\mathscr{E}$ is a $\mathscr{B}$-$*$-algebra. It is also easy to show that $A\subset\mathscr{E}$. Hence, since the $\mathscr{B}$-$*$-algebra $\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle$ is generated by A, we proved that $\mathscr{E}=\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle$. This ends our proof. □

11.2. Completeness of semigroup identities

We are now able to prove the main result of this paper which shows that the system (M), (S) and $(P(S))$ for all finite semigroups, is complete. It will immediately follow from the following theorem.

Theorem 11.2. *Let A be an alphabet and let (E, F) be a rational identity over A. Then, there exists a finite semigroup S such that*

$$(P(H))_{H\in\mathcal{A}(S)} \wedge P(S) \overset{(M),(S)}{\longmapsto} E \approx F.$$

Proof. Let $E \approx F$ be a rational identity over A. By Proposition 11.1, there exist two automata (I, M, T) and (J, N, V) recognizing respectively E and F modulo (M) and (S). Then let $(M_a)_{a\in A}$ and $(N_a)_{a\in A}$ be the boolean matrices such that

$$M = \sum_{a\in A} aM_a \quad \text{and} \quad N = \sum_{a\in A} aN_a.$$

We can now introduce the family of matrices $(\mathcal{M}_a)_{a\in A}$ that will synchronize the two automata recognizing E and F. For every $a \in A$, we define

$$\mathcal{M}_a = \left(\begin{array}{c|c} M_a & 0 \\ \hline 0 & N_a \end{array}\right).$$

Let S be the semigroup generated by the matrices $(\mathcal{M}_a)_{a\in A}$. By Corollary 10.2, there exists a finite subset W of A^* and rational expressions $(F_w)_{w\in W}$ such that

$$(P(H))_{H\in\mathcal{A}(S)} \wedge (M) \wedge (S)$$
$$\overset{P(S)}{\longmapsto} \left(\sum_{a\in A} a\mathcal{M}_a\right)^* = \left(\begin{array}{c|c} M^* & 0 \\ \hline 0 & N^* \end{array}\right) \approx \sum_{w\in W} F_w \left(\begin{array}{c|c} M_w & 0 \\ \hline 0 & N_w \end{array}\right).$$

It follows immediately that

$$(P(H))_{H\in\mathcal{A}(S)} \wedge P(S) \overset{(M),(S)}{\longmapsto} M^* \approx \sum_{w\in W} F_w M_w,$$

$$(P(H))_{H\in\mathcal{A}(S)} \wedge P(S) \overset{(M),(S)}{\longmapsto} N^* \approx \sum_{w\in W} F_w N_w.$$

Hence, multiplying these relations by the initial and final states vectors associated with the two automata recognizing E and F, we deduce

$$(P(H))_{H\in\mathcal{A}(S)} \wedge P(S) \overset{(M),(S)}{\longmapsto} E \approx \sum_{w\in W} F_w (I.M_w.T),$$

$$(P(H))_{H\in\mathcal{A}(S)} \wedge P(S) \overset{(M),(S)}{\longmapsto} F \approx \sum_{w\in W} F_w (J.N_w.V).$$

But $I.M_w.T = 1$ iff the automaton (I, M, T) recognizes the word w, i.e. iff w belongs to the language $\lambda(E)$. In the same way, $J.N_w.V = 1$ iff w belongs to the language

$\lambda(F)$. Hence, since $\lambda(E)=\lambda(F)$ here, we have for every $w\in W$,

$$IM_wT = JN_wV. \qquad (*)$$

Using the two previous identities, it is now straightforward to obtain

$$(P(H))_{H\in\mathscr{A}(S)} \wedge P(S) \overset{(M),(S)}{\vdash\!\!\!-\!\!\!-} E \approx F.$$

Therefore, this ends the proof of our theorem. □

Notes. (1) The algorithmic process described in this theorem can be applied to any couple (E, F) of $\mathscr{B}$-rational expressions. Thus it gives us a "deductive" method to check if (E, F) is an identity: indeed, it will suffice to see if the above relations $(*)$ are all satisfied.

(2) If the automata associated above with E and F are deterministic, we can avoid the use of $P(S)$, according to a note following Corollary 10.2.

Corollary 11.3. *Let $\mathscr{S}$ be the class of finite semigroups. Then the following system is a complete system of $\mathscr{B}$-rational identities for any alphabet A:*

$$(M), (S), (P(S))_{S\in\mathscr{S}}.$$

Proof. It is an immediate consequence of Theorem 11.2. □

Corollary 11.4. *Let $\mathscr{C}$ be the class of finite* commutative *semigroups. Then, the following system is a complete system of $\mathscr{B}$-rational identities for the one letter alphabet $A=\{a\}$:*

$$(M), (S), (P(S))_{S\in\mathscr{C}}.$$

Proof. Observe that the semigroup S constructed in the proof of Theorem 11.2 is monogenic, hence commutative when $|A|=1$. The corollary now follows easily from Theorem 11.2. □

Note. Corollary 11.3 solves an open question of Conway (cf. [7, p. 116]) and gives us the first well described complete system of $\mathscr{B}$-rational identities.

12. Stability of semigroup identities

12.1. Subsemigroup

Proposition 12.1. *Let S be a finite semigroup, let ρ be a subset of S and let T be a subsemigroup of S. Then, for every t in T, we have*

$$P(S, \rho, t) \overset{(M),(S)}{\vdash\!\!\!-\!\!\!-} P(T, \rho\cap T, t).$$

Proof. Let us denote by A_ρ and $A_{\rho\cap T}$ the two alphabets $A_\rho = \{a_s, s \in \rho\}$ and $A_{\rho\cap T} = \{a_t, t \in \rho \cap T\}$ and by σ the substitution from A_ρ into $A_{\rho\cap T}$ defined by

$$\forall t \in \rho \cap T, \quad \sigma(a_t) = a_t \quad \text{and} \quad \forall s \in \rho - \rho \cap T, \quad \sigma(a_s) = 0.$$

Then we clearly have the following decomposition:

$$\sigma(C(S,\rho)) = \begin{matrix} \\ T \\ S-T \end{matrix} \begin{pmatrix} \overset{T}{C(T,\rho\cap T)} & \overset{S-T}{0} \\ P & Q \end{pmatrix}$$

which shows that we have modulo (M) and (S),

$$\sigma([C(S,\rho)]^+) = (\sigma(C(S,\rho))^+) = \begin{pmatrix} [C(T,\rho\cap T)]^+ & 0 \\ Q^*P[C(T,\rho\cap T)]^* & Q^+ \end{pmatrix}.$$

Now let $t \in \rho \cap T$. It follows from the previous relation that we have

$$\sigma(u_t.[C(S,\rho)]^+.u) = u_t.\sigma([C(T,\rho\cap T)]^+).u = u'_t.[C(T,\rho\cap T)]^+.u',$$

where u'_t and u' are of order T. Hence, it follows that we have modulo (M) and (S), $\sigma(P(S,\rho,t)) = P(T,\rho\cap T,t)$. It is now straightforward to conclude. □

Corollary 12.2. *Let S be a finite semigroup, let ρ be a subset of S and let T be a subsemigroup of S. Then, we have*

$$(P(H))_{H\in\mathcal{A}(S)} \wedge P(S,\rho) \overset{(M),(S)}{\longmapsto} P(T,\rho\cap T).$$

Proof. Since $\mathcal{A}(T) \subset \mathcal{A}(S)$, this corollary follows immediately from Propositions 12.1 and 8.2. □

Corollary 12.3. *Let S be a finite semigroup and let T be a subsemigroup of S. Then, we have*

$$(P(H))_{H\in\mathcal{A}(S)} \wedge P(S) \overset{(M),(S)}{\longmapsto} P(T).$$

Proof. It is an immediate consequence of Corollary 12.2. □

12.2. Quotient

Before studying the relations existing between the identities associated with a semigroup and with its quotients, let us give the following definition.

Definition 12.1. Let $n=(n_1,\ldots,n_r)\in(\mathbb{N}^*)^r$ and let $M\in\mathcal{M}_{r\times r}(\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle)$. Then we will denote by $M\otimes_n J$ the matrix which is defined by

$$M\otimes_n J=\begin{array}{c} \\ n_1 \\ \vdots \\ n_r \end{array}\begin{array}{c} \begin{array}{ccc} n_1 & & n_r \end{array} \\ \left(\begin{array}{c|c|c} M_{1,1}J_{1,1} & \cdots & M_{1,r}J_{1,r} \\ \hline \vdots & & \vdots \\ \hline M_{r,1}J_{r,1} & \cdots & M_{r,r}J_{r,r} \end{array}\right) \end{array}$$

where $J_{i,j}$ denotes the matrix of $\mathcal{M}_{n_i\times n_j}(\mathcal{B})$ all of whose entries are 1.

The following proposition appears as a new generalization of Lemma 7.7

Proposition 12.4. *Let M be a matrix of $\mathcal{M}_{m\times m}(\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle)$ with a* zero constant coefficient. *Then, for every $n\in(\mathbb{N}^*)^r$, we have*

$$(M)\wedge(S)\vdash(M\otimes_n J)^+\approx M^+\otimes_n J.$$

Proof. We can show this result by induction on the order r of the r-tuple n. The case $r=1$ follows from Lemma 7.7. When $r\geqslant 2$, we can compute $(M\otimes_n J)^+$ with the following decomposition:

$$M\otimes J=\left(\begin{array}{c|c} M_{1,1}J_{1,1} & B \\ \hline C & N\otimes_m J \end{array}\right)$$

where N denotes the matrix $M_{i,j\geqslant 2}$ and $m=(n_2,\ldots,n_r)$. Using a similar method as in Proposition 9.7 for instance, it is easy to show that our proposition follows from the induction hypothesis applied to the matrix $N\otimes_m J$ and from Lemma 7.7 applied to $M_{1,1}J_{1,1}$. □

Proposition 12.5. *Let $\equiv$ be a congruence of a finite semigroup S and let π be the projection of S on the quotient semigroup $S/\equiv$. Then, for every subset ρ of S and every s in S, we have*

$$P(S,\rho,s)\xrightarrow{(M),(S)}P(S/\equiv,\pi(\rho),\pi(s)).$$

Proof. Let us denote $\pi(t)=\bar{t}$ for every t in S and σ the substitution from $A_\rho=\{a_r,\ r\in\rho\}$ into $A_{\bar{\rho}}=\{a_{\bar{r}},\ \bar{r}\in\bar{\rho}\}$ defined by $\sigma(a_r)=a_{\bar{r}}$ for every r in ρ. Since we work with $\mathcal{B}$, we immediately have for every s, $t\in S$,

$$\sigma\left(\sum_{su=t}^{u\in\rho}a_u\right)=\sum_{su=t}^{u\in\rho}a_{\bar{u}}=\sum_{\bar{s}\bar{u}=\bar{t}}^{u\in\rho}a_{\bar{u}}. \tag{1}$$

Now let $R=\{s_i,\ i\in[1,r]\}$ be a section of $\equiv$ and let $\mathrm{cl}(s)$ denote the equivalence class of $s\in S$ for $\equiv$. Finally let us introduce the notations

$$n=(|\mathrm{cl}(s_1)|,\ldots,|\mathrm{cl}(s_r)|),$$

$$\forall i,j\in[1,r],\quad J_{i,j}=(1)\in\mathcal{M}_{\mathrm{cl}(s_i)\times\mathrm{cl}(s_j)}(\mathcal{B})$$

$$\forall i,j\in[1,r],\quad s_{i,j}=\sum_{(\bar{s_i})\bar{u}=(\bar{s_j})}a_{\bar{u}},$$

where $\bar{u} \in \bar{\rho}$ in this last relation. It follows now from (1) that we have

$$\sigma[C(S,\rho)] = \begin{array}{c} \\ \mathrm{cl}(s_1) \\ \vdots \\ \mathrm{cl}(s_r) \end{array} \begin{array}{c} \begin{array}{ccc} \mathrm{cl}(s_1) & \cdots & \mathrm{cl}(s_r) \end{array} \\ \begin{pmatrix} s_{1,1}J_{1,1} & \cdots & s_{1,r}J_{1,r} \\ \vdots & & \vdots \\ s_{r,1}J_{r,1} & \cdots & s_{r,r}J_{r,r} \end{pmatrix} \end{array} = C(S/\equiv, \bar{\rho}) \otimes_n J.$$

Hence, we obtain by Proposition 12.4, that

$$(M) \wedge (S) \vdash \sigma[C(S,\rho)^+] = \sigma[C(S,\rho)]^+$$
$$= (C(S/\equiv, \bar{\rho}) \otimes_n J)^+ \approx C(S/\equiv, \bar{\rho})^+ \otimes_n J.$$

Now let s be an element of S. Then, we have

$$(M) \wedge (S) \vdash \sigma[u_s C(S,\rho)^+ u] \approx u_s (C(S/\equiv, \bar{\rho})^+ \otimes_n J).u.$$

But, according to the structure of $\mathscr{B}$, an easy computation gives

$$u_s (C(S/\equiv, \bar{\rho})^+ \otimes_n J)u = u_{\bar{s}} C(S/\equiv, \bar{\rho})^+ u',$$[9]

where $u_{\bar{s}}$ and u' denote vectors of order $S/\equiv$. Thus, we have proved that

$$(M) \wedge (S) \vdash \sigma[u_s C(S,\rho)^+.u] \approx u_{\bar{s}} C(S/\equiv, \bar{\rho})^+.u'.$$

It is now straightforward to obtain our proposition. □

Corollary 12.6. *Let $\equiv$ be a congruence of a finite semigroup S and let π be the projection of S on $S/\equiv$. Then, for every subset ρ of S, we have*

$$(P(H))_{H \in \mathscr{A}(S)} \wedge P(S,\rho) \overset{(M),(S)}{\vdash\!\!\!\!\!\!-\!\!\!\!\!\!-} P(S/\equiv, \pi(\rho)).$$

Proof. Since we have $\mathscr{A}(S/\equiv) \subset \mathscr{A}(S)$, the corollary follows easily from Propositions 12.5 and 8.2. □

Corollary 12.7. *Let $\equiv$ be a congruence of a semigroup S. Then, we have*

$$(P(H))_{H \in \mathscr{A}(S)} \wedge P(S) \overset{(M),(S)}{\vdash\!\!\!\!\!\!-\!\!\!\!\!\!-} P(S/\equiv).$$

Proof. It is an immediate consequence of Corollary 12.6. □

12.3. Homomorphic image

We can easily express the previous results in terms of homomorphic image.

[9] This relation is obtained by adding in the first member several times the same terms of the second member. Thus it holds, since we have here $1+1=1$.

Proposition 12.8. *Let S, T be two finite semigroups and let φ be a semigroup morphism from S into T. Then, for every subset $\rho \subset S$, we have*

$$(P(H))_{H \in \mathscr{A}(S)} \wedge P(S, \rho) \xrightarrow{(M),(S)} P(\varphi(S), \varphi(\rho)).$$

Proof. Let $\equiv$ denote the semigroup congruence defined by $u \equiv v$ iff $\varphi(u) = \varphi(v)$ for every $u, v \in S$. Since $\varphi(S) \simeq S/\equiv$, our result follows from Corollary 12.6. □

Corollary 12.9. *Let S, T be two finite semigroups and let φ be a semigroup morphism from S into T. Then, we have*

$$(P(H))_{H \in \mathscr{A}(S)} \wedge P(S) \xrightarrow{(M),(S)} P(\varphi(S)).$$

Proof. The corollary follows immediately from Proposition 12.8. □

12.4. Division

Let S and T be two semigroups. Then we say that S *divides* T, and we denote it by $S < T$, iff S is a quotient of a subsemigroup of T (cf. [17] or [9] for more details). We can give the following two results which are immediate consequences of Corollaries 12.2 and 12.6.

Proposition 12.10. *Let S be a finite semigroup that divides a finite semigroup T and let ρ be a subset of T. Then there exists a subsemigroup U of T and a congruence $\equiv$ on U such that $S = U/\equiv$. Let us denote by π the canonical projection from U onto S. Then, we have*

$$(P(H))_{H \in \mathscr{A}(T)} \wedge P(T, \rho) \xrightarrow{(M),(S)} P(S, \pi(\rho \cap U)).$$

Corollary 12.11. *Let S and T be two finite semigroups. Then, if S divides T, we have*

$$(P(H))_{H \in \mathscr{A}(T)} \wedge P(T) \xrightarrow{(M),(S)} P(S).$$

12.5. Direct product

Proposition 12.12. *Let S and T be two finite semigroups and let ρ and ρ' be respectively two subsets of S and T. Then, we have*

$$(P(H))_{H \in \mathscr{A}(S) \cup \mathscr{A}(T)} \wedge P(S, \rho) \wedge P(T, \rho') \xrightarrow{(M),(S)} P(S \times T, \rho \times \rho').$$

Proof. We can write for every pair (s, t) and (u, v) in $S \times T$,

$$[C(S \times T), \rho \times \rho']_{(s,t),(u,v)} = \sum_{\substack{s\alpha = u, \alpha \in \rho \\ t\beta = v, \beta \in \rho'}} a_{(\alpha,\beta)}.$$

Then let us now introduce the substitution σ from A_ρ, into $\mathcal{M}_{S\times S}(\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A_{\rho\times\rho'}\rangle)$ which is defined as follows:

$$\forall t\in\rho',\quad \sigma(a_t)=\left[\sum_{s\alpha=u,\alpha\in\rho} a_{(\alpha,t)}\right]_{(s,u)\in\rho\times\rho'}$$

Observe that we obviously have

$$\sigma[C(T,\rho')]=C(S\times T,\rho\times\rho'). \tag{1}$$

But, we can write, according to Proposition 8.2.

$$(P(H))_{H\in\mathcal{A}(T)}\wedge P(T,\rho')\ \overset{(M),(S)}{\vdash\!\!\!-\!\!\!-}\ C(T,\rho')^+u\approx A^+_{\rho'}u,$$

where u is a vector of order T. Applying σ to this relation, it follows from (1), from Theorem 8.4 and from Proposition 3.9 that we have

$$(P(H))_{H\in\mathcal{A}(T)}\wedge P(T,\rho')\ \overset{(M),(S)}{\vdash\!\!\!-\!\!\!-}\ C(S\times T,\rho\times\rho')^+u\approx\sigma(A_{\rho'})^+u. \tag{2}$$

Let us now study $\sigma(A_{\rho'})$. We can clearly write

$$\begin{aligned}\sigma(A_{\rho'})&=\left[\sum_{t\in\rho'}\left(\sum_{s\alpha=u,\alpha\in\rho} a_{(\alpha,t)}\right)\right]_{(s,u)}\\&=\left[\sum_{s\alpha=u,\alpha\in\rho}\left(\sum_{t\in\rho'} a_{(\alpha,t)}\right)\right]_{(s,u)}\end{aligned}$$

It follows from this computation that we have

$$\sigma(A_{\rho'})=\tau[C(S,\rho)] \tag{3}$$

if we denote by τ the substitution from A_ρ into $A_{\rho\times\rho'}$ which is defined by

$$\forall s\in\rho,\quad \tau(a_s)=\sum_{t\in\rho'} a_{(s,t)}.$$

Therefore, according to the relations (2) and (3), we obtain

$$(P(H))_{H\in\mathcal{A}(T)}\wedge P(T,\rho')\ \overset{(M),(S)}{\vdash\!\!\!-\!\!\!-}\ C(S\times T,\rho\times\rho')^+u\approx\tau[C(S,\rho)^+u].$$

Using $P(S,\rho)$, it follows by Proposition 8.2 that

$$(P(H))_{H\in\mathcal{A}(S)\cup\mathcal{A}(T)}\wedge P(T,\rho')\wedge P(S,\rho)\ \overset{(M),(S)}{\vdash\!\!\!-\!\!\!-}\ C(S\times T,\rho\times\rho')^+u\approx\tau[A^+_\rho u].$$

Observe now that we have

$$\tau(A_\rho)=\sum_{s\in\rho}\sum_{t\in\rho'} a_{(s,t)}=A_{\rho\times\rho'}.$$

Hence, it follows immediately from the previous identity that

$$(P(H))_{H\in\mathcal{A}(S)\cup\mathcal{A}(T)}\wedge P(T,\rho')\wedge P(S,\rho)\ \overset{(M),(S)}{\vdash\!\!\!-\!\!\!-}\ C(S\times T,\rho\times\rho')^+u\approx A^+_{\rho\times\rho'}u.$$

It is now straightforward to conclude to our proposition. □

Note. The above proof shows also that the semigroup identity $P(S\times T, \rho\times\rho')$ is completely defined modulo $(P(H))_{H\in\mathscr{A}(S)\cup\mathscr{A}(T)}$.

The following two results are immediate consequences of Proposition 12.12.

Corollary 12.13. *Let S be a finite semigroup and let ρ be a subset of S. Then, for every $n\in\mathbb{N}^*$, we have*

$$(P(H))_{H\in\mathscr{A}(S)} \wedge P(S,\rho) \xrightarrow{(M),(S)} P(S^n, \rho^n).$$

Corollary 12.14. *Let S and T be two finite semigroups. Then, we have*

$$(P(H))_{H\in\mathscr{A}(S)\cup\mathscr{A}(T)} \wedge P(S) \wedge P(T) \xrightarrow{(M),(S)} P(S\times T).$$

12.6. Semidirect product

Let S, T be two semigroups and let . be a left action of T on S. Then, the *semidirect product* $S \ltimes T$ is the semigroup constructed over $S\times T$ whose law is defined for every s, u in S and t, v in T by

$$(s, t).(u, v) = (s(t.u), tv).$$

We refer the reader to [9] or to [17] for more details.

Proposition 12.15. *Let S be a finite semigroup that acts on the left by . on a finite semigroup T, let $\rho\subset S$ and let $\rho'\subset T$. Then, we have*

$$(P(H))_{H\in\mathscr{A}(S)\cup\mathscr{A}(T)} \wedge P(S, T.\rho) \wedge P(T,\rho') \xrightarrow{(M),(S)} P(S\ltimes T, \rho\times\rho').$$

Proof. We clearly have, for every pair (s, t) and (u, v) in $S\times T$,

$$[C(S\ltimes T, \rho\times\rho')]_{(s,t),(u,v)} = \sum_{s(t.\alpha)=u,\alpha\in\rho}^{t\beta=v,\beta\in\rho'} a_{(\alpha,\beta)}$$

$$= \sum_{sx=u,x\in T.\rho} \sum_{t\beta=v,\beta\in\rho'} \sum_{t.\alpha=x,\alpha\in\rho} a_{(\alpha,\beta)}.$$

Let us now consider the substitution σ from $A_{T.\rho}$ into $\mathscr{M}_{T\times T}(\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A_{\rho\times\rho'}\rangle)$ that is defined by

$$\forall s\in A_{T.\rho},\quad \sigma(a_s) = \left(\sum_{tv=v,\beta\in\rho'} \sum_{t.\alpha=s,\alpha\in\rho} a_{(\alpha,\beta)}\right)_{(t,v)\in T\times T}.$$

The previous relation shows that we have

$$\sigma[C(S, T.\rho)] = C(S\ltimes T, \rho\times\rho'). \tag{1}$$

Hence, it follows from (1) that

$$(M) \wedge (S) \vdash [C(S \leftthreetimes T, \rho \times \rho')]^+.u \approx \sigma[C(S, T.\rho)^+.u].$$

Using $P(S, T.\rho)$, we obtain according to Propositions 8.2, 3.9 and Theorem 8.4 that

$$(P(H))_{H \in \mathcal{A}(S)} \wedge P(S, T.\rho) \xvdash{(M),(S)} [C(S \leftthreetimes T, \rho \times \rho')]^+.u \approx \sigma[A^+_{T,\rho} u]. \qquad (2)$$

But an easy computation permits us to show that we have

$$\begin{aligned}\sigma(A_{T.\rho}) &= \left[\sum_{s \in T.\rho} \sum_{t\beta = v, \beta \in \rho'} \sum_{t.\alpha = s, \alpha \in \rho} a_{(\alpha,\beta)}\right]_{(t,v) \in T \times T} \\ &= \left[\sum_{t\beta = v, \beta \in \rho'} \sum_{s \in T.\rho} \sum_{t.\alpha = s, \alpha \in \rho} a_{(\alpha,\beta)}\right]_{(t,v) \in T \times T} \\ &= \left[\sum_{t\beta = v, \beta \in \rho'} \sum_{\alpha \in \rho} a_{(\alpha,\beta)}\right]_{(t,v) \in T \times T}.\end{aligned}$$

Let us now introduce the substitution τ from $A_{\rho'}$ into $A_{\rho \times \rho'}$ defined by

$$\forall v \in \rho', \quad \tau(a_v) = \sum_{u \in \rho} a_{(u,v)}.$$

Therefore the previous relations show that

$$\sigma(A_{T.\rho}) = \left[\sum_{t\beta = v, \beta \in \rho'} \tau(a_\beta)\right]_{(t,v) \in T \times T} = \tau(C(T, \rho')).$$

Hence, relation (2) can be written as follows.

$$(P(H))_{H \in \mathcal{A}(S)} \wedge P(S, T.\rho) \xvdash{(M),(S)} [C(S \leftthreetimes T, \rho \times \rho')]^+.u \approx \tau[C(T, \rho')^+ u].$$

Using $P(T, \rho')$, it follows easily from Proposition 8.2 that we have

$$(P(H))_{H \in \mathcal{A}(S) \cup \mathcal{A}(T)} \wedge P(S, T.\rho) \wedge P(T, \rho')$$

$$\xvdash{(M),(S)} [C(S \leftthreetimes T, \rho \times \rho')]^+.u \approx \tau[A^+_{\rho'} u].$$

In order to conclude, let us compute $\tau(A_{\rho'})$:

$$\tau(A_{\rho'}) = \sum_{v \in \rho'} \sum_{u \in \rho} a_{(u,v)} = A_{\rho \times \rho'}.$$

Therefore, it follows immediately from the previous identity that

$$(P(H))_{H \in \mathcal{A}(S) \cup \mathcal{A}(T)} \wedge P(S, T.\rho) \wedge P(T, \rho')$$

$$\xvdash{(M),(S)} [C(S \leftthreetimes T, \rho \times \rho')]^+ u \approx A^+_{\rho \times \rho'} u.$$

It is now easy to obtain our proposition. □

Corollary 12.16. *Let S be a finite semigroup that acts on the left by . on a finite semigroup T, let ρ be a . stable subset of S and let $\rho' \subset T$. Then, we have*

$$(P(H))_{H \in \mathscr{A}(T) \cup \mathscr{A}(T)} \wedge P(S, \rho) \wedge P(T, \rho') \vdash^{(M),(S)} P(S \ltimes T, \rho \times \rho').$$

Proof. It is an immediate consequence of Proposition 12.15 and of the fact that $P(S, \rho)$ implies here $P(S, T.\rho)$ according to Proposition 6.2. □

Corollary 12.17. *Let S be a finite semigroup that acts on the left by . on a finite semigroup T. Then, we have*

$$(P(H))_{H \in \mathscr{A}(S) \cup \mathscr{A}(T)} \wedge P(S) \wedge P(T) \vdash^{(M),(S)} P(S \ltimes T)$$

Proof. The corollary follows obviously from Corollary 12.16. □

12.7. Wreath product

Let S and T be two semigroups. Then, the *wreath product* of S and T is the semigroup denoted $S \circ T$ which is the semidirect product $S^{T^1} \ltimes T$ associated with the action of T on S^{T^1} defined for every $f \in S^{T^1}$ and $t \in T$ by

$$t.f : T^1 \to S$$
$$t' \to f(t't).$$

The wreath product is the most general semidirect product possible (see [17] or [9] for more details). Note also that we shall say here that a subset of ρ of S is T-stable iff ρ^{T^1} is T-stable. We can now give the following proposition.

Proposition 12.18. *Let S, T be two finite semigroups, let ρ' be a subset of T and let ρ be a T-stable subset of S. Then, we have*

$$(P(H))_{H \in \mathscr{A}(S) \cup \mathscr{A}(T)} \wedge P(S, \rho) \wedge P(T, \rho') \vdash^{(M),(S)} P(S \circ T, \rho^{T^1} \times \rho').$$

Proof. It follows clearly from Corollary 12.16 that we have

$$(P(H))_{H \in \mathscr{A}(S^{T^1}) \cup \mathscr{A}(T)} \wedge P(S^{T^1}, \rho^{T^1}) \wedge P(T, \rho') \vdash^{(M),(S)} P(S \circ T, \rho^{T^1} \times \rho').$$

But, Corollary 12.13 shows that we have

$$(P(H))_{H \in \mathscr{A}(S)} \wedge P(S, \rho) \vdash^{(M),(S)} P(S^{T^1}, \rho^{T^1}).$$

It is easily shown that every group of $\mathscr{A}(S^{T^1})$ is included in a product of groups of $\mathscr{A}(S)$. Therefore, according to Corollaries 12.3 and 12.14, we have

$$(P(H))_{H \in \mathscr{A}(S)} \vdash^{(M),(S)} (P(H))_{H \in \mathscr{A}(S^{T^1})}.$$

Grouping together the three previous deductions, the proposition now follows immediately. □

Corollary 12.19. *Let S, T be two finite semigroups. Then, we have*

$$(P(H))_{H\in\mathcal{A}(S)\cup\mathcal{A}(T)} \wedge P(S) \wedge P(T) \overset{(M),(S)}{\vdash\!\dashv} P(S\circ T).$$

Proof. It is an obvious consequence of the previous proposition. □

13. Completeness of group identities

13.1. Semigroup and group identities

Let us now recall Krohn-Rhodes's theorem (cf. [9, p. 39] of [15, p. 87]). It will be our main tool to reduce semigroup identities to group identities. Let S be a finite semigroup. Then, S divides the wreath product

$$S < S_1 \circ \cdots \circ S_n \qquad (*)$$

where each S_i is either a simple group dividing S, or is U_2. Moreover, the proof of Krohn-Rhodes's theorem (see [9, pp. 39-42]) shows that all groups that appear in (*) are commutative when S is commutative.

Definition 13.1. For every finite semigroup S, we shall denote by $\mathcal{K}(S)$ the family of groups that appear in Krohn-Rhodes's decomposition (*).

Remark. When S is aperiodic, $\mathcal{K}(S)=\{1\}$ (see [9, Chap. III, Theorem 7.6]).

Theorem 13.1. *Let S be a finite semigroup. Then, we have*

$$(P(H))_{H\in\mathcal{A}(S)\cup\mathcal{K}(S)} \overset{(M),(S)}{\vdash\!\dashv} (P(H))_{H\in\mathcal{A}(S)} \wedge P(S).$$

Proof. It follows immediately from Proposition 8.2, from Corollaries 12.19 and 12.11, from the aperiodicity of U_2 and from Proposition 8.9 that we have

$$(P(H))_{H\in\mathcal{K}(S)} \overset{(M),(S)}{\vdash\!\dashv} P(S).$$

Conversely, since every group in $\mathcal{K}(S)$ divides S, Corollary 12.11 implies that

$$(P(H))_{H\in\mathcal{A}(S)} \wedge P(S) \overset{(M),(S)}{\vdash\!\dashv} (P(H))_{H\in\mathcal{K}(S)}.$$

Thus, this ends our proof. □

We can now solve the second conjecture of Conway [7, p. 116] which claimed that semigroup identities can be reduced to group identities.

Corollary 13.2. *Let $\mathscr{S}$ be the class of finite semigroups and let $\mathscr{G}$ be the class of finite groups. Then, we have the following equivalence:*

$$(P(G))_{G\in\mathscr{G}} \overset{(M),(S)}{\longmapsto} (P(S))_{S\in\mathscr{S}}.$$

Proof. It is an obvious consequence of the previous theorem. □

Corollary 13.3. *Let $\mathscr{SC}$ be the class of* commutative *finite semigroups and let $\mathscr{GC}$ be the class of* commutative *finite groups. Then, we have*

$$(P(G))_{G\in\mathscr{GC}} \overset{(M),(S)}{\longmapsto} (P(S))_{S\in\mathscr{SC}}.$$

Proof. The corollary follows from Theorem 13.1 and from the fact that every group in $\mathscr{K}(S)$ is commutative when S is commutative. □

We can also show that every semigroup identity is equivalent to an identity associated with *only one* group.

Corollary 13.4. *Let S be a finite semigroup. Then, there exists a finite group G_s such that we have*

$$(P(H))_{H\in\mathscr{A}(S)} \wedge P(S) \overset{(M),(S)}{\longmapsto} P(G_s).$$

Proof. By Theorem 13.1, it suffices to construct a group G_s such that

$$(P(H))_{H\in\mathscr{K}(S)\cup\mathscr{A}(S)} \overset{(M),(S)}{\longmapsto} P(G_s) \tag{1}$$

Let us prove that (1) is satisfied with G_s equal to the direct product of the groups in $\mathscr{K}(S)\cup\mathscr{A}(S)$. First, Corollary 12.14 shows that

$$(P(H))_{H\in\mathscr{K}(S)\cup\mathscr{A}(S)} \overset{(M),(S)}{\longmapsto} P(G_s).$$

On the other hand, since every group in $\mathscr{K}(S)\cup\mathscr{A}(S)$ is isomorphic to a subgroup of G_s, Corollary 12.3 gives the converse deduction. Hence, this ends our proof. □

13.2. Completeness of group identities

The previous results now lead us immediately to the following two results of completeness for systems of group identities.

Theorem 13.5. *Let $\mathscr{G}$ be the class of finite groups. Then, the following system is a complete system of $\mathscr{B}$-rational identities for any alphabet A:*

$$(M), (S), (P(G))_{G\in\mathscr{G}}.$$

Proof. It is an immediate consequence of Corollaries 13.2 and 11.3. □

Theorem 13.6. *Let $\mathcal{GC}$ be the class of* commutative *finite groups. Then, the following system is a complete system of $\mathcal{B}$-rational identities for any* one *letter alphabet $A = \{a\}$:*

$$(M), (S), P(G))_{G \in \mathcal{GC}}.$$

Proof. The theorem follows immediately from Corollaries 13.3 and 11.4. □

13.3. Identities of aperiodic semigroups

First, let us recall (see Section 8.1) that it is possible to define the semigroup identity of an aperiodic semigroup only modulo (M) and (S). Theorem 13.1 allows us also to solve an open question of D. Perrin concerning the identities associated with aperiodic semigroups.

Corollary 13.7 (Aperiodic semigroups). *Let S be an aperiodic semigroup. Then, we have $(M) \wedge (S) \vdash P(S)$.*

Proof. The corollary follows clearly from Theorem 13.1 since we have here the following relations: $\mathcal{K}(S) = \mathcal{A}(S) = \{1\}$. □

Note. Thus this corollary generalizes Proposition 8.9. This result justifies also the denomination of *aperiodic identities* for (M) and (S).

We can now give the following result which characterizes the aperiodic semigroups in terms of rational identities.

Theorem 8.8 (Characterization of aperiodic semigroups). *Let S be a finite semigroup. Then the following statements are equivalent:*

(i) *S is an aperiodic semigroup;*

(ii) $(M) \wedge (S) \vdash P(S^1, 1)$.

Proof. Since $\mathcal{A}(S) = \{1\}$, (i) → (ii) follows from Corollary 13.7, Propositions 6.3 and 8.2. To prove (ii) → (i), let us suppose that (ii) holds and that S is not aperiodic. Hence, there would exist a non-trivial group $G \subset S$. Let us denote by G' the semigroup equal to G if $1_G = 1_{S^1}$ and to G^1 if not. Then, it follows from Proposition 12.1 that we have

$$(M) \wedge (S) \vdash P(S^1, 1) \vdash P(G', 1).$$

But, since $\mathcal{A}(G') = \{1\}$, it follows from Proposition 8.2 that we have

$$P(G', 1) \overset{(M),(S)}{\longmapsto} P(G', 1_G).$$

If $G' = G$, $P(G', 1_G)$ is equivalent modulo (M) and (S) to $P(G)$ by Corollary 7.5.

If $G' = G^1$, $P(G', 1_G)$ is equivalent modulo (M) and (S) to $P(G', G, 1_G)$ by Proposition 6.3 and it is easy to see that this last identity is exactly equal to $P(G)$. Therefore, it follows that

$$(M) \wedge (S) \vdash P(G).$$

But there exists clearly an element $g \in G$ of prime order $p \geqslant 2$. Hence, it follows obviously from Proposition 12.3 and Lemma 7.16 that we have

$$(M) \wedge (S) \vdash P(G) \vdash P(\mathbb{Z}/p\mathbb{Z}) \vdash P(p).$$

But, this is in contradiction with Theorem 2.5. Hence, this ends our proof. □

13.4. Reduced action matrices

With Theorem 13.1, we can also reformulate Theorem 10.1, using here only group identities. Observe that our new result is now closely related to Theorem 7.24 which gives a similar result for non-reduced action matrices.

Theorem 13.9. *Let S be a finite semigroup that acts on the right on a free $\mathcal{B}$-module $M = \mathcal{B}\langle E\rangle$ of finite basis E, let $(E_s)_{s\in S}$ denote the universal rational expressions associated with S and let $(R_s)_{s\in S}$ be the reduced action matrices of S on M. Then, we have*

$$(P(H))_{H\in\mathcal{A}(S)\cup\mathcal{K}(S)} \overset{(M),(S)}{\vdash\!\dashv} \left(\sum_{s\in S} a_s R_s\right)^+ \approx \sum_{s\in S} E_s R_s.$$

Proof. It is an immediate consequence of Theorems 10.1 and 13.1. □

13.5. Group identities and Jordan-Hölder sequences

Let us recall (cf. [4, Chap. 1, Section 4.7]) that a Jordan-Hölder sequence of a group G is an increasing sequence $(G_i)_{i=1,n}$ of subgroups of G such that

$$\{1\} = G_1 \subset G_2 \subset \cdots \subset G_{n-1} \subset G_n = G$$

which also satisfies the following two conditions:

$$\forall i \in [1, n-1], \quad G_i \lhd G_{i+1} \quad \text{and} \quad G_{i+1}/G_i \text{ is a simple group.}$$

We can now give the following result.

Proposition 13.10. *Let G be a finite group and let H be a normal subgroup of G. Then, we have*

$$P(G) \overset{(M),(S)}{\vdash\!\dashv} P(H) \wedge P(G/H).$$

Proof. First, it follows from Corollaries 12.3 and 12.7 that

$$P(G) \overset{(M),(S)}{\vdash} P(H) \wedge P(G/H).$$

Conversely, $G < H \circ (G/H)$ by Corollary 2.2.3 of [9]. Hence it follows that

$$P(H) \wedge P(G/H) \overset{(M),(S)}{\longmapsto} P(G)$$

by Corollaries 12.11 and 12.19. □

Proposition 13.11. *Let $(G_i)_{i=1,n}$ be a Jordan-Hölder sequence associated with a finite group G. Then, we have*

$$P(G) \overset{(M),(S)}{\longmapsto} (P(G_{i+1}/G_i))_{i=1,n-1}.$$

Proof. It suffices to use an induction on the length n of a Jordan-Hölder sequence with Proposition 13.10. Observe that the induction starts clearly for $n=1$ since $P(\{1\})$ is the trivial identity $a_1^* \approx a_1^*$. □

Then, we obtain the following result of Conway by a new method.

Corollary 13.12 (Conway [7, p. 116]) (Soluble groups). *Let $\mathcal{P}$ denote the set of prime integers and let G be a finite* soluble *group. Then, we have*

$$(P(\mathbb{Z}/p\mathbb{Z}))_{p\in\mathcal{P}} \overset{(M),(S)}{\longmapsto} P(G).$$

Proof. Let $(G_i)_{i=1,n}$ be a Jordan-Hölder sequence associated with a finite soluble group G. Then, by [4, Corollary 1.72] there exists a family $(p_i)_{i=1,n-1}$ of prime integers such that we have $G_{i+1}/G_i \simeq \mathbb{Z}/p_i\mathbb{Z}$ for every i in $[1, n-1]$. Our result now follows immediately from Proposition 13.11. □

Note. By Proposition 13.11, we can in fact say that we had above

$$(P(\mathbb{Z}/p_i\mathbb{Z}))_{i=1,n-1} \overset{(M),(S)}{\longmapsto} P(G).$$

Corollary 13.13. *Let G be a finite* commutative *group. Then, we have*

$$(P(\mathbb{Z}/p\mathbb{Z}))_{p\in\mathcal{P}} \overset{(M),(S)}{\longmapsto} P(G).$$

Proof. This result follows clearly from Corollary 13.12 since every commutative group is soluble. □

13.6. Some complete systems of $\mathfrak{B}$-rational identities

Using the results of the previous section, we show here how the complete systems obtained in Section 2 can be reduced. Note that the symmetric and the alternating group of order n will be respectively denoted by $\mathfrak{S}_n$ and by $\mathfrak{A}_n$.

Theorem 13.14. *The following system is a complete system of $\mathcal{B}$-rational identities for any alphabet A:*

$$(M), (S), (P(\mathfrak{S}_n))_{n\geqslant 2}.$$

Proof. By Cayley's theorem, every group is a subgroup of some $\mathfrak{S}_n$ with $n \geqslant 2$. Our result now follows easily from Theorem 13.5 and Corollary 12.3. □

Note. Therefore we have obtained the first explicitly described complete system of $\mathcal{B}$-rational identities. Nevertheless, it should not be forgotten that the identity $P(\mathfrak{S}_n)$ uses an alphabet with $n!$ letters!

Corollary 13.15. *The following system is a complete system of $\mathcal{B}$-rational identities for any alphabet A:*

$$(M), (S), (P(\mathfrak{A}_n))_{n\geqslant 2}.$$

Proof. We have $\mathfrak{A}_n \lhd \mathfrak{S}_n$ and $\mathfrak{S}_n/\mathfrak{A}_n \simeq \mathbb{Z}/2\mathbb{Z}$ for every $n \geqslant 2$ (see [5]). It now follows easily from Theorem 13.14 and Proposition 13.10 that

$$(M), (S), P(\mathbb{Z}/2\mathbb{Z}), (P(\mathfrak{A}_n))_{n\geqslant 2} \tag{1}$$

is a complete system of rational identities for A. Since $\mathbb{Z}/2\mathbb{Z}$ is isomorphic to the subgroup $\{(2143), (1234)\}$ of $\mathcal{A}_4$, it follows from Corollary 12.3 that

$$P(\mathfrak{A}_4) \overset{(M),(S)}{\longmapsto} P(\mathbb{Z}/2\mathbb{Z}). \tag{2}$$

Our result now follows easily from (2) and from the completeness of (1). □

Corollary 13.16. *For every integer $m \geqslant 2$, the following system is a complete system of $\mathcal{B}$-rational identities for any alphabet A:*

$$(M), (S), (P(\mathfrak{S}_n))_{n\geqslant m}.$$

Proof. For every $n \geqslant 3$, $\mathfrak{S}_n$ contains the subgroup $S_n = \{\sigma \in \mathfrak{S}_n, \sigma(n) = n\}$ which is clearly isomorphic to $\mathfrak{S}_{n-1}$. It now follows from Corollary 12.3 that

$$P(\mathfrak{S}_n) \overset{(M),(S)}{\longmapsto} P(\mathfrak{S}_{n-1}). \tag{1}$$

Since (1) is true for every $n \geqslant 3$, the corollary now follows obviously from Theorem 13.14. □

Note. Thus, we showed in particular that the system given in Theorem 13.14 is not composed of independent indentities. Indeed, the above proof shows that we have in fact the following sequence of deductions:

$$P(\mathfrak{S}_2) \overset{(M),(S)}{\longmapsto} P(\mathfrak{S}_3) \overset{(M),(S)}{\longmapsto} \cdots \overset{(M),(S)}{\longmapsto} P(\mathfrak{S}_{n-1}) \overset{(M),(S)}{\longmapsto} P(\mathfrak{S}_n) \cdots$$

Therefore, it is not possible to extract from the system given by Theorem 13.14 any subsystem composed of independent identities.

Corollary 13.17. *For every integer $m \geqslant 2$, the following system is a complete system of $\mathcal{B}$-rational identities for any alphabet A:*

$$(M), (S), (P(\mathfrak{A}_n))_{n \geqslant m}.$$

Proof. This result can be easily obtained as in Corollary 13.16. □

Theorem 13.18. *Let $\mathcal{FS}$ be the class of finite simple groups. The following system is a complete system of $\mathcal{B}$-rational identities for any alphabet A:*

$$(M), (S), (P(G))_{G \in \mathcal{FS}}.$$

Proof. It is an immediate consequence of Theorem 13.5 and Proposition 13.11. □

Note. We gave this result though the above system is not optimal. Indeed, the identities associated with the alternating groups of order $\geqslant 5$, which are simple, already form a complete system by Corollary 13.17. With this theorem, we just want to indicate that an interesting research direction would be to see if there are other families of $\mathcal{FS}$ that lead to complete systems.

The following result gives us a complete system for a one letter alphabet which is very close to the system (M), (S), $(P(p))_{p \in \mathcal{P}}$ whose completeness was known in that case (see [7, Chap. 4]).

Theorem 13.19. *Let $A = \{a\}$ be an alphabet with only* one *letter. Then, the following system is a complete system of $\mathcal{B}$-rational identities for $A = \{a\}$:*

$$(M), (S), (P(\mathbb{Z}/p\mathbb{Z}))_{p \in \mathcal{P}}.$$

Proof. The theorem follows immediately from Theorem 13.6 and Corollary 13.13. □

14. Letter reduction conjectures

14.1. The weak letter reduction conjecture

We showed in the last chapter that the system $\mathfrak{S} = (M)$, (S), $(P(\mathfrak{S}_n))_{n \geqslant 2}$ was a complete system of $\mathcal{B}$-rational identities for every alphabet A. Unfortunately, this system is very complex since the identity $(P(\mathfrak{S}_n))$ uses an alphabet with $n!$ letters. In the system $\mathfrak{A} = (M)$, (S), $(P(\mathfrak{U}_n)_{n \geqslant 2})$ which is also complete (cf. Corollary 13.15), the identity $(P(\mathfrak{A}_n))$ uses $\frac{1}{2}n!$ letters, which is not very different. We will present

here a conjecture which, if true, would permit us to reduce the system $\mathfrak{S}$ to an equivalent system with identities involving only two letters. But, let us give first some notations.

In the sequel, σ and ρ will denote respectively the following transposition and cycle of order n of the symmetric group of order n:

$$\sigma = (1\ 2) \quad \text{and} \quad \rho = (2\ 3\ \ldots\ n\ 1).$$

The couple $\{\sigma, \rho\}$ is a generating system for $\mathfrak{S}_n$: thus, the symmetric group is said to be *dicyclic* (see [5, p. 181]).

We can now define the weak letter reduction conjecture which was already given in an equivalent way by Conway (cf. [7, pp. 118, 119]).

Conjecture 14.1. *If $\{\sigma, \rho\}$ is the above generating system of $\mathfrak{S}_n$, we have*

$$P(\mathfrak{S}_n, \{\sigma, \rho\}) \overset{(M),(S)}{\vdash\!\!\!-\!\!\!-} P(\mathfrak{S}_n).$$

Note. This conjecture is extremely strong since it claims that the identity in *two* letters $P(\mathfrak{S}_n, \{\sigma, \rho\})$ implies the identity in $n!$ letters $P(\mathfrak{S}_n)$. Indeed, this is the last important open problem for $\mathcal{B}$-rational identities.

The following proposition shows that, if the conjecture was true, there would exist complete systems using only *two*-letter identities.

Proposition 14.1. *If Conjecture* 14.1 *is true, the following system is a complete system of* two-*letter $\mathcal{B}$-rational identities for any alphabet A*:

$$(M), (S), (P(\mathfrak{S}_n, \{\sigma, \rho\}))_{n \geqslant 2}.$$

Proof. The proposition follows immediately from Theorem 13.14. □

14.2. The identity $P(\mathfrak{S}_n, \{\rho, \sigma\})$

In this section, we will study the identity $P(\mathfrak{S}_n, \{\sigma, \rho\})$ more closely in order to make explicit the weak reduction letter conjecture.

Lemma 14.2. *Let $A = \{a, b\}$ be a two-letter alphabet, let $n \geqslant 3$ and let us consider the following permutations of $\mathfrak{S}_{n-1}$:*

$$\forall i \in [2, n-1], \quad \sigma_i = (n-i, n+1-i) \in \mathfrak{S}_{n-1}$$

and

$$r = (n-1, \ldots, 2, 1) \in \mathfrak{S}_{n-1}.$$

We will denote the action matrices of the elements $(\sigma_i)_{i=2,n-1}$, r and r^{-1} for the natural action of $\mathfrak{S}_{n-1}$ on itself as follows:

$$\forall i \in [2, n-1], \quad \mathcal{B}_i = M_{\sigma_i} \quad \text{and} \quad \mathcal{B}_0 = M_r, \quad \mathcal{B}_1 = M_{r^{-1}}.$$

Let us define $A = aI$ and $B_i = b\mathcal{B}_i$ for every i in $[2, n-1]$ and let us finally introduce the matrix M defined by

$$M = \left(\begin{array}{cc|ccccc} 0 & A+B_0 & 0 & 0 & 0 & \dots & 0 \\ B_1 & 0 & A & 0 & 0 & \dots & 0 \\ \hline 0 & 0 & B_2 & A & 0 & \dots & 0 \\ 0 & 0 & 0 & B_3 & A & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & & & \vdots \\ 0 & 0 & 0 & 0 & 0 & \dots & A \\ A & 0 & 0 & 0 & 0 & \dots & B_{n-1} \end{array}\right)$$

Then, we have the identity

$$P(\mathfrak{S}_{n-1}) \overset{(M),(S)}{\longmapsto} u_1 M^* u$$
$$\approx ((a+b)(b+(ab^*)^{n-2}a))^*\left(1+(a+b)\left(\sum_{i=0}^{n-2}(ab^*)^i\right)\right).$$

Proof. To compute its star, let us decompose M as follows:

$$M^* = \left(\begin{array}{c|cccc} 0 & A+B_0 & 0 & \dots & 0^* \\ \hline B_1 & 0 & A & \dots & 0 \\ 0 & 0 & B_2 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & A \\ A & 0 & 0 & \dots & B_{n-1} \end{array}\right)$$
$$= \left(\begin{array}{c|c} 0 & B \\ \hline C & D \end{array}\right)^* = \left(\begin{array}{c|c} (BD^*C)^* & B(D+CB)^* \\ \hline X & Y \end{array}\right).$$

Since we clearly have $B(C+CB)^* = BD^*(CBD^*)^* = (BD^*C)^*BD^*$ modulo (M) and (S), it follows immediately that

$$(M) \wedge (S) \longmapsto u_1 M^* u \approx u_1 (BD^*C)^*(u + BD^*u).^{10} \tag{0}$$

In order to compute the star of D, observe now that we can write

$$D = b\Delta + aN \quad \text{with } \Delta = \begin{pmatrix} 0 & & & 0 \\ & \mathcal{B}_2 & & \\ & & \ddots & \\ 0 & & & \mathcal{B}_{n-1} \end{pmatrix} \text{ and } N = \begin{pmatrix} 0 & I & 0 & \dots & 0 \\ 0 & 0 & I & \ddots & \vdots \\ \vdots & & \ddots & \ddots & I \\ 0 & & & \dots & 0 \end{pmatrix}.$$

It follows easily that we have modulo (M) and (S),

$$D^* = (b\Delta)^*(aN(b\Delta)^*)^* \tag{1}$$

[10] The two notations "u" denote here two vectors of distinct orders. We will constantly use such a convention in the sequel.

In order to compute $(b\Delta)^*$, let us define

$$\Delta' = \begin{pmatrix} \mathcal{B}_2 & & \\ & \ddots & \\ & & \mathcal{B}_{n-1} \end{pmatrix} \in \mathcal{M}_Q(\mathcal{B}) \quad \text{where } Q=[2,n-1]\times\mathfrak{S}_{n-1}.$$

Every matrix $\mathcal{B}_i$ is the action matrix of a transposition. Therefore $\mathcal{B}_i$ can be interpretated as the action matrix of $1\in\mathbb{Z}/2\mathbb{Z}$ for a left action of $\mathbb{Z}/2\mathbb{Z}$ on the set Q. It follows now from Corollary 7.3 and Lemma 7.16 that we have

$$\begin{aligned}(M)\wedge(S) &\longmapsto (b\Delta')^* \approx (I+b\Delta')(b^2)^* \\ &\overset{(M),(S)}{\longmapsto} (b\Delta')^* \approx (b^2)^*(I+b\Delta'). \end{aligned} \tag{2}$$

Finally, let us introduce the matrix δ, decomposed in the same way as Δ:

$$\delta = \begin{pmatrix} 0 & & & \\ & I & & \\ & & \ddots & \\ & & & I \end{pmatrix}$$

It follows easily from (2) that we have

$$(M)\wedge(S) \vdash (b\Delta)^* \approx I+(b^2)^+\delta+(b^2)^*b\Delta.$$

Since $N\delta = N$, it follows that we have modulo (M) and (S),

$$aN(b\Delta)^* = a(N+(b^2)^+N\delta+(b^2)^*bN\Delta) = a(b^2)^*\mathcal{N} \tag{3}$$

where $\mathcal{N}$ stands for

$$\mathcal{N} = N+bN\Delta = \begin{pmatrix} 0 & I+b\mathcal{B}_2 & 0 & \dots & 0 \\ \vdots & 0 & I+b\mathcal{B}_3 & \dots & 0 \\ & & & & I+b\mathcal{B}_{n-1} \\ 0 & & \dots & & 0 \end{pmatrix}.$$

Then, identities (3) and (1) show that we have modulo (M) and (S),

$$D^* = [I+(b^2)^+\delta+(b^2)^*b\Delta](a(b^2)^*\mathcal{N})^*.$$

But, by iterated applications of (M), we obtain

$$(a(b^2)^*\mathcal{N})^* = \sum_{i=0}^{n-2}(a(b^2)^*\mathcal{N})^i + (a(b^2)^*\mathcal{N})^{n-1}(a(b^2)^*\mathcal{N})^*.$$

Since we have here $(a(b^2)^*\mathcal{N})^{n-1}=0$, it follows immediately that

$$D^* = (I+(b^2)^+\delta+(b^2)^*b\Delta)\left(\sum_{i=0}^{n-2}[a(b^2)^*\mathcal{N}]^i\right). \tag{4}$$

Using (4), we are now able to compute the expression BD^*C that occurs in (0).

But, first let us define for every $i \in [2, n-1]$,

$$\Pi_i = (a(b^2)^*)(I + b\mathcal{B}_2) \dots (a(b^2)^*)(I + b\mathcal{B}_i).$$

Observe now that $B(I + (b^2)^+\delta + (b^2)^* b\Delta) = B$. Then, it follows from (4) that

$$BD^* = B\left(\sum_{i=0}^{n-2} [a(b^2)^*\mathcal{N}]^i\right) = [(aI + b\mathcal{B}_i)\Pi_i]_{i=2,n-1}. \tag{5}$$

It follows immediately from (5) that we have

$$BD^*C = (aI + b\mathcal{B}_1)(b\mathcal{B}_0 + \Pi_{n-1}a). \tag{6}$$

We are now going to use the two relations (5) and (6), obtained with (M) and (S), in order to report them in (0). First, observe that

$$P(\mathbb{Z}/2\mathbb{Z}) \xrightarrow{(M),(S)} \Pi_i u = ((a(b^2)^*(1+b))^i u \approx (ab^*)^i u.$$

Since $n \geqslant 3$, $\mathbb{Z}/2\mathbb{Z}$ can be identified as a subgroup of $\mathfrak{S}_{n-1}$. Therefore, we have according to Corollary 12.3,

$$P(\mathfrak{S}_{n-1}) \xrightarrow{(M),(S)} \Pi_i u \approx (ab^*)^i u. \tag{7}$$

Relation (5) now gives immediately

$$P(\mathfrak{S}_{n-1}) \xrightarrow{(M),(S)} BD^*u \approx \left[(a+b)\left(\sum_{i=0}^{n-2} (ab^*)^i\right)\right] u. \tag{8}$$

Hence, reporting this identity in (0), we obtain

$$P(\mathfrak{S}_{n-1}) \xrightarrow{(M),(S)} u_1 M^* u \approx u_1 (BD^*C)^* u \left(1 + (a+b)\left(\sum_{i=0}^{n-2} (ab^*)^i\right)\right). \tag{9}$$

Thus, we must now study $u_1(BD^*C)^*u$. First, observe that it follows from relations (6) and (7) that we have

$$P(\mathfrak{S}_{n-1}) \xrightarrow{(M),(S)} BD^*Cu \approx (a+b)(b + (ab^*)^{n-2}a)u. \tag{10}$$

But by (6), BD^*C belongs to the $\mathcal{B}$-algebra $\mathcal{C}[\mathfrak{S}_{n-1}]$. Thus it can be written as follows

$$BD^*C = \sum_{\sigma \in \mathfrak{S}_{n-1}} \alpha_\sigma M_\sigma \quad \text{for some } \alpha_\sigma \text{ in } \mathcal{C}_{\mathcal{B}}\mathcal{R}\text{at}\langle a, b\rangle,$$

where (M_σ) are the action matrices associated with the natural action of $\mathfrak{S}_{n-1}$ on itself. Hence, using $P(\mathfrak{S}_{n-1})$, we obtain, by Proposition 7.2,

$$P(\mathfrak{S}_{n-1}) \xrightarrow{(M),(S)} (BD^*C)^*u \approx [u_1(BD^*C)u]^*u.$$

This last relation can be also written, according to (10),

$$P(\mathfrak{S}_{n-1}) \xrightarrow{(M),(S)} (BD^*C)^*u \approx [(a+b)(b + (ab^*)^{n-2}a)]^*u.$$

Therefore, it follows from this last deduction and from (9) that we have

$$P(\mathfrak{S}_{n-1}) \xmapsto{(M),(S)} u_1 M^* u \approx ((a+b)(b+(ab^*)^{n-2}a))^*\left(1+(a+b)\left(\sum_{i=0}^{n-2}(ab^*)^i\right)\right).$$

Thus, this ends the proof of the lemma. □

Proposition 14.3. *Let $n \geqslant 2$, let $\{\sigma, \rho\}$ be the generating system of $\mathfrak{S}_n$ which was previously defined and let us denote by $R(a, b)$ the rational expression*

$$R(a,b) = [(a+b)(b+(ab^*)^{n-2}a)]^*\left(1+(a+b)\left(\sum_{i=0}^{n-2}(ab^*)^i\right)\right).$$

Then, we have modulo (M) and (S),

$$P(\mathfrak{S}_n, \{\sigma, \rho\}) \xmapsto{P(\mathfrak{S}_{n-1})} (a_\sigma + a_\rho)^* \approx R(a_\rho, a_\sigma).$$

Proof. First, observe that this result is obvious for $n = 2$. Now let $n \geqslant 3$ and let us consider the subgroup H of $\mathfrak{S}_n$ defined by

$$H = \mathrm{Fix}(1) = \{\tau \in \mathfrak{S}_n,\ \tau(1) = 1\}.$$

Using the above denotations, it is easy to see that we have

$$\forall i \in [0, n-1], \quad H\rho^i = \{h.\rho^i,\ h \in H\} = \{\tau \in \mathfrak{S}_n,\ \tau(1) = i+1\}. \tag{0}$$

It follows clearly that the family $(H\rho^i)_{i=0,n-1}$ is a partition of $\mathfrak{S}_n$. Observe finally that for every $i \in [2, n-1]$, we have

$$\rho^i \sigma \rho^{-i} = (n+1-i,\ n+2-i) = \sigma_i \in H.$$

It follows that we have for every $i \in [2, n-1]$,

$$(H\rho^i)\sigma = H\rho^i\sigma\rho^{-1}\rho^i = (H\sigma_i)\rho^i. \tag{1}$$

Note that

$$H\sigma_i = H \tag{2}$$

for every $i \in [2, n-1]$ since H is a subgroup of $\mathfrak{S}_n$. Let us now define the element r of H by $\sigma\rho^{-1} = (n \quad n-1 \quad \ldots \quad 3 \quad 2) = r \in H$. Then, we have

$$H\sigma = (H\sigma\rho^{-1})\rho = (Hr)\rho \quad \text{and} \quad (H\rho)\sigma = Hr^{-1}. \tag{3}$$

Since H is a subgroup of $\mathfrak{S}_n$, we have

$$Hr^{-1} = Hr = H. \tag{4}$$

Let us now introduce the following action matrices for r, r^{-1} and $(\sigma_i)_{i=2,n-1}$ associated with the natural action of H on itself:

$$M_0 = \mathrm{Mat}_H Hr, \quad M_1 = \mathrm{Mat}_H Hr^{-1} \quad \text{and} \quad \forall i \in [2, n-1],\ M_i = \mathrm{Mat}_H H\sigma_i.$$

Hence, if we order H, it follows from relations (1), (2), (3) and (4) that we can decompose the matrix $C(\mathfrak{S}_n, \{\sigma, \rho\})$ in the following way:

$$C(\mathfrak{S}_n, \{\sigma, \rho\}) = \begin{array}{c} \\ H \\ H\rho \\ \\ \\ H\rho^{n-1} \end{array} \begin{array}{c} \begin{array}{cccccc} H & H\rho & H\rho^2 & & \cdots & H\rho^{n-1} \end{array} \\ \left(\begin{array}{cccccc} 0 & a_\rho I + a_\sigma M_0 & 0 & 0 & \cdots & 0 \\ a_\sigma M_1 & 0 & a_\rho I & 0 & \cdots & 0 \\ 0 & 0 & a_\sigma M_2 & a_\rho I & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & 0 & \cdots & a_\rho I \\ a_\rho I & 0 & 0 & 0 & \cdots & a_\sigma M_{n-1} \end{array}\right) \end{array}.$$

Using the natural isomorphism of H onto $\mathfrak{S}_{n-1}$, our result now follows clearly from the previous lemma. □

The above proposition leads us naturally to the following definition.

Definition 14.1. Let $n \geq 2$. Then, we shall call *symmetric identity* of order n, and denote by $R(n)$, the following $\mathcal{B}$-rational identity on $A = \{a, b\}$:

$$R(n): \quad (a+b)^* \approx [(a+b)(b+(ab^*)^{n-2}a)]^* \left(1 + (a+b)\left(\sum_{i=0}^{n-2} (ab^*)^i\right)\right).$$

Remark. When we substitute 0 for a (resp. 0 for b) in $R(n)$, we obtain $P(2)$ (resp. $P(n)$). This is a good trick to remember quickly that b is associated with σ and a with ρ in $R(n)$.

We can now define the system given in Proposition 14.1.

Corollary 14.4. *If Conjecture* 14.1 *is true, the following system is a complete system of* two-*letter $\mathcal{B}$-rational identities for any alphabet A:*

$$(M), (S), (R(n))_{n \geq 2}.$$

Proof. With Conjecture 14.1 and Proposition 14.3, it can be easily shown by induction on n that we have for every $n \geq 2$,

$$(R(i))_{i=2,n} \overset{(M),(S)}{\longmapsto} (P(\mathfrak{S}_i, \{\sigma, \rho\}))_{i=2,n}. \qquad (*)$$

Our result now follows clearly from Theorem 13.14, Conjecture 14.1 and (*). □

14.3. The strong letter reduction conjecture

Though the resolution of Conjecture 14.1 would suffice to give a complete system of two-letter identities, it may also be asked whether, for a group G, the $|G|$-letter identity $P(G)$ is a consequence of the $|\gamma|$-letter identity $P(G, \gamma)$ associated with a

generating system γ of G. Such a result would be in the spirit of Section 12 where we showed how natural algebraic operations on semigroups can be expressed in terms of deductions for the associated identities. Let us now give the strong letter reduction conjecture.

Conjecture 14.2. *Let G be a finite group and let γ be a generating system for G. Then, we have*

$$P(G, \gamma) \overset{(M),(S)}{\longmapsto} P(G).$$

Notes. (1) Conjecture 14.2 implies obviously Conjecture 14.1.

(2) The converse deduction of the above follows easily from Proposition 6.2.

(3) A similar conjecture can also be proposed for finite semigroups.

Conjecture 14.2 is motivated by a result of Conway which permits us to show that it is true when G is a commutative finite group, as we will see in the sequel. First, let us recall Conway's theorem.

Theorem 14.5 (Conway [7]). *For every $n \geqslant 2$, we have*

$$P(n) = P(\mathbb{Z}/n\mathbb{Z}, \{1\}) \overset{(M),(S)}{\longmapsto} P(\mathbb{Z}/n\mathbb{Z}).$$

Proof. The fact that $P(n) = P(\mathbb{Z}/p\mathbb{Z}, \{1\})$ comes from Lemma 7.16. The theorem can now be found in [7, Chap. 13, pp. 112–115] by putting together Theorem 4 of [7, p. 112] and the proof of the "boiling process" [7, pp. 113–115]. □

Notes. (1) Conway's proof of the above theorem requires a meta-rule that will be presented and studied in the next section.

(2) With Theorem 14.5 and Corollary 13.12, we can obtain Theorem 6 of Chapter 13 of [7] which says that we have for every soluble group G,

$$(P(p))_{p \in \mathcal{P}} \overset{(M),(S)}{\longmapsto} P(G).$$

We can now prove that the strong letter reduction conjecture is true for every commutative group. But, first, let us show it in the case of finite primary cyclic groups.

Lemma 14.6. *Let $n \geqslant 1$, let p be a prime integer and let γ be a generating system of $\mathbb{Z}/p^n\mathbb{Z}$. Then, we have*

$$P(\mathbb{Z}/p^n\mathbb{Z}, \gamma) \overset{(M),(S)}{\longmapsto} P(\mathbb{Z}/p^n\mathbb{Z}).$$

Proof. Let us consider $\gamma = \{\bar{n}_1, \ldots, \bar{n}_r\}$, a generating system of $\mathbb{Z}/p^n\mathbb{Z}$. Then, using Bezout identity, it follows easily that

$$\text{pcgd}(p^n, (n_i)_{i=1,r}) = 1 \qquad (*)$$

Thus, there exists some $i \in [1, r]$ such that

$$\text{pgcd}(n_i, p^n) = 1 \qquad (**)$$

since, if it were not the case, the prime integer p would divide each n_i and (*) could not be satisfied. Hence, γ contains an element $\bar{n}_i$, given by (**), which is alone a generating system for $\mathbb{Z}/p^n\mathbb{Z}$. Thus, as we have by Proposition 6.2,

$$P(\mathbb{Z}/p^n\mathbb{Z}, \gamma) \overset{(M),(S)}{\longmapsto} P(\mathbb{Z}/p^n\mathbb{Z}, \{\bar{n}_i\}),$$

it suffices to prove the lemma when $\gamma = \{x\}$ is reduced to a single element. In this case, it is easy to see that

$$C(\mathbb{Z}/p^n\mathbb{Z}, \{1\}) = P^{-1}C(\mathbb{Z}/p^n\mathbb{Z}, \{x\}) = P^{-1}C(\mathbb{Z}/p^n\mathbb{Z}, \gamma)P, \qquad (1)$$

where P denotes the boolean permutation matrix associated with σ defined by $\sigma(k) = k.x$ for every k in $\mathbb{Z}/p^n\mathbb{Z}$, which is a permutation of $\mathbb{Z}/p^n\mathbb{Z}$, since $\{x\}$ generates this group. Using the same method as in Proposition 7.2, it follows easily from (1) that

$$(M) \wedge (S) \vdash C(\mathbb{Z}/p^n\mathbb{Z}, \{1\})^+ \approx P^{-1}C(\mathbb{Z}/p^n\mathbb{Z}, \gamma)^+P.$$

Then, it is obvious to deduce from this relation that we have

$$P(\mathbb{Z}/p^n\mathbb{Z}, \{1\}) \overset{(M),(S)}{\longmapsto} P(\mathbb{Z}/p^n\mathbb{Z}, \gamma).$$

Our lemma now follows clearly from Theorem 14.5.

We can now prove that the strong letter reduction conjecture is true for finite commutative groups.

Proposition 14.7 (Letter reduction for commutative groups). *Let G be a* commutative *group and let γ be a generating system of G. Then, we have the deduction*

$$P(G, \gamma) \overset{(M),(S)}{\longmapsto} P(G).$$

Proof. By the classical structure theorem of finite abelian groups, there exist prime integers $(p_i)_{i=1,n}$ and integers $(n_i)_{i=1,n}$ such that

$$G \simeq \prod_{1 \leq i \leq n} \mathbb{Z}/p_i^{n_i}\mathbb{Z}.$$

Let us now consider the projection π_i of G onto its ith component $\mathbb{Z}/p_i^{n_i}\mathbb{Z}$. The system $\gamma_i = \pi_i(\gamma)$ is clearly a generating system for the group $\mathbb{Z}/p_i^{n_i}\mathbb{Z}$. Hence, by Lemma 14.6, we obtain the deductions

$$\forall i \in [1, n], \quad P(\mathbb{Z}/p_i^{n_i}\mathbb{Z}, \gamma_i) \overset{(M),(S)}{\longmapsto} P(\mathbb{Z}/p_i^{n_i}\mathbb{Z}).$$

But, according to Proposition 12.8, we have

$$\forall i \in [1, n], \quad P(G, \gamma) \overset{(M),(S)}{\vdash\!\!\!-\!\!\!-} P(\pi_i(G), \pi_i(\gamma)) = P(\mathbb{Z}/p_i^{n_i}\mathbb{Z}, \gamma_i).$$

Grouping the two last identities, it follows that

$$P(G, \gamma) \overset{(M),(S)}{\vdash\!\!\!-\!\!\!-} \{P(\mathbb{Z}/p_i^{n_i}\mathbb{Z})\}_{i=1,n} \tag{1}$$

But Corollary 12.14 shows that

$$\{P(\mathbb{Z}/p_i^{n_i}\mathbb{Z})\}_{i=1,n} \overset{(M),(S)}{\vdash\!\!\!-\!\!\!-} P\left(\prod_{1 \leqslant i \leqslant n} \mathbb{Z}/p_i^{n_i}\mathbb{Z}\right) = P(G). \tag{2}$$

The proposition follows now immediately from (1) and (2). □

Note. The previous result can probably be generalized to soluble groups.

14.4. A complete system for a one-letter alphabet

Theorem 14.5 permits us to give the following simple proof of the completeness of the classical axioms for a one-letter alphabet.

Theorem 14.8 (Completeness of the classical axioms for $A = \{a\}$). *Let $\mathscr{P}$ be the set of prime integers. Then the following system is a complete system of $\mathscr{B}$-rational independent identities for $A = \{a\}$:*

$$(M), (S), (P(p))_{p \in \mathscr{P}}.$$

Proof. It follows immediately from Theorems 13.19, 14.5 and 2.5. □

Notes. (1) The classical proof of this result can be found in [7, Chap. 4].

(2) This theorem gives us a complete system of two-letter identities for a one-letter alphabet which is optimal in the sense of Theorem 2.4.

14.5. Matrix versions of group identities

It follows also from the strong letter reduction conjecture that every $|\gamma|$-letter identity $P(G, \gamma)$ implies its matrix versions for every group G and every generating system γ of G.

Proposition 14.9. *Let γ be a generating system of a finite group G. Then, if conjecture* 14.2 *is true, we have for every matrix substitution σ,*

$$P(G, \gamma) \overset{(M),(S)}{\vdash\!\!\!-\!\!\!-} \sigma(P(G, \gamma)).$$

Proof. Theorem 8.4 shows that we have for every matrix substitution σ,

$$P(G) \overset{(M),(S)}{\longmapsto} \sigma(P(G)). \tag{1}$$

Since $P(G, \gamma)$ is a consequence of $P(G)$ by Proposition 6.2, it follows from relation (1) and Proposition 3.9 that we have

$$P(G) \overset{(M),(S)}{\longmapsto} \sigma(P(G, \gamma)).$$

Our proposition now follows immediately from Conjecture 14.2. □

The following corollary generalizes the corresponding result of Conway that was given for $G = \mathbb{Z}/n\mathbb{Z}$ with $P(n)$ (cf. [7, p. 115]).

Corollary 14.10. *Let γ be a generating system of a finite* commutative *group G. Then, for every matrix substitution σ, we have*

$$P(G, \gamma) \overset{(M),(S)}{\longmapsto} \sigma(P(G, \gamma)).$$

Proof. It follows immediately from Propositions 14.9 and 14.7. □

15. Complete systems of rules

15.1. The concept of meta-rule

Up to now, we have worked only with $\mathscr{B}$-rational identities. But, it can be also interesting to use rules of deduction. Hence, let us now define what we mean by *rule*: let $\mathscr{S}, \mathscr{T}$ be two vectors with coefficients in $\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle B\rangle$, let $\mathscr{I}, \mathscr{J}$ be two $\mathscr{B}$-rational expressions in $\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle B\rangle$ and let us suppose that we have

$$\forall \mathscr{E} \in (\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle)^B, \quad \lambda(\mathscr{S}(\mathscr{E})) = \lambda(\mathscr{T}(\mathscr{E})) \Rightarrow \lambda(\mathscr{I}(\mathscr{E})) = \lambda(\mathscr{J}(\mathscr{E})). \tag{*}$$

Definition 15.1. Then, we call *meta-rule* associated with (*), the deduction rule denoted ($\mathscr{MR}$) and defined by

$$\forall \mathscr{E} \in (\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle)^B, \quad \mathscr{S}(\mathscr{E}) \approx \mathscr{T}(\mathscr{E}) \Rightarrow \mathscr{I}(\mathscr{E}) \approx \mathscr{J}(\mathscr{E}).$$

Note. More generally, we can suppose that (*) holds under certain hypotheses on $\mathscr{E}$ (such as asking that the constant coefficient of certain entries of $\mathscr{E}$ is 0, for instance). This leads to a more general model of meta-rule. But, all the results that are given in the sequel remain valid for such rules.

Observe that a meta-rule is *consistent* by construction: this means that, if the interpretation of the first member of a meta-rule is valid, it is also the case for the

interpretation of the second member. Thus, we can define the notion of deduction using a meta-rule.

Definition 15.2. Let $\mathscr{A}$ be a system of $\mathscr{B}$-rational identities and let $(\mathscr{MR})$ be a meta-rule associated with a condition $(*)$. Then, one says that a $\mathscr{B}$-rational identity (E, F) is a *consequence* from $\mathscr{A}$ and from $(\mathscr{MR})$ and one denotes

$$\mathscr{A}, (\mathscr{MR}) \vdash E \approx F \quad \text{or} \quad \mathscr{A} \overset{(\mathscr{MR})}{\vdash\!\!\!-\!\!\!-} E \approx F$$

iff there exists a sequence of $\mathscr{B}$-rational identities $(E_i, F_i)_{i=1,n}$ ending with (E, F), such that we are, for every $k \in [1, n]$, either in one of the situations $(\mathrm{D}_i)_{i=1,8}$ of Definition 2.3, or in the situation

(D_9) $\quad \exists (i_b)_{b \in B} \in [1, k[^B, \exists \mathscr{E} \in (\mathscr{E}_{\mathscr{B}} \mathscr{R} \mathrm{at}\langle A \rangle)^B,$

$$(E_{i_b}, F_{i_b}) = (\mathscr{S}_i(\mathscr{E}), \mathscr{T}_i(\mathscr{E})) \quad \text{and} \quad (E_k, F_k) = (\mathscr{I}(\mathscr{E}), \mathscr{J}(\mathscr{E})).$$

Note. (D_9) expresses that we can apply the meta-rule in order to deduce its conclusion when the premises of the meta-rule are deduced.

All the vocabulary concerning deductions that we defined in Sections 2 and 3, can be extended without difficulty to deductions using meta-rules. Thus we can in particular speak of:

- matrix deductions using meta-rules (defined as in Section 3.1);
- complete systems of meta-rules (defined as in Definition 2.5);
- models of a meta-rule: Definition 2.7 can be easily adapted. Observe also that Proposition 2.6 still holds for meta-rules.

Let us end by defining the notion of consequence of a meta-rule.

Definition 15.3. Let $\mathscr{A}$ and $(\mathscr{MR})$ be respectively two systems of $\mathscr{B}$-rational identities and of meta-rules and let $(\mathscr{MR}_1)$ be a meta-rule given by

$$\forall \mathscr{E} \in \mathscr{E}_{\mathscr{B}} \mathscr{R} \mathrm{at}\langle A \rangle, \quad \mathscr{P}_1(\mathscr{E}) \Rightarrow \mathscr{C}_1(\mathscr{E}).$$

Then, the meta-rule $(\mathscr{MR}_1)$ is said to be a *consequence* of $\mathscr{A}$ and of $(\mathscr{MR})$ iff

$$\forall \mathscr{E} \in \mathscr{E}_{\mathscr{B}} \mathscr{R} \mathrm{at}\langle A \rangle, \quad \mathscr{P}_1(\mathscr{E}) \overset{\mathscr{A}, (\mathscr{MR}_1)}{\vdash\!\!\!-\!\!\!-} \mathscr{C}_1(\mathscr{E}).$$

We shall denote such a situation as follows:

$$\mathscr{A}, (\mathscr{MR}) \vdash (\mathscr{MR}_1).$$

Note. If a meta-rule $(\mathscr{MR}_1)$ is a consequence of $\mathscr{A}$ and $(\mathscr{MR})$, every consequence of $(\mathscr{MR}_1)$ is clearly a consequence of $\mathscr{A}$ and $(\mathscr{MR})$.

15.2. Conway's meta-rule

We are going to study here a meta-rule introduced by Conway (cf. [7, p. 116]) who claimed without proof that his rule was equivalent with the corresponding monoid identity. Following Platieau [18], we shall now show this equivalence.

Lemma 15.1 (Platieau [18]). *Let M be a finite monoid and let $(E_m)_{m\in M}$ be a family of $\mathcal{B}$-rational expressions. Let us now define for every m, n in M,*

$$E_{m,n} = \sum_{mu=n} E_u.$$

Then, we have the deduction

$$\{E_m E_n \leqslant E_{mn}\}_{m,n\in M} \vdash \{E_{m,n}E_{n,p} \leqslant E_{m,p}\}_{m,n,p\in M}.$$

Proof. Let $(E_m)_{m\in M}$ be expressions in $\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle$ that satisfy the premises of the deduction to be proved and let $m, n, p \in M$. Then, we have

$$\{E_m E_n \leqslant E_{mn}\}_{m,n\in M} \vdash E_{m,n}E_{n,p} = \sum_{mu=n}\sum_{nv=p} E_u E_v \leqslant \sum_{mu=n}^{nv=p} E_{uv}$$

$$\vdash E_{m,n}E_{n,p} \leqslant \sum_{mw=p} E_w = E_{m,p}.$$

This ends our proof. □

Lemma 15.2 (Platieau 18]). *Let M be a finite* set *and let $(E_{m,n})_{m,n\in M}$ be a family of $\mathcal{B}$-rational expressions. Let us introduce the matrix*

$$\mathcal{M} = [E_{m,n}]_{(m,n)\in M} \in \mathcal{M}_{M\times M}(\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle).$$

Then, we have the following deduction:

$$\left.\begin{array}{l} \forall m, n, p \in M, \quad E_{m,n}E_{n,p} \leqslant E_{m,p} \\ \forall m \in M, \quad E^*_{m,m} \approx E_{m,m} \end{array}\right\} \vdash^{(M),(S)} \mathcal{M}^* \approx \mathcal{M}.$$

Proof. We shall use an induction on $|M|$. At first, the lemma is clear when $|M| = 1$. Now let $n \geqslant 2$ and let us suppose that our result is proved for every $|M| < n$. Then, let $M = \{m_1, \ldots, m_n\}$ and let $(E_m)_{m\in M}$ be a family of rational expressions that satisfy the premises, denoted $\mathcal{P}(\mathcal{E})$, of the deduction to be proved. We can decompose $\mathcal{M}$ as follows:

$$\mathcal{M} = \left(\begin{array}{c|ccc} E_{1,1} & E_{1,2} & \ldots & E_{1,n} \\ \hline E_{2,1} & E_{2,2} & \ldots & E_{2,n} \\ \vdots & \vdots & & \vdots \\ E_{n,1} & E_{n,2} & \ldots & E_{n,n} \end{array}\right) = \left(\begin{array}{c|c} E_{1,1} & B \\ \hline C & D \end{array}\right), \quad \text{where } E_{i,j} = E_{m_i,m_j}.$$

The matrix $\mathcal{M}^*$ can be written modulo (M) and (S) as follows:

$$\mathcal{M}^* = \left(\begin{array}{c|c} \mathcal{A} & \mathcal{B} \\ \hline \mathcal{C} & \mathcal{D} \end{array}\right)$$

where we will make $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$ and $\mathcal{D}$ more precise later. It follows from the induction hypothesis that we have

$$\mathcal{P}(E) \vdash^{(M),(S)} D^* \approx D. \tag{0}$$

We can now study $\mathscr{A}$ and write

$$\begin{aligned}
\mathscr{P}(E) &\vdash^{(M),(S)} \mathscr{A} = (E_{1,1} + BD^*C)^* \approx (E_{1,1} + BDC)^* \\
&\vdash \mathscr{A} \leqslant (E_{1,1} + \sum_{k,l \geqslant 2} E_{1,k} E_{k,l} E_{l,1})^* \\
&\vdash^{\mathscr{P}(E)} \mathscr{A} \leqslant (E_{1,1} + \sum_{k,l \geqslant 2} E_{1,1})^* = E_{1,1}^* \\
&\vdash^{\mathscr{P}(E)} \mathscr{A} \leqslant E_{1,1}. \qquad (1)
\end{aligned}$$

Let us now study $\mathscr{C}$. It follows from (0) and (1) that we have

$$\begin{aligned}
\mathscr{P}(E) &\vdash^{(M),(S)} \mathscr{C} = D^*C\mathscr{A} \approx DC\mathscr{A} \leqslant DCE_{1,1} \\
&\vdash \mathscr{C} \leqslant \left[\sum_{k \geqslant 2} E_{i,k} E_{k,1} E_{1,1} \right]_{i=2,n} \\
&\vdash^{\mathscr{P}(E)} \mathscr{C} \leqslant \left[\sum_{k \geqslant 2} E_{i,1} \right]_{i=2,n} = [E_{i,1}]_{i=2,n}. \qquad (2)
\end{aligned}$$

Let us come now to the study of $\mathscr{D}$. We have, therefore,

$$\begin{aligned}
\mathscr{P}(E) &\vdash^{(M),(S)} \mathscr{D} = (D + CE_{1,1}^* B)^* \approx (D + CE_{1,1} B)^* \\
&\vdash \mathscr{D} \approx [E_{i,j} + E_{i,1} E_{1,1} E_{1,j}]_{i,j \geqslant 2}^* \\
&\vdash^{\mathscr{P}(E)} \mathscr{D} \leqslant [E_{i,j} + E_{i,j}]_{i,j \geqslant 2}^* = [E_{i,j}]_{i,j \geqslant 2}^* \\
&\vdash^{(M),(S)} \mathscr{D} \leqslant [E_{i,j}]_{i,j \geqslant 2}, \qquad (3)
\end{aligned}$$

where the last deduction comes from the induction hypothesis applied to D. Finally let us end with $\mathscr{B}$. Then, we have by (3),

$$\begin{aligned}
\mathscr{P}(E) &\vdash^{(M),(S)} \mathscr{B} = E_{1,1}^* B\mathscr{D} \approx E_{1,1} B\mathscr{D} \leqslant E_{1,1} B[E_{i,j}]_{i,j \geqslant 2} \\
&\vdash \mathscr{B} \leqslant \left[E_{1,1} \left(\sum_{i \geqslant 2} E_{1,i} E_{i,j} \right) \right]_{j \geqslant 2} \\
&\vdash^{\mathscr{P}(E)} \mathscr{B} \leqslant \left[\sum_{i \geqslant 2} E_{1,j} \right]_{j \geqslant 2} = [E_{1,j}]_{j \geqslant 2}. \qquad (4)
\end{aligned}$$

The four identities (1), (2), (3) and (4) mean exactly that we have

$$\mathscr{P}(E) \vdash^{(M),(S)} \mathscr{M}^* \leqslant \mathscr{M}. \qquad (5)$$

But, we clearly have

$$(M) \wedge (S) \vdash \mathscr{M}^* \approx I + \mathscr{M} + \mathscr{M}^2 \mathscr{M}^* \geqslant \mathscr{M}. \qquad (6)$$

The lemma follows now from (5), (6) and Proposition 2.9. □

Proposition 15.3 (Conway [7, p. 116] and [18]). *Let M be a finite monoid and let $(E_m)_{m\in M}$ be a family of $\mathcal{B}$-rational expressions on an alphabet A. Then, we have modulo (M) and (S),*

$$\left.\begin{array}{l}\forall m, n \in M,\ E_m E_n \leqslant E_{mn} \\ \forall m \in M,\ \left(\sum_{mu=m} E_u\right)^* \approx \sum_{mu=m} E_u\end{array}\right\} \overset{Q(M,1)}{\longmapsto} \left(\sum_{m\in M} E_m\right)^* \approx \sum_{m\in M} E_m.$$

Proof. Let us denote by $\mathcal{P}(E)$ the premises of the deduction to be proved. Let us now introduce the following matrix:

$$\mathcal{M} = [E_{m,n}]_{(m,n)\in M} \in \mathcal{M}_{M\times M}(\mathcal{C}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle), \quad \text{where } E_{m,n} = \sum_{mu=n} E_u.$$

It follows from Lemmas 15.1 and 15.2 that we have

$$\mathcal{P}(E) \overset{(M),(S)}{\longmapsto} \mathcal{M}^* \approx \mathcal{M}. \tag{1}$$

On the other hand, using $Q(M, 1)$, we obtain

$$Q(M,1) \vdash \left[\sum_{m\in M} E_{1,m}\right]^* \approx \sum_{m\in M} (\mathcal{M}^*)_{1,m}.$$

Therefore, it follows from (1) that

$$\mathcal{P}(E) \wedge Q(M,1) \overset{(M),(S)}{\longmapsto} \left[\sum_{m\in M} E_{1,m}\right]^* \approx \sum_{m\in M} E_{1,m}$$

$$\longmapsto \left[\sum_{m\in M} E_m\right]^* \approx \sum_{m\in M} E_m.$$

Hence, this ends our proof. □

This proposition allows us to give the following definition.

Definition 15.4. Let M be a finite monoid. Then we call *meta-rule of Conway* associated with M, and we denote by $\mathcal{R}(M)$, the deduction rule defined by: for every family $(E_m)_{m\in M}$ of $\mathcal{B}$-rational expressions, we have

$$\left.\begin{array}{l}\forall m, n \in M,\ E_m E_n \leqslant E_{mn} \\ \forall m \in M,\ \left(\sum_{mu=m} E_u\right)^* \approx \sum_{mu=m} E_u\end{array}\right\} \Rightarrow \left(\sum_{m\in M} E_m\right)^* \approx \sum_{m\in M} E_m.$$

Remarks. (1) A similar meta-rule can be given for semigroups (it suffices to replace the star by +). It can be shown that the meta-rule associated in this way with the semigroup S is equivalent to $\mathcal{R}(S^1)$. We shall not develop this viewpoint here: indeed, we can work equivalently with monoids or semigroups. Moreover, Conway's meta-rule will be essentially used with groups.

(2) When G is a finite group G, the rule $\mathcal{R}(G)$ says just that: for every family $(E_g)_{g\in G}$ of $\mathcal{B}$-rational expressions, we have

$$\left.\begin{array}{l}\forall g, h \in G, E_g E_h \leqslant E_{gh} \\ E_1^* \approx E_1\end{array}\right\} \Rightarrow \left(\sum_{g\in G} E_g\right)^* \approx \sum_{g\in G} E_g.$$

We can now establish the equivalence between $\mathcal{R}(M)$ and $Q(M, 1)$. This result was claimed, but not proved, by Conway (cf. [7, p. 116]) and it seems that the first proof of this fact was given by Platieau [18].

Lemma 15.4 (Conway [7]). *Let M be a finite monoid and let $(E_m)_{m\in M}$ be the family of the $\mathcal{B}$-rational expressions associated with M by Corollary 7.27. Then, for every rational expression $\mathcal{E} \in \mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A_M\rangle$, we have modulo (M) and (S),*

$$\mathcal{E}(a_m)_{m\in M} \leqslant \sum_{mu=n} E_u \xrightarrow{P(H)_{H\in\mathcal{A}(M)}} \mathcal{E}(E_m)_{m\in M} \leqslant \sum_{mu=n} E_u.$$

Proof. According to Corollary 7.27, we can write modulo (M) and (S),

$$(P(H))_{H\in\mathcal{A}(M)} \vdash [C(M)]^* \approx \sum_{m\in M} E_m M_m,$$

where $(M_m)_{m\in M}$ is the family of action matrices for the natural action of M on itself. Let us denote by σ the substitution of $\mathcal{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A_M\rangle$ defined by

$$\forall m \in M, \quad \sigma(a_m) = E_m.$$

Then, the previous relation can be written

$$(P(H))_{H\in\mathcal{A}(M)} \vdash [C(M)]^* \approx \sigma(C(M)). \tag{1}$$

According to Theorem 3.1, Corollary 3.2 and (1), it follows from Proposition 2.2 that the following deductions hold:

$$\begin{aligned}(P(H))_{H\in\mathcal{A}(M)} &\longmapsto [C(M)]^{**} \approx [\sigma(C(M))]^* \\ &\xrightarrow{(M),(S)} [C(M)]^* \approx [\sigma(C(M))]^* \\ &\xrightarrow{(P(H))_{H\in\mathcal{A}(M)}} \sigma(C(M)) \approx [\sigma(C(M))]^* \\ &\longmapsto \sigma(C(M)) \approx \sigma[C(M)]^* \\ &\xrightarrow{(P(H))_{H\in\mathcal{A}(M)}} \sum_{m\in M} E_m M_m \approx \sum_{m\in M} \sigma(E_m) M_m.\end{aligned}$$

Hence, if we identify the entries of the row associated with 1_M in this last relation, we obtain immediately

$$\forall m \in M, \quad (P(H))_{H\in\mathcal{A}(M)} \xrightarrow{(M),(S)} E_m \approx \sigma(E_m).$$

It follows easily that we have for every $\mathscr{E}$ in $\mathscr{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A_M\rangle$,

$$\mathscr{E}(a_m)_{m\in M} \leq \sum_{mu=n} E_u \longmapsto \sigma(\mathscr{E}(a_m)_{m\in M}) \leq \sum_{mu=n} \sigma(E_u)$$

$$\overset{(P(H))_{H\in\mathscr{A}(M)}}{\longmapsto} \mathscr{E}(E_m)_{m\in M} \leq \sum_{mu=n} E_u.$$

Therefore, our lemma is proved. □

Proposition 15.5 (Conway [7, p. 116] and [18]). *Let M be a finite monoid. Then, we have modulo (M) and (S),*

$$\mathcal{R}(M) \overset{(P(H))_{H\in\mathscr{A}(M)}}{\longmapsto\!\!\dashv} Q(M,1).$$

Proof. According to Proposition 15.3, we just have to prove

$$\mathcal{R}(M) \overset{(M),(S)}{\longmapsto} Q(M,1).$$

Let us denote by $(E_m)_{m\in M}$ the family of $\mathcal{B}$-rational expressions defined by Corollary 7.27. According to this result, we have

$$(P(H))_{H\in\mathscr{A}(M)} \vdash [C(M)]^* \approx \left[\sum_{mu=n} E_u\right]_{(m,n)\in M\times M}. \tag{1}$$

Let us now prove that the family $(E_m)_{m\in M}$ satisfies the premises of $\mathcal{R}(M)$. First, observe that we have for every m, n in M,

$$(M)\wedge(S) \vdash a_m a_n \leq a_m\left[\sum_{mu=mn} a_u\right] \leq [C(M)^2]_{1,mn} \leq [C(M)]^*_{1,mn},$$

according to Propositions 3.1 and 3.2. Therefore, it follows from (1) that

$$(P(H))_{H\in\mathscr{A}(M)} \overset{(M),(S)}{\longmapsto} a_m a_n \leq E_{mn}.$$

Hence, applying the previous lemma, we obtain

$$(P(H))_{H\in\mathscr{A}(M)} \overset{(M),(S)}{\longmapsto} E_m E_n \leq E_{mn}. \tag{2}$$

It can also be easily proved by induction on the order of a matrix that every diagonal entry of the star of a matrix is of the form Z^*. Using Proposition 2.2, it follows from this remark that we have for every matrix M in $\mathcal{M}_{n\times n}(\mathscr{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle)$ and for every i in $[1,n]$,

$$(M)\wedge(S) \vdash (M^*)_{i,i} \approx [(M^*)_{i,i}]^*.$$

Applying this identity to $C(M)$ and using (1), we obtain for every m in M,

$$(P(H))_{H\in\mathscr{A}(M)} \overset{(M),(S)}{\longmapsto} \left[\sum_{mu=m} E_u\right]^* \approx \sum_{mu=m} E_u. \tag{3}$$

Then, the two relations (2) and (3) show that the family $(E_m)_{m\in M}$ satisfy the premises of the rule $\mathscr{R}(M)$. Hence, using this rule, it follows that

$$(P(H))_{H\in\mathscr{A}(M)} \wedge (M) \wedge (S) \vdash\!\!\!\xrightarrow{\mathscr{R}(M)}\!\!\!- \left[\sum_{m\in M} E_m\right]^* \approx \sum_{m\in M} E_m. \tag{4}$$

But, according to (1), we can also write

$$(P(H))_{H\in\mathscr{A}(M)} \wedge (M) \wedge (S) \vdash a_m = [C(M)]_{1,m} \leqslant [C(M)^*]_{1,m} \approx E_m.$$

Thus, it follows from Proposition 2.10 that we have

$$(P(H))_{H\in\mathscr{A}(M)} \wedge (M) \wedge (S) \vdash \sum_{m\in M} E_m \leqslant A_M^* = \left(\sum_{m\in M} a_m\right)^* \leqslant \left(\sum_{m\in M} E_m\right)^*.$$

According to Proposition 2.9, it follows from this relation and from (4) that

$$\begin{aligned}(P(H))_{H\in\mathscr{A}(M)} \wedge (M) \wedge (S) &\vdash\!\!\!\xrightarrow{\mathscr{R}(M)}\!\!\!- \sum_{m\in M} E_m \leqslant A_M^* \leqslant \sum_{m\in M} E_m \\ &\vdash\!\!\!- \sum_{m\in M} E_m \approx A_M^*.\end{aligned}$$

Since this last identity is obviously equivalent to $Q(M, 1)$, this ends the proof of our proposition. □

When M is a group, the previous proposition gives us more simply the following corollary.

Corollary 15.6 (Conway's meta-rule for groups). *Let G be a finite group. Then, we have*

$$\mathscr{R}(G) \vdash\!\!\!\xrightarrow{(M),(S)}\!\!\!\dashv P(G).$$

Proof. Since $\mathscr{A}(G) = \{1\}$ for a group, the corollary follows immediately from Proposition 15.5, Corollary 7.5 and Proposition 6.4.

Corollary 157.7 (Completeness of Conway's meta-rule). *Let $\mathscr{G}$ be the class of finite groups. Then, the following system is a complete system of rules for every alphabet A:*

$$(M), (S), (\mathscr{R}(G))_{G\in\mathscr{G}}.$$

Proof. It is an immediate consequence of Corollary 15.6 and of Theorem 13.5. □

Note. Using Proposition 15.5, the other complete systems obtained in Section 13 can also be easily transformed into complete systems of rules.

15.3. Salomaa's meta-rules

Let us introduce now the definition of Salomaa's meta-rules.

Definition 15.5. (1) We call *Salomaa's meta-rule* the deduction rule, denoted by $(\mathcal{S})$, which is defined by

$$\forall E, F, G \in \mathscr{C}_{\mathscr{R}}\mathrm{at}\langle A\rangle, \quad \begin{cases} E \approx EF + G \\ c(F) = 0 \end{cases} \Rightarrow E \approx GF^*.$$

(2) We call *Salomaa's unitary meta-rule* the deduction rule, denoted by $(\mathcal{S}1)$, which is defined by

$$\forall E, F \in \mathscr{C}_{\mathscr{R}}\mathrm{at}\langle A\rangle, \quad \begin{cases} E \approx EF + 1 \\ c(F) = 0 \end{cases} \Rightarrow E \approx F^*.$$

(3) We call *Salomaa's alphabetic meta-rule* the deduction rule, denoted by $(\mathcal{SA})$, which is defined by

$$\forall A, \forall E \in \mathscr{C}_{\mathscr{R}}\mathrm{at}\langle A\rangle, \quad E \approx 1 + E.A \Rightarrow E \approx A^*.$$

Note. Salomaa showed that (M), (S), $(\mathcal{S})$ is a complete system (see [23] and [11, Chap. 5]). He conjectured that (M), (S), $(\mathcal{S}1)$ remains also complete.

Proposition 15.8. *Let $\mathcal{G}$ be the class of finite groups. Then, we have the following sequence of deductions*:

$$(\mathcal{S}) \vdash (\mathcal{S}1) \vdash (\mathcal{SA}) \overset{(M),(S)}{\vdash\!\!\!-\!\!\!-} (P(G))_{G\in\mathcal{G}}.$$

Proof. Clearly, the only non-trivial deduction to prove is

$$(\mathcal{SA}) \overset{(M),(S)}{\vdash\!\!\!-\!\!\!-} (P(G))_{G\in\mathcal{G}}. \tag{0}$$

Let G be a finite group, let $(M_g)_{g\in G}$ be the action matrices for the natural action of G on itself and let $(E_g)_{g\in G}$ be the universal rational expressions associated with G which are defined according to Corollary 7.3 by

$$(M) \wedge (S) \vdash \Big(\sum_{g\in G} a_g M_g\Big)^+ \approx \sum_{g\in G} E_g M_g.$$

By Proposition 8.2, the identity $P(G)$ is defined modulo (M) and (S) by

$$A_G^+ \approx E, \quad \text{where } E = \sum_{g\in G} E_g.$$

According to Theorem 3.1 and to Proposition 3.9, we can write

$$(M) \wedge (S) \vdash \Big(\sum_{g\in G} a_g M_g\Big)^+ \approx \sum_{g\in G} a_g M_g + \Big(\sum_{g\in G} a_g M_g\Big)^+ \Big(\sum_{g\in G} a_g M_g\Big)$$

$$\vdash \Big(\sum_{g\in G} E_g M_g\Big) \approx \sum_{g\in G} a_g M_g + \Big(\sum_{g\in G} E_g M_g\Big)\Big(\sum_{g\in G} a_g M_g\Big).$$

It follows easily from this relation that

$$(M)\wedge(S) \vdash \sum_{g\in G} E_g M_g \approx \sum_{g\in G}\left(a_g + \sum_{uv=g} E_u a_v\right) M_g.$$

Applying the vector u to the two members of this relation, we obtain

$$\begin{aligned}(M)\wedge(S) &\vdash E = \sum_{g\in G} E_g \approx \sum_{g\in G}\left(a_g + \sum_{uv=g} E_u a_v\right) = A_G + EA_G \\ &\vdash 1+E \approx 1+(1+E)A_G. \qquad (1)\end{aligned}$$

We can now apply the rule $(\mathcal{SA})$ to $1+E$. It follows immediately that

$$(M)\wedge(S) \vdash^{(\mathcal{SA})} 1+E \approx A_G^* \vdash A_G + E.A_G \approx A_G^+ \vdash^{(M),(S)} E \approx A_G^+,$$

the last deduction coming from (1). It is now easy to obtain (0). Therefore, our proposition is proved. □

As an immediate consequence of Proposition 15.8, we have the following result which solves positively Salomaa's conjecture recalled above.

Corollary 15.9. *The two following systems are complete systems of rules*:

$$(M),(S),(\mathcal{S}1) \quad \textit{and} \quad (M),(S),(\mathcal{SA}).$$

Note. Observe that proposition 15.8 proves also with a new method that (M), (S), $(\mathcal{S})$ is a complete system of rules.

The result we obtained above allows us to show the completeness of weakened versions of Salomaa's unitary meta-rule. First, let us give the following result which follows easily from Propositions 2.10 and 15.8.

Proposition 15.10. *Let us consider the two-following meta-rules*:

$$\forall E, F \in \mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle, \quad \begin{cases} E \approx FE+1 \\ c(F)=0 \end{cases} \Rightarrow E \geqslant F^*, \quad (\mathcal{S}1\geqslant)$$

$$\forall A, \forall E \in \mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle, \quad E \approx 1+A.E \Rightarrow E \geqslant A^*. \quad (\mathcal{SA}\geqslant)$$

Then, we have the deductions

$$(\mathcal{S}1\geqslant) \vdash^{(M),(S)} (\mathcal{SA}\geqslant) \vdash^{(M),(S)} (\mathcal{SA}).$$

Note. The reader will easily check the consistency of $(\mathcal{S}1\geqslant)$ and of $(\mathcal{SA}\geqslant)$.

The following result now follows clearly from Proposition 15.10 and Corollary 15.9.

Corollary 15.11. *The following systems are complete systems of rules for every alphabet* A:

$$(M), (S), (\mathscr{S}1\geqslant) \quad \textit{and} \quad (M), (S), (\mathscr{S}1\mathscr{A}\geqslant).$$

15.4. Boffa's meta-rule

Boffa introduced in [3] the following very simple meta-rule.

Definition 15.6. Let A be an alphabet. Then, we call *Boffa's meta-rule* the deduction rule, denoted $(\mathscr{B}\ell)$, which is defined by

$$\forall E \in \mathscr{C}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle, \quad E^2 \approx E \;\Rightarrow\; E^* \approx 1 + E.$$

Boffa related his meta-rule with Salomaa's and Conway's meta-rules by the following result proved in [3].

Theorem 15.12 (Boffa [3]). *Let $\mathscr{G}$ be the class of finite groups. Then, we have the following sequence of deductions*:

$$(\mathscr{S}) \vdash (\mathscr{S}1) \overset{(M),(S)}{\vdash\!\!\!-\!\!\!-} (\mathscr{B}\ell) \overset{(M),(S)}{\vdash\!\!\!-\!\!\!-} (\mathscr{R}(G))_{G\in\mathscr{G}}.$$

Therefore, the following corollary follows immediately from this theorem.

Corollary 15.13. *The following system is a complete system of rules for every alphabet* A:

$$(M), (S), (\mathscr{B}\ell).$$

Note. It follows also from Theorem 15.12 that (M), (S), $(\mathscr{S}1)$ is complete.

15.5. Commutation meta-rules

We present here other complete systems of rules that Conway introduced in [7, pp. 103–108] where their completeness was claimed, but not proved.

Definition 15.7. Let A be an alphabet. We shall call *commutation meta-rules* the following deduction rules:

($\mathscr{C}0$) $\forall E, F, G \in \mathscr{C}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle$, $EF = FG \;\Rightarrow\; E^*F = FG^*$,
($\mathscr{C}1\ell$) $\forall E, F, G \in \mathscr{C}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle$, $EF \leqslant FG \;\Rightarrow\; E^*F \leqslant EF^*$,
($\mathscr{C}1\mathrm{r}$) $\forall E, F, G \in \mathscr{C}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle$, $EF \geqslant FG \;\Rightarrow\; E^*F \geqslant FG^*$,
($\mathscr{C}2\ell$) $\forall E, F \in \mathscr{C}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle$, $EF = F \;\Rightarrow\; E^*F = F$,

$$(\mathscr{C}2\mathrm{r})\ \forall E, F \in \mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle,\quad EF = E \Rightarrow EF^* = E,$$
$$(\mathscr{C}3\ell)\ \forall E, F \in \mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle,\quad EF \leqslant F \Rightarrow E^*F \leqslant F,$$
$$(\mathscr{C}3\mathrm{r})\ \forall E, F \in \mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle,\quad EF \geqslant E \Rightarrow EF^* \geqslant E.$$

Note. The reader will easily check that all these rules are consistent.

Proposition 15.14. *Let A be an alphabet. Then, for every $i \in [1, 3]$, we have*

$$(\mathscr{C}0) \overset{(M)}{\vdash\!\!\!-\!\!\!-} (\mathscr{B}\ell), \qquad (\mathscr{C}i\ell) \overset{(M)}{\vdash\!\!\!-\!\!\!-} (\mathscr{B}\ell) \quad \textit{and} \quad (\mathscr{C}i\mathrm{r}) \overset{(M)}{\vdash\!\!\!-\!\!\!-} (\mathscr{B}\ell).$$

Proof. $(\mathscr{C}0)$ implies clearly $(\mathscr{B}\ell)$ since we have for every E in $\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle$,

$$E^2 \approx E \overset{(\mathscr{C}0)}{\vdash\!\!\!-\!\!\!-} E^*.E \approx E.1^* = E \overset{(M)}{\vdash\!\!\!-\!\!\!-} E^* \approx 1 + E^*.E \approx 1 + E.$$

The same method can be used to prove our result for $(\mathscr{C}2\ell)$ and $(\mathscr{C}2\mathrm{r})$. Let us now show that $(\mathscr{C}1\ell)$ implies $(\mathscr{B}\ell)$. For every E in $\mathscr{E}_{\mathscr{B}}\mathscr{R}\mathrm{at}\langle A\rangle$, we have

$$E^2 \approx E \vdash\!\!\!-\!\!\!- E.E \leqslant E.1 \overset{(\mathscr{C}1\ell)}{\vdash\!\!\!-\!\!\!-} E^*.E \leqslant E.1^* = E$$

$$\overset{(M)}{\vdash\!\!\!-\!\!\!-} E^* \approx 1 + E^*.E \leqslant 1 + E.$$

But, using two times (M), we clearly have

$$(M) \vdash E^* \geqslant 1 + E.$$

It follows immediately that

$$E^2 \approx E \overset{(\mathscr{C}1\ell),(M)}{\vdash\!\!\!-\!\!\!-} E^* \approx 1 + E.$$

Hence, $(\mathscr{C}1\ell)$ implies $(\mathscr{B}\ell)$ modulo (M). The same argument can also be applied with $(\mathscr{C}1\mathrm{r})$, $(\mathscr{C}3\mathrm{r})$ and $(\mathscr{C}3\ell)$. □

Corollary 15.15. *All the systems that follow are complete systems of rules for every alphabet A:*

$(M), (S), (\mathscr{C}0)$; $(M), (S), (\mathscr{C}1\ell)$; $(M), (S), (\mathscr{C}1\mathrm{r})$;
$(M), (S), (\mathscr{C}2\ell)$; $(M), (S), (\mathscr{C}2\mathrm{r})$; $(M), (S), (\mathscr{C}3\ell)$;
$(M), (S), (\mathscr{C}3\mathrm{r})$.

Proof. Our result follows immediately from Proposition 15.14 and Corollary 15.13. □

15.6. Iteration meta-rule

We shall end this section by considering a rule which was studied by Conway (see [7, p. 102]) and by Salomaa [23].

Definition 15.8. Let A be an alphabet. We call *iteration meta-rule*, and we shall denote by $(\mathcal{I}t)$ the following deduction rule:

$$\forall E, F, G, H \in \mathscr{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle, \quad [\forall n \in \mathbb{N}, EF^nG \leqslant H] \Rightarrow EF^*G \leqslant H.$$

Note. The consistency of this rule is clear.

Proposition 15.16. *Let A be an alphabet. Then, we have* $(\mathcal{I}t) \overset{(M)}{\vdash\!\!\!-\!\!\!-} (\mathcal{B}\mathcal{f})$.

Proof. We have for every E in $\mathscr{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle$,

$$E^2 \approx E \vdash (E.E^n.1 \approx E \leqslant E)_{n\geqslant 0} \overset{(\mathcal{I}t)}{\vdash\!\!\!-\!\!\!-} E.E^* \leqslant E.$$

The proposition now follows using the same argument as in Proposition 15.14. □

Corollary 15.17. *The following system is a complete system of rules for every alphabet A:*

$$(M), (S), (\mathcal{I}t).$$

Proof. It is an immediate consequence of Proposition 15.16 and Corollary 15.13. □

Note. For every rational expression E, let us denote by $n(E)$ the number of letters appearing in E, counting each letter each time it occurs in E. Let us now define for every E in $\mathscr{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle$:

$$M(E) = 2^{n(E)} + 2.$$

Then, the following rule is consistent (see [13] for instance):

$$\forall E, F, G, H \in \mathscr{E}_{\mathcal{B}}\mathcal{R}\mathrm{at}\langle A\rangle, \quad [\forall n \leqslant M(D), EF^nG \leqslant H] \Rightarrow EF^*G \leqslant H.$$

The proof of Proposition 15.16 now permits us to show that (M), (S) and this rule forms a complete system of rules.

16. Independence of group identities

16.1. Conway's model

We will first recall the construction of a model which was introduced by Conway (see [7, pp. 117, 118]). It will allow us to solve several questions of independence for rational identities associated with groups. Therefore let us consider a finite group G and a family $\mathcal{F}$ of subgroups of G *containing both* $\{1\}$ *and* $\emptyset$. Furthermore, let $G_\infty = G \cup \{\infty\}$ be the semigroup obtained by adding to G an absorbing element ∞. We can now give the following definition.

Definition 16.1. We shall call *Conway's model*, associated with the group G and with the family $\mathcal{F}$, the $\mathcal{B}$-$*$-bound-algebra $M_{\mathcal{F}}(G)$ defined by

$$M_{\mathcal{F}}(G) = (\mathcal{P}(G_\infty), \cup, \times_{,\cdot_{\mathcal{B}}}, *),$$

where the addition is the union, the product is defined by

$$\forall A, B \in \mathcal{P}(G_\infty), \quad A.B = \{a.b, a \in A, b \in B\}$$

and where the star operation is defined by

$$\begin{cases} A^* = \langle A \rangle, & \text{if } \langle A \rangle \in \mathcal{F}, \\ A^* = \langle A \rangle \cup \{\infty\}, & \text{otherwise,} \end{cases}$$

where $\langle A \rangle$ denotes the submonoid of G_∞ generated by A.

Notes. (1) Since, by convention, $\langle \emptyset \rangle = \{1\}$, the reader will easily check that $M_{\mathcal{F}}(G)$ is really a $\mathcal{B}$-$*$-bound-algebra.

(2) For every subset A of G_∞, $\langle A \rangle$ is either a subgroup of G, or the union of a subgroup of G with ∞.

Lemma 16.1. *Let G, H be finite groups, let $\mathcal{F}$ be a family of subgroups of G containing $\{1\}$ and $\emptyset$ and let $(A_h)_{h \in H}$ be a family in $M_{\mathcal{F}}(G)$ such that*

$$A_1^* = A_1 \quad \text{and} \quad \forall u, v \in H, \quad A_u A_v \subset A_{uv} \tag{$*$}$$

Then, the subset A of G defined by

$$\bigcup_{h \in H} A_h = A$$

is either the union of a subgroup of G and of ∞, or a subgroup of G, according as ∞ belongs to some A_h or not.

Proof. Let $(A_h)_{h \in H}$ be a family of subsets of G which satisfies $(*)$. Then, if $\infty \notin A_1$, it follows from Definition 16.1 that we have

$$A_1^* = A_1 \Rightarrow A_1 = \langle A_1 \rangle.$$

Hence, A_1 is a subgroup of G belonging to $\mathcal{F}$. It follows that $1 \in A_1$ and hence that $1 \in A$. Conversely, if $\infty \in A_1$, we have

$$A_1^* = A_1 \Rightarrow A_1 = \langle A_1 \rangle \cup \{\infty\}$$

by Definition 16.1. It follows also that 1 belongs to A_1 and hence to A. Moreover, we clearly have

$$A.A = \bigcup_{u,v \in H} A_u A_v \subset \bigcup_{u,v \in H} A_{uv} \subset A.$$

Thus, A is stable for the product of G_∞ and contains 1: hence, A is clearly a submonoid of G_∞. It is now straightforward to conclude. □

Proposition 16.2. *Let G, H be finite groups, let $\mathcal{F}$ be a family of subgroups of G containing both $\{1\}$ and $\emptyset$ and let $(A_h)_{h\in H}$ be a family of elements of $\mathcal{P}(G)\subset M_{\mathcal{F}}(G)$ that satisfies*

$$A_1^* = A_1 \quad \text{and} \quad \forall u, v \in H, \quad A_u A_v \subset A_{uv} \tag{*}$$

Then, the subset $A\subset G$ defined by

$$\bigcup_{h\in H} A_h = A$$

is a subgroup of G. Moreover, A_1 is a normal subgroup of A which belongs to the family $\mathcal{F}$ and the quotient group A/A_1 divides H[11], i.e.

$$A_1 \in \mathcal{F}, \quad A_1 \lhd A \quad \text{and} \quad A/A_1 < H.$$

Proof. Let $(A_h)_{h\in H}$ be a family of subsets of G which satisfies (*). It follows from Lemma 16.1 and from its proof that A and A_1 are subgroups of G and that A_1 belongs to $\mathcal{F}$. This point being proved, we can introduce

$$NE = \{h \in H, A_h \neq \emptyset\}.$$

Since A_1 is a subgroup of G, $1 \in NE$. We also have for every u, v in NE,

$$\emptyset \neq A_u A_v \subset A_{uv} \Rightarrow A_{uv} \neq \emptyset \Rightarrow uv \in NE.$$

Hence, NE is in fact a subgroup of H. Now let us show that we have

$$\forall u, v \in NE, \quad |A_u| = |A_v|. \tag{1}$$

Indeed, let u, v be in NE. Therefore, we clearly have $|A_u A_{u^{-1}v}| \geqslant |A_u|$ since the subsets A_u and $A_{u^{-1}v}$ of G are not empty. But we also have

$$A_u A_{u^{-1}v} \subset A_v \Rightarrow |A_u A_{u^{-1}v}| \leqslant |A_v|.$$

Thus, by symmetry, relation (1) follows easily from the two last inequalities. Now let us prove that

$$\forall u, v \in NE, \quad A_u A_v = A_{uv}. \tag{2}$$

Let us consider u, v in NE. According to (*), we have $A_u A_v \subset A_{uv}$. But, it follows also from (1) that $|A_{uv}| = |A_u| \leqslant |A_u A_v|$. This inequality, joined with the previous inclusion, shows that we have $A_{uv} = A_u A_v$. Hence, relation (2) is proved. Let us now show that we have

$$\forall a \in A, \quad a \in A_u \Rightarrow a^{-1} \in A_{u^{-1}}. \tag{3}$$

For every a in A, let us denote by φ_a the mapping from A into A defined by

$$\begin{aligned} \varphi_a : A &\to A \\ h &\to ha. \end{aligned}$$

[11] That is, A/A_1 is a quotient group of a subgroup of H.

Let $a \in A$ and let $u \in NE$ such that $a \in A_u$. According to (1) and (2), φ_a clearly induces a bijection from A_{u^i} onto $A_{u^{i+1}}$ for every $i \geqslant 0$. It follows that

$$\forall i \geqslant 0, \quad A_{u^{i+1}} = \varphi_a(A_{u^i}) = (\varphi_a)^{i+1}(A_1) = \varphi_{a^{i+1}}(A_1).$$

Then, if n denotes the order of a, we necessarily have

$$A_{u^n} = \varphi_{a^n}(A_1) = \varphi_1(A_1) = A_1.$$

It now follows from (2) that we have

$$A_{u^{n-1}} = A_{u^n} A_{u^{-1}} = A_1 A_{u^{-1}} = A_{u^{-1}}.$$

Using (2), we can write

$$a^{-1} = a^{n-1} \in (A_u)^{n-1} = A_{u^{n-1}} = A_{u^{-1}}.$$

Hence, (3) is shown. This point being proved, we can now easily show that A_1 is a normal subgroup of A. Indeed, for every a in A, let us consider u in NE such that $a \in A_u$. Therefore, we have according to (3) and (2),

$$a A_1 a^{-1} \subset A_u A_1 A_{u^{-1}} = A_{u1u^{-1}} = A_1.$$

Hence, we have proved that $A_1 \lhd A$. In order to conclude, let us now show that

$$\forall u, v \in NE, \quad A_u \neq A_v \Rightarrow A_u \cap A_v = \emptyset. \tag{4}$$

Indeed, let us suppose that there exists $x \in A_u \cap A_v$ with $u, v \in NE$. Then, using φ_x, it follows easily from (1) and (2) that we have for every z in A_v,

$$\varphi_x(A_u) = A_{uv} = A_u A_v \Rightarrow xz \in A_u A_v = \varphi_x(A_u).$$

Therefore, there exists t in A_u such that $xz = tx$. It follows that

$$z = x^{-1} t x \in A_{v^{-1}} A_v A_u = A_u,$$

according to (3) and (2). Thus, we have proved that $A_v \subset A_u$. The symmetry of the problem implies the equality. Hence, relation (4) is proved.

Let us introduce the group U formed with the *sets* belonging to the family $(A_u)_{u \in NE}$ and equipped with the product defined by (2). Let us also denote by Φ the mapping which associates to every $a \in A$ the unique subset A_u of A which contains a. According to (4), this mapping is well defined and it is clearly a group morphism of kernel A_1. Thus, it follows that $A/A_1 \simeq U$.

Let us also denote by Ψ the mapping of NE into U which associates to every $u \in NE$ the corresponding element A_u of U. Relation (2) shows that Ψ is a group morphism. Since Ψ is a surjection, it follows that $U \simeq NE/\mathrm{Ker}\ \Psi$. Therefore, the two last relations prove that A/A_1 is isomorphic to a quotient of the subgroup NE of H, i.e. that A/A_1 divides H. Hence, this ends our proof. □

We shall now use Proposition 16.2 in order to obtain some properties of Conway's model. At first, we shall study under which conditions on $\mathscr{F}$, Conway's model is a model for the aperiodic identities (M) and (S).

Proposition 16.3. *Let $\mathcal{F}$ be a family of subgroups of a finite group G that contains $\{1\}$ and $\emptyset$. Then, Conway's model $M_{\mathcal{F}}(G)$ is a model of the identity (S) iff $\mathcal{F}$ satisfies the following property:*

$$\forall F \in \mathcal{F}, \quad H \text{ subgroup of } F \Rightarrow H \in \mathcal{F}. \tag{$\mathcal{S}$}$$

Proof. First, let us suppose the property $(\mathcal{S})$ is satisfied. Then, let A, B be in $M_{\mathcal{F}}(G)$. If A or B is empty or contains ∞, we can easily check that

$$(A \cup B)^* = (A^*B)^*A^*. \tag{σ}$$

Therefore, we must only prove that (σ) is true when A and B do not contain ∞ and are not empty, in order to show that $M_{\mathcal{F}}(G)$ is a model for (S). From now on, let us suppose that these conditions hold. Then, let us show that

$$\langle A \cup B\rangle = \langle\langle A\rangle B\rangle. \tag{1}$$

We clearly have $\langle\langle A\rangle B\rangle \subset \langle A \cup B\rangle$. Conversely, since we clearly have $B \subset \langle\langle A\rangle B\rangle$, it suffices to prove that $A \subset \langle\langle A\rangle B\rangle$ in order to obtain the other inclusion. But this last relation is true since we can write for every a in B,

$$a = abb^{-1} \in AB\langle B\rangle \subset \langle\langle A\rangle B\rangle, \quad \text{where } b \in B.$$

Therefore, (1) is proved. Let us suppose now that $\langle A \cup B\rangle \in \mathcal{F}$. Then, according to (1), $\langle\langle A\rangle B\rangle \in \mathcal{F}$. It follows from $(\mathcal{S})$ that $\langle A\rangle \in \mathcal{F}$. Thus we have

$$(A \cup B)^* = \langle A \cup B\rangle = \langle\langle A\rangle B\rangle\langle A\rangle = (A^*B)^*A^*.$$

Conversely, if $\langle A \cup B\rangle \notin \mathcal{F}$, it follows from (1) that $\langle\langle A\rangle B\rangle \notin \mathcal{F}$. Hence, we have

$$(A \cup B)^* = \langle A \cup B\rangle \cup \{\infty\} = (\langle\langle A\rangle B\rangle \cup \{\infty\})\langle A\rangle = (A^*B)^*A^*$$

in all cases. Therefore, these two last relations prove that $M_{\mathcal{F}}(G)$ is a model for (S). Conversely, let us suppose that $M_{\mathcal{F}}(G)$ is a model for (S) and that $(\mathcal{S})$ is not satisfied. Hence, there would exist a group H of $\mathcal{F}$ which has a subgroup $A \notin \mathcal{F}$. Then, we would have

$$\begin{aligned}(A \cup H)^* = H^* = \langle H\rangle \neq (A^*H)^*A^* &= [\langle(\langle A\rangle \cup \{\infty\})H\rangle \cup \{\infty\}](\langle A\rangle \cup \{\infty\}) \\ &= \langle H\rangle \cup \{\infty\}.\end{aligned}$$

Hence, $M_{\mathcal{F}}(G)$ is not a model for (S). This contradiction shows that $(\mathcal{S})$ must be satisfied. Thus, this ends our proof. □

Note. In other terms, $M_{\mathcal{F}}(G)$ is a model for (S) iff $\mathcal{F}$ is stable by subgroups.

Proposition 16.4. *Let $\mathcal{F}$ be a family of subgroups of a finite group G that contains $\{1\}$ and $\emptyset$. Then, Conway's model $M_{\mathcal{F}}(G)$ is a model of the identity (M) iff $\mathcal{F}$ satisfies the following property:*

$$\forall g \in G, \quad H \in \mathcal{F} \Rightarrow gHg^{-1} \in \mathcal{F}. \tag{$\mathcal{M}$}$$

Proof. First, let us suppose that the property $(\mathcal{M})$ is satisfied. Then, let A, B be in $M_{\mathcal{F}}(G)$. If A or B is empty or contains ∞, we can easily check that

$$(AB)^* = \{1\} \cup A(BA)^*B. \qquad (\mathcal{m})$$

Hence, we just have to prove that $(\mathcal{m})$ is true when A and B do not contain ∞ and are not empty, in order to show that $M_{\mathcal{F}}(G)$ is a model for (M). From now on, let us suppose that these conditions hold for A, B. Then, let us show that

$$\forall a \in A, \quad \langle AB \rangle = a\langle BA \rangle a^{-1}. \qquad (1)$$

Let $a \in A$. Then, we can write, for every $\alpha \in A$ and every $\beta \in B$,

$$a(\beta\alpha)a^{-1} = (a\beta)(\alpha\beta)(a\beta)^{-1} \in \langle AB \rangle.$$

It follows that we have

$$a\,BA\,a^{-1} \subset \langle AB \rangle \Rightarrow \langle a\,BA\,a^{-1} \rangle = a\langle BA \rangle a^{-1} \subset \langle AB \rangle. \qquad (2)$$

Since the mapping which associates axa^{-1} to x is a bijection, it follows from (2) that $|\langle BA \rangle| \leqslant |\langle AB \rangle|$. Hence, $|\langle AB \rangle| = |\langle BA \rangle|$ by symmetry. It now follows from (2) that $\langle AB \rangle = a\langle BA \rangle a^{-1}$, i.e. that (1) holds. This point being proved, we can show that $M_{\mathcal{F}}(G)$ is a model for (M). Indeed, let us suppose that $\langle AB \rangle$ belongs to $\mathcal{F}$. Then, according to (1) and to $(\mathcal{M})$, $\langle BA \rangle \in \mathcal{F}$. Thus, we have

$$(AB)^* = \langle AB \rangle = \{1\} \cup A\langle BA \rangle B = \{1\} \cup A(BA)^*B.$$

Conversely, if $\langle AB \rangle \notin \mathcal{F}$, $\langle BA \rangle \notin \mathcal{F}$ according to (1) and to $(\mathcal{M})$. Then, we can easily check that we have

$$(AB)^* = \langle AB \rangle \cup \{\infty\} = \{1\} \cup A(\langle BA \rangle \cup \{\infty\})B = \{1\} \cup A(BA)^*B.$$

Thus, $(\mathcal{m})$ is always satisfied and $M_{\mathcal{F}}(G)$ is really a model of (M). Conversely, let us suppose that $M_{\mathcal{F}}(G)$ is a model of (M), but that $(\mathcal{M})$ is not satisfied. Therefore, there would exist $H \in \mathcal{F}$ and $g \in G$ such that $gHg^{-1} \notin \mathcal{F}$. Let us now define $A = gG$ and $B = \{g^{-1}\}$. With these notations, we would have

$$(AB)^* = (gGg^{-1})^* = \langle gGg^{-1} \rangle \cup \{\infty\} = gGg^{-1} \cup \{\infty\},$$

$$\{1\} \cup A(BA)^*B = \{1\} \cup gG\langle G \rangle g^{-1} = \{1\} \cup gGg^{-1}.$$

It follows that $(\mathcal{m})$ is not satisfied: hence, $M_{\mathcal{F}}(G)$ is not a model of (M). This contradiction ensures that the property $(\mathcal{M})$ is true if $M_{\mathcal{F}}(G)$ is a model for (M). Therefore, our proposition is proved. □

Notes. (1) Thus, $M_{\mathcal{F}}(G)$ is a model of (M) iff $\mathcal{F}$ is stable by conjugation.

(2) $(\mathcal{M})$ can also be equivalently given as an equivalence.

Proposition 16.5 (Conway [7, p. 117]). *Let G be a finite group, let H be a subgroup of G and let $\mathcal{F}$ be a family of subgroups of G that contains $\emptyset$ and $\{1\}$ but not H and*

which satisfies the properties $(\mathcal{S})$ *and* $(\mathcal{M})$ *of Propositions* 16.3 *and* 16.4. *Then, Conway's model* $M_{\mathcal{F}}(G)$ *is not a model for the identity* $P(H)$.

Proof. Since $M_{\mathcal{F}}(G)$ is here a model for (M) and (S) according to Propositions 16.3 and 16.4, it suffices by Corollary 15.6 and Proposition 2.6 to see that $M_{\mathcal{F}}(G)$ is not a model of $\mathcal{R}(H)$. Let us now consider the family $(A_h)_{h\in H}$ defined by $A_h = \{h\}$ for every h in H. Then, according to the hypotheses, we clearly have

$$\forall g, h \in H, \quad A_g A_h = A_{gh} \subset A_{gh} \quad \text{and} \quad A_1^* = \{1\}^* = \{1\} = A_1.$$

But, we also have

$$\bigcup_{h\in H} A_h = H \notin \mathcal{F} \Rightarrow \left(\bigcup_{h\in H} A_h\right)^* = H \cup \{\infty\} \neq H.$$

It immediately follows that $M_{\mathcal{F}}(G)$ is not a model for the rule $\mathcal{R}(H)$. □

Proposition 16.6. *Let* G *be a finite* simple *group and let us consider the family of subgroups of* G *which are different from* G:

$$\mathcal{F} = \{H \text{ subgroup of } G,\ H \neq G\} \cup \{\emptyset\}.$$

Then, Conway's model $M_{\mathcal{F}}(G)$ *is a model for* (M) *and* (S). *Moreover, when* H *is a group,* $M_{\mathcal{F}}(G)$ *is a model of the group identity* $P(H)$ *iff* G *does not divide* H.

Proof. It follows clearly from Propositions 16.3 and 16.4 that $M_{\mathcal{F}}(G)$ is a model for (M) and (S). Let H be a finite group. Then, we can now study if $M_{\mathcal{F}}(G)$ is a model for the identity $P(H)$, since it is only defined modulo (M) and (S). According to Proposition 2.6 and Corollary 15.6, it suffices to see that $M_{\mathcal{F}}(G)$ is a model for the rule $\mathcal{R}(H)$ iff G does not divide H, in order to show our result. Hence, let us suppose now that H is not divided by G and let $(A_h)_{h\in H}$ be a family of elements of $M_{\mathcal{F}}(G)$ which satisfies the premises of $\mathcal{R}(H)$. Observe that $\leqslant$ becomes the inclusion in the sense of $M_{\mathcal{F}}(G)$. Thus, we have

$$\forall u, v \in H, \quad A_u A_v \subset A_{uv} \quad \text{and} \quad A_1^* = A_1.$$

Then, according to Lemma 16.1, the element A defined by

$$A = \sum_{h\in H} A_h = \bigcup_{h\in H} A_h$$

is a submonoid of G_∞. It follows that $A = \langle A\rangle$. Let us now show that $A = A^*$. First, if some A_h contains ∞, we have

$$A^* = \langle A\rangle \cup \{\infty\} = A. \tag{1}$$

Secondly, if no A_h contains ∞ and if $\langle A\rangle = A \in \mathcal{F}$, we have

$$A^* = \langle A\rangle = A. \tag{2}$$

Finally, if no A_h contains ∞ and if $\langle A\rangle = A \notin \mathscr{F}$, it follows that $A = G$ by definition of $\mathscr{F}$. Then, according to Proposition 16.2, A_1 is a subgroup of G in $\mathscr{F}$ and $A_1 \lhd A$. Since G is simple, it follows that $A_1 = \{1\}$. But Proposition 16.2 says also that A/A_1 divides H: it follows here that $G < H$. But, this last situation is in contradiction with our hypothesis. Hence, we always have $A^* = A$; i.e.,

$$\left(\sum_{h\in H} A_h\right)^* = \sum_{h\in H} A_h.$$

Thus, $M_{\mathscr{F}}(G)$ is a model for $\mathscr{R}(H)$. Conversely, let us suppose that $M_{\mathscr{F}}(G)$ is a model for the rule $\mathscr{R}(H)$ associated with a finite group H. If $G < H$, $M_{\mathscr{F}}(G)$ is a model for $\mathscr{R}(G)$ according to Corollaries 15.6, 12.11 and Proposition 2.6. But, since G does not belong to $\mathscr{F}$, $M_{\mathscr{F}}(G)$ is not a model of $\mathscr{R}(G)$ according to Proposition 16.5. This contradiction implies that G does not divide H when $M_{\mathscr{F}}(G)$ is a model of $\mathscr{R}(H)$. Therefore, our proposition is proved. □

Proposition 16.7 (Conway [7, p. 117]). *Let G be a finite group and let us consider the family $\mathscr{F}$ of all soluble subgroups of G:*

$$\mathscr{F} = \{H \text{ subgroup of } G,\ H \text{ soluble}\} \cup \{\emptyset\}.$$

Then, Conway's model $M_{\mathscr{F}}(G)$ is a model for (M) and (S). Moreover it is a model for every group identity $P(H)$ associated with a finite soluble *group H.*

Proof. It follows clearly from Propositions 16.3 and 16.4 that $M_{\mathscr{F}}(G)$ is a model for (M) and (S). According to Corollary 15.6 and Proposition 2.6, it suffices to show that $M_{\mathscr{F}}(G)$ is a model for the rule $\mathscr{R}(H)$ when H is soluble in order to prove our proposition. Then, let H be a soluble group and let $(A_h)_{h\in H}$ be a family of elements of $M_{\mathscr{F}}(G)$ which satisfies the premises of $\mathscr{R}(G)$. Then, arguing as in Proposition 16.6, we can show that, if we define A by

$$A = \bigcup_{h\in H} A_h,$$

we will have $A^* = A$, except possibly if we have $A = \langle A\rangle \notin \mathscr{F}$ and if each A_h does not contain ∞. In this case, Proposition 16.2 shows that A_1 is a normal subgroup of A belonging to $\mathscr{F}$ and that A/A_1 divides H. hence, according to the definition of $\mathscr{F}$, A_1 is a soluble subgroup of G. Moreover, since H is soluble, A/A_1 is also soluble (see [4, Chap. 1, Section 6.4]). Thus, A_1 and A/A_1 are soluble groups. It follows that A is soluble (see [4, Chap. 1, Section 6.4]). But, this is not possible since $A \notin \mathscr{F}$ here. Therefore, we always have $A = A^*$. In other words, $M_{\mathscr{F}}(G)$ is a model for the rule $\mathscr{R}(H)$ when H is a soluble group. □

Let us recall finally the following result of Conway (cf. [7, p. 118]) which corresponds to the particular case of $\mathfrak{S}_n$.

Proposition 16.8. *Let $n \geqslant 5$. Let us consider the following family $\mathcal{F}$ formed of the subgroups of $\mathfrak{S}_n$ which are distinct from $\mathfrak{G}_n$ and $\mathfrak{A}_n$:*

$$\mathcal{F} = \{G \text{ subgroup of } \mathfrak{S}_n,\ G \neq \mathfrak{S}_n,\ G \neq \mathfrak{A}_n\} \cup \{\emptyset\}.$$

Then, Conway's model $M_{\mathcal{F}}(\mathfrak{S}_n)$ is a model for (S) and (M). Moreover, when H is a finite group, $M_{\mathcal{F}}(\mathfrak{S}_n)$ is a model for the group identity $P(H)$ iff $\mathfrak{S}_n$ and $\mathfrak{A}_n$ do not divide H. Finally, $M_{\mathcal{F}}(\mathfrak{S}_n)$ is not a model of $R(n)$.

Proof. The fact that $M_{\mathcal{F}}(\mathfrak{S}_n)$ is a model of (M), (S) and the characterization of the groups H for which $M_{\mathcal{F}}(\mathfrak{S}_n)$ is a model can be proved as in Proposition 16.6 with some obvious modifications. In order to show that $\mathfrak{S}_n$ is not a model for $R(n)$, it suffices to consider $A = \{\rho\}$ and $B = \{\sigma\}$ where ρ and σ denote the generating system of $\mathfrak{S}_n$ introduced in Section 14. Then, arguing as in the proof of Theorem 8, Chap. 13 of [7], we can check that the identity $R(n)$ is not satisfied in $M_{\mathcal{F}}(\mathfrak{S}_n)$. □

Note. A substantial part of the previous result is contained in Theorem 8, Chap. 13 of [7]. Here, the only original result is in fact the characterization of the groups H such that $M_{\mathcal{F}}(\mathfrak{S}_n)$ is a model for $P(H)$.

16.2. Independence of group identities

We can now use the results that we showed in the last section, in order to prove independence results for group identities.

Proposition 16.9. *Let G be a finite* simple *group and let us denote by $\mathcal{ND}$ the family of the groups that G does not divide. Then, the identity $P(G)$ is independent of the system*

$$(M), (S), (P(H))_{H \in \mathcal{ND}}.$$

Proof. It is an immediate consequence of Propositions 16.6 and 2.6. □

Corollary 16.10. *Let G be a finite non-commutative* simple *group. Then, the identity $P(G)$ is independent of the following system:*

$$(M), (S), (P(p))_{p \in \mathcal{P}}.$$

Proof. Observe that if G divided $\mathbb{Z}/p\mathbb{Z}$ for some prime integer p, G would be commutative. Our result now easily follows from Proposition 16.9 and Theorem 14.5. □

Corollary 16.11. *Let $n \geqslant 5$. Then, the identity $P(\mathfrak{U}_n)$ is independent from the following system:*

$$(M), (S), P(\mathfrak{U}_{n-1}), (P(p))_{p \in \mathcal{P}}.$$

Proof. The argument given in Corollary 16.10 shows that $\mathfrak{U}_n$ does not divide $\mathbb{Z}/p\mathbb{Z}$ for every prime integer p. On the other hand, $\mathfrak{U}_n$ does not divide $\mathfrak{U}_{n-1}$ since, if it were the case, we would have $|\mathfrak{A}_n| \leqslant |\mathfrak{A}_{n-1}||$. Therefore, our corollary follows from proposition 16.9 since $\mathfrak{A}_n$ is simple when $n \geqslant 5$. □

Proposition 16.12 (Conway [7, p. 118]). *Let $n \geqslant 5$. Then, the identity $R(n)$ is independent from the following system:*

$$(M), (S), P(\mathfrak{S}_{n-1}), (P(p))_{p\in\mathscr{P}}.$$

Proof. With the arguments given for $\mathfrak{A}_n$, we can also prove that $\mathfrak{S}_n$ and $\mathfrak{A}_n$ divide neither $\mathfrak{S}_{n-1}$, nor any cyclic commutative group when $n \geqslant 5$. Hence, it follows now from Propositions 16.8 and 2.6 that $R(n)$ is independent from

$$(M), (S), P(\mathfrak{S}_{n-1}), (P(\mathbb{Z}/p\mathbb{Z}))_{p\in\mathscr{P}}.$$

Then, the corollary follows immediately from Theorem 14.5. □

Note. The independence of $R(n)$ with $P(\mathfrak{S}_{n-1})$ was not shown in [7].

Corollary 16.13. *Let $n \geqslant 5$. Then, the identity $R(n)$ is independent of the following system:*

$$(M), (S), (R(m))_{m<n}, (P(p))_{p\in\mathscr{P}}.$$

Proof. It follows from the proof of Corollary 14.4, from Corollary 12.2 and from Proposition 6.2 that we have

$$P(\mathfrak{S}_{n-1}) \overset{(M),(S)}{\longmapsto} (P(\mathfrak{S}_m, \{\sigma, \rho\}))_{m<n} \overset{(M),(S)}{\longmapsto} (R(m))_{m<n}.$$

Then, it is easy to adapt the proof of Proposition 16.12 in order to deduce our corollary from Propositions 16.8 and 2.6. □

Corollary 16.14. *Let $4 \leqslant i < j$. Then, the identity $P(\mathfrak{S}_i)$ (resp. $P(\mathfrak{A}_i)$) is independent of the identity $P(\mathfrak{S}_j)$ (resp. $P(\mathfrak{A}_j)$).*

Proof. The corollary follows immediately from Corollary 16.11 and Proposition 16.12, according to the proof of Corollary 13.16 and to Corollary 13.17. □

Note. When $n = 2$, 3 or 4, the two previous corollaries are false since $\mathfrak{S}_n$ is soluble here. Therefore, according to the note following Theorem 14.5, $P(\mathfrak{S}_n)$ is then a consequence of $(P(p))_{p\in\mathscr{P}}$ and it is also the case for $R(n)$ according to Propositions 14.3, 6.2 and Corollary 12.3. More precisely, it can be shown that

$$P(2) \wedge P(3) \overset{(M),(S)}{\longmapsto} P(\mathfrak{S}_4) \overset{(M),(S)}{\longmapsto} R(4),$$

$$P(2) \wedge P(3) \overset{(M),(S)}{\vdash\!\dashv} P(\mathfrak{S}_3) \overset{(M),(S)}{\vdash\!\dashv} R(3),$$

$$P(2) \overset{(M),(S)}{\vdash\!\dashv} P(\mathfrak{S}_2) \overset{(M),(S)}{\vdash\!\dashv} R(2).$$

These results are obtained by using Jordan-Hölder sequences of $\mathfrak{S}_2$, $\mathfrak{S}_3$ and $\mathfrak{S}_4$ (see [5] for instance) and Proposition 13.11.

Let us end with two results dealing with solubles groups.

Proposition 16.15 (Conway [7, p. 117]). *Let G be a finite non-soluble group. Then the identity $P(G)$ is independent of the following system*:

$$(M), (S), (P(p))_{p \in \mathscr{P}}.$$

Proof. Our result follows easily from Propositions 16.7, 2.6 and Theorem 14.5. □

Note. According to Corollary 13.12 and Theorem 14.5, the identity associated with a non-soluble group is independent of all the identities associated with the soluble finite groups.

Proposition 16.16. *The system that follows is not a complete system of rational identities for every alphabet A with more than* two *letters*:

$$(M), (S), (P(p))_{p \in \mathscr{P}}.$$

Proof. The proposition follows from Corollary 16.13, since $R(n)$ is a two-letter identity. □

Note. This result illustrates clearly the difference between alphabets with more than two letters and alphabets with one letter. In fact, it corresponds to the difference between commutativity and non-commutativity for groups.

16.3. Non-finiteness of two-letter identities in a complete system

The following result was proved by Conway (see [7, p. 118]). We obtain it here as a consequence of our results.

Theorem 16.17 (Conway [7, p. 118]). *Let A be an alphabet formed with more than* two *letters. Then, every complete system of $\mathscr{B}$-rational identities for A has necessarily an infinite number of identities using more than two letters.*

Proof. Let us suppose that there exists a complete system $\mathscr{A}$ of $\mathscr{B}$-rational identities for A which has only a finite number of identities using more than two letters. Then, we can decompose $\mathscr{A}$ as follows:

$$\mathscr{A} = \mathscr{B} \cup ((E_i, F_i))_{i=1,n},$$

where the identities of $\mathscr{B}$ use just one letter. Since the system $(P(\mathfrak{S}_n))_{n\geqslant 2}$ is complete, there exists a finite part $I \subset \mathbb{N}$ such that

$$(P(\mathfrak{S}_i))_{i\in I} \overset{(M),(S)}{\longmapsto} (E_i \approx F_i)_{i=1,n}.$$

Then, according to Corollary 12.9, we have

$$P\left(\prod_{i\in I} \mathfrak{S}_i\right) \overset{(M),(S)}{\longmapsto} (P(\mathfrak{S}_i))_{i\in I}.$$

But, according to Cayley's theorem, the group $\prod_{i\in I} \mathfrak{S}_i$ is also a subgroup of $\mathfrak{S}_N$ for some integer N. It follows that

$$P(\mathfrak{S}_N) \overset{(M),(S)}{\longmapsto} P\left(\prod_{i\in I} \mathfrak{S}_i\right)$$

by Corollary 12.3. Thus, it is now straightforward to obtain

$$P(\mathfrak{S}_N) \overset{(M),(S)}{\longmapsto} (E_i \approx F_i)_{i=1,n}. \tag{1}$$

But, it follows from Theorem 13.19 that the system $(P(\mathbb{Z}/p\mathbb{Z}))_{p\in\mathscr{P}}$ is complete for a one-letter alphabet. Therefore, we have by (1),

$$(P(\mathbb{Z}/p\mathbb{Z}))_{p\in\mathscr{P}} \wedge P(\mathfrak{S}_N) \overset{(M),(S)}{\longmapsto} \mathscr{A}.$$

Since $\mathscr{A}$ is complete, this relation shows that the system

$$\mathscr{C} = (M), (S), (P(\mathbb{Z}/p\mathbb{Z}))_{p\in\mathscr{P}}, P(\mathfrak{S}_N)$$

is also a complete system of rational identities. But Proposition 14.12 shows that the two-letter identity $R(N+1)$ is not a consequence of the above system. Therefore, this contradiction ends our proof. □

Note. This result shows in particular that the system of identities whose completeness was conjectured in Corollary 14.4, is optimal in a certain sense. Moreover, we have also obtained a new proof of Theorem 2.4.

Acknowledgment

I want especially to thank Professor D. Perrin who proposed me to work on this beautiful subject. I thank also Professor C. Choffrut who corrected a substantial part of the English version of the present paper. Finally I must thank Professor M. Boffa for all his interest in my work and especially for the talks he permitted me to give in Mons University.

References

[1] J. Barwise, ed., *Handbook of Mathematical Logic* (North-Holland, Amsterdam, 1978).

[2] J. Berstel and C. Reutenauer, *Les Séries Formelles et leurs Langages* (Masson, Paris, 1985).

[3] M. Boffa, Une remarque sur les systèmes complets d'identités rationelles, *Theoret. Inform. Applic.* **24**(4) (1990) 419-423.

[4] N. Bourbaki, *Algèbre* (CCLS, 1981) Chap. 1-3.

[5] A. Bouvier and D. Richard, *Groupes* (Hermann, Paris, 1979).

[6] J. A. Brzozowski, Derivatives of regular expressions, *J. Assoc. Comput. Mach.*, **11**(4), (1964) 481-494.

[7] J.H. Conway, *Regular Algebras and Finite Machines* (Chapman & Hall, London, 1974).

[8] S. Eilenberg, *Automata, Languages and Machines, Vol. A* (Academic Press, New York, 1972).

[9] S. Eilenberg, *Automata, Languages and Machines, Vol. B* (Academic Press, New York, 1976).

[10] N. Jacobson, *Basic Algebra, Vol. II* (Freemann, New York, 1980).

[11] D. Krob, Expressions $\mathcal{K}$-rationnelles, Doctorat d'Université, University of Paris 7, LITP Technical Report, 88-23, 1988.

[12] D. Krob, On aperiodic semigroups, LITP Technical Report, 89-76, 1989.

[13] D. Krob, Expressions rationnelles sur un anneau: *Proc. Séminaire d'Algèbre M.P. Malliavin*, Lecture Notes in Mathematics (Springer, Berlin) to appear.

[14] D. Krob, A complete system of $\mathcal{B}$-rational identities, in: *Proc. ICALP 90*, Lecture Notes in Computer Science Vol. 443 (Springer, Berlin, 1990), 60-73.

[15] G. Lallement, *Combinatorial Semigroup Theory* (Wiley, New York, 1979).

[16] D. Perrin, Finite automata, LITP Technical Report, 89-26, 1989.

[17] J.E. Pin, *Variétés de Langages Formels* (Masson, Paris, 1985).

[18] J. Platieau, Automates finis et algèbres régulières de Kleene, Mémoire de Licence, University of Mons, 1984.

[19] V.N. Redko, On the determining totality of an algebra of regular events, *Ukrain. Mat. Z.* **16** (1964), 120-126 (in Russian).

[20] V.N. Redko, On the algebra of commutative events, *Ukrain. Mat. Z.* **16** (1964), 185-195 (in Russian).

[21] G. Renault, *Algèbre Non Commutative* (Gauthiers-Villars, Paris, 1975).

[22] J. Sakarovitch, Cours de DEA, 86-87, University of Paris VI.

[23] A. Salomaa, Two complete axiom systems for the algebra of regular events, *J. Assoc. Comput. Mach.* **13**(1) (1966) 158-169.

[24] A. Salomaa, On regular expressions and regular canonical systems, *Math. Systems Theory* **2** (1968) 341-355.

[25] M.P. Schützenberger, On finite monoids having only trivial subgroups, *Inform. and Control* **8** (1965) 190-194.

[26] J.P. Serre, *Représentation Linéaire des Groupes Finis* (Hermann, Paris, 1979).

[27] R. Tenam, *Analyse numérique*, Cours de Maitrise, 1969/70, University of Orsay.