

A complete system of identities for one-letter rational expressions with multiplicities in the tropical semiring

Agnès Bonnier-Rigny – Daniel Krob

Université de Rouen and CNRS (Institut Blaise Pascal; LITP) ¹

1 Introduction

The *tropical semiring* \mathcal{M} is the semiring $\mathbb{N} \cup \{+\infty\}$ equipped with minimum as sum and usual addition as product. This semiring which is often used in the context of the analysis of discrete event systems (cf [1] for instance), appeared initially in language theory in Simon's solution of the finite power property problem (see [16]). It was also used by Hashigushi in the same context (see [5]) and in his study of the star-height of rational languages (see [6] for instance). The tropical semiring was then strongly explored in connection with language theory (see [17] for a survey).

Among several important questions concerning \mathcal{M} was the *equality problem*. We recently solved it by proving that it is undecidable to decide whether two \mathcal{M} -rational series over an alphabet A are equal when $|A| \geq 2$ (see [12]). Hence this shows in particular that the equational theory of \mathcal{M} -rational expressions is also undecidable when A has at least two letters.

On the other hand, the equality of two \mathcal{M} -rational series over a one-letter alphabet $A = \{a\}$ is decidable (see [12, 17] for this classical result). Therefore a natural question occurs : is it possible to find a "good" complete axiomatization of the equational theory of one-letter \mathcal{M} -rational expressions ? As we will see, this paper proposes an answer to it. In fact, this question is connected to the general theory of rational identities over an arbitrary semiring that we already studied (see [8, 11]). This theory is the natural generalization of the usual theory of ordinary boolean rational identities that was studied by a lot of authors (see [3, 7, 9] for more details).

We can now recall that a complete axiomatization of usual one-letter boolean expressions, due to Redko, is known (see [3, 13] for instance). Thus this paper can be seen as the generalization of Redko's result for the tropical semiring. It is also interesting to note

¹ All correspondence should be sent to the second author : Daniel KROB - LITP - Université Paris 7 - 2, place Jussieu - 75251 Paris Cedex 05 - FRANCE; e-mail : dk@litp.ibp.fr

the reader will find among the lines of our results a new proof of Redko's theorem, using the natural embedding of the boolean semiring \mathcal{B} into \mathcal{M} .²

Hence our paper gives a new contribution to the study of the equational theory of rational expressions with multiplicities in a semiring. We finally recall that complete systems of rational identities are known in the usual boolean case (see [3, 9]) and in the ring case (see [10]). This paper proposes also such a complete axiomatization for one-letter expressions with multiplicities in the tropical semiring, which is here the maximal general case that we can consider as we already saw. It may certainly be an interesting challenge to obtain the same kind of results for other special semirings.

2 Preliminaries

2.1 The tropical semiring

The *tropical semiring* \mathcal{M} is the semiring $\mathbb{N} \cup \{+\infty\}$ equipped with addition and product defined by $x \oplus y = \min(x, y)$ and by $x \otimes y = x + y$ for every $x, y \in \mathbb{N} \cup \{+\infty\}$. Note that the units of \mathcal{M} for sum and product are respectively equal to $0_{\mathcal{M}} = +\infty$ and $1_{\mathcal{M}} = 0$. We refer to [6, 12, 17] for all details concerning \mathcal{M} . The symbols \oplus and \otimes will also be used throughout this paper to denote addition and multiplication of series with multiplicities in the tropical semiring.

2.2 \mathcal{M} -rational expressions and identities

Let A be an alphabet and let Ω be the set of functional symbols which is defined by $\Omega = \{\oplus, \otimes, *\} \cup \mathcal{M}$ where \oplus and \otimes are symbols of arity 2, where $*$ is a symbol of arity 1 and where every element of \mathcal{M} is considered as a constant. Then the *\mathcal{M} -rational expressions* are exactly the elements of the free Ω -algebra $F(A, \Omega)$ constructed over A that we quotient by the usual axioms of \mathcal{M} -algebra and by the rules

$$\forall p \in \mathcal{M}, p^* = 0$$

that connects the formal star with the real star in \mathcal{M} . In particular, the set of \mathcal{M} -rational expressions is a \mathcal{M} -algebra that we denote by $\mathcal{E}_{\mathcal{M}}\text{Rat}(A)$. We refer to [8, 11] for more details concerning the construction of this algebra.

We can now define a unique \mathcal{M} -algebra morphism ϵ that preserves stars and maps $\mathcal{E}_{\mathcal{M}}\text{Rat}(A)$ into the \mathcal{M} -algebra $\mathcal{M} \ll A \gg$, by the formulas

$$\forall a \in A, \epsilon(a) = a \in \mathcal{M} \ll A \gg .$$

In other words, ϵ is just the mapping that associates with every \mathcal{M} -rational expression the \mathcal{M} -rational series that corresponds naturally to it (see [2, 15] for more details on rational series). This leads us to the important notion of rational identity.

DEFINITION 2.1 : Let E, F be two \mathcal{M} -rational expressions. Then we say that the pair (E, F) is a *\mathcal{M} -rational identity* and we denote it by $E \approx F$ iff $\epsilon(E) = \epsilon(F)$.

² This natural embedding maps $0 \in \mathcal{B}$ onto $+\infty$ and $1 \in \mathcal{B}$ onto 0 .

Note : Hence $E \approx F$ is a rational identity iff E and F are two \mathcal{M} -rational expressions that denote the same \mathcal{M} -rational series.

DEFINITION 2.2 : Let (\mathcal{A}) be a set of \mathcal{M} -rational identities. Then a \mathcal{M} -rational identity $E \approx F$ is said to be *deducible* from (\mathcal{A}) and we denote it by

$$(\mathcal{A}) \vdash E \approx F$$

iff one can obtain the identity $E \approx F$ after a finite number of elementary deductions that consist in using an identity of (\mathcal{A}) , making a substitution in an already deduced identity or using one of the following deduction rules

$$\frac{\emptyset}{E \approx E}, \frac{E \approx F}{F \approx E}, \frac{E \approx F, F \approx G}{E \approx G}, \frac{E \approx F, G \approx H}{E \oplus G \approx F \oplus H}, \frac{E \approx F, G \approx H}{E \otimes G \approx F \otimes H}, \frac{E \approx F}{E^* \approx F^*}.$$

A system of \mathcal{M} -rational identities is then said to be *complete* iff every \mathcal{M} -rational identity is deducible from it. As we explained, the purpose of this paper is to construct such a system when A is a one-letter alphabet.

We can now give the important definition of rational inequality.

DEFINITION 2.3 : Let E, F be two \mathcal{M} -rational expressions. Then we say that we have the *\mathcal{M} -rational inequality* $E \leq F$ iff we have $F \approx E \oplus F$.

Notes : 1) As in the boolean case, it is not difficult to see that we have $E \leq F$ iff there exists a \mathcal{M} -rational expression G such that $E \oplus G \approx F$.

2) Observe that the natural order on \mathcal{M} which is used in definition 2.3 is the *opposite* of the usual order $\leq_{\mathbb{N}}$ on \mathbb{N} . Hence $E \leq F$ iff $\epsilon(E)$ is bigger than $\epsilon(F)$ in the ordering of $\mathcal{M} \ll A \gg$ induced by the usual ordering of \mathbb{N} !

As in the boolean case (cf [3] p. 36), it is easy to prove that we have

1. $E \leq F, F \leq G \vdash E \leq G,$
2. $E \leq F, F \leq E \vdash E \approx F,$
3. $E \leq F, G \leq H \vdash E \oplus G \leq F \oplus H,$
4. $E \leq F, G \leq H \vdash E \otimes G \leq F \otimes H,$
5. $(M), (S), E \leq F \vdash E^* \leq F^*$

for every \mathcal{M} -rational expressions E, F, G, H . Property 2 is important since it will be as in the boolean case the basis of our proofs by inequalities for \mathcal{M} -rational identities.

2.3 The classical axioms

Conway introduced in [3] a family of boolean identities that he called *classical axioms*. In fact, these identities are universal (see [8, 11]). In our case, they are exactly equal to the following \mathcal{M} -rational identities

$$(M) \quad (ab)^* \approx 0 \oplus a(ba)^*b \quad \text{and} \quad (S) \quad (a \oplus b)^* \approx a^*(ba^*)^*$$

together with the family of \mathcal{M} -rational identities indexed by $n \in \mathbb{N}$ and defined by

$$(P(n)) \quad a^* \approx (0 \oplus a \oplus \dots \oplus a^{n-1})(a^n)^*.$$

Classical axioms are very important since a lot of useful identities are consequences of them (cf [3] for instance). Note also that Redko's theorem (cf [3] p. 34-40) says that classical

axioms are a complete axiomatization for one-letter usual boolean rational expressions. However let us now give some results involving classical axioms in our framework.

LEMMA 2.1 : Let $i \in \mathbb{N}$ and let $p \in \mathcal{M}$. Then we have

$$(M) \vdash a(pa^i)^* \approx (pa^i)^* a .$$

Proof : If $i = 0$, there is nothing to prove. Hence we can suppose that $i \geq 1$. In this case, we can write

$$(M) \vdash a(pa^i)^* \approx a(0 \oplus pa^{i-1}(pa^i)^*a) = (0 \oplus pa^i(pa^i)^*) a \approx (pa^i)^* a .$$

This ends therefore our proof. \blacksquare

Note : It follows from lemma 2.1 that every polynomial of $\mathcal{M}[a]$ commutes with any expression of the form $(pa^i)^*$ with respect to (M) .

Let us also recall the following classical identity whose proof goes as in the usual boolean case (see [3] p. 36).

LEMMA 2.2 : We have $(M), (S) \vdash a^*b^* \leq (a \oplus b)^*$.

3 Normalized one-letter \mathcal{M} -rational expressions

3.1 A family of \mathcal{M} -rational identities

Let us first prove the following lemma.

LEMMA 3.1 : Let $p, q \in \mathcal{M}$. Then we have in $\mathcal{M} \ll a \gg$

$$(pa)^* \otimes (qa)^* = ((p \oplus q)a)^* .$$

Proof : An obvious computation shows that we have

$$(pa)^* = \bigoplus_{i=0}^{+\infty} ip a^i \quad (3.1) .$$

We easily get from relation (3.1) that

$$(pa)^* \otimes (qa)^* = \bigoplus_{n=0}^{+\infty} a^n \min_{i+j=n} (ip + jq) \quad (3.2) .$$

It is then easy to deduce that $(pa)^* \otimes (qa)^* = ((p \oplus q)a)^*$ when p or q is equal to $+\infty$. Thus let us now suppose that p and q are in \mathbb{N} . Then we can write

$$ip + jq \geq (i + j) \min(p, q) = n(p \oplus q)$$

for every $i, j \in \mathbb{N}$ such that $i + j = n$. Hence $\min_{i+j=n} (ip + jq) = n(p \oplus q)$, the minimum being obtained either for $i = 0$ or for $j = 0$. Reporting this result in relation (3.2), we clearly get $(pa)^* \otimes (qa)^* = ((p \oplus q)a)^*$. This ends our proof. \blacksquare

The previous lemma shows therefore that the \mathcal{M} -rational identities

$$(P(p, q)) \quad ((p \oplus q)a)^* \approx (pa)^* \otimes (qa)^*$$

are consistent for every $p, q \in \mathcal{M}$.

Let us now give the following result.

PROPOSITION 3.2 : Let r, s, p, q be four elements of \mathcal{M} . Then there exists an integer $N \in \mathbb{N}$ such that we have for every $k \geq N$

$$(M), (P(p, q)) \vdash r(pa)^* \oplus s(qa)^* \approx P_k(a) \oplus ta^k(ma)^*$$

where $t, m \in \mathcal{M}$ and where $P_k(a)$ is a polynomial of $\mathcal{M}[a]$ of degree $< k$.

Proof : Our result is clearly true with $N = 0$ when r or s are equal to $+\infty$. Indeed if $r = +\infty$ for instance, we get by iterated uses of (M)

$$(M) \vdash r(pa)^* \oplus s(qa)^* = s(qa)^* \approx \left(\bigoplus_{i=0}^{k-1} (s+iq) a^i \right) \oplus (s+kq) a^k (qa)^* .$$

The conclusion is also clear with $N = 0$ when $p = q$ since we have in the same way

$$(M) \vdash r(pa)^* \oplus s(qa)^* = (r \oplus s)(pa)^* \approx (r \oplus s) \otimes \left(\left(\bigoplus_{i=0}^{k-1} ip a^i \right) \oplus kp a^k (pa)^* \right) .$$

Let us now suppose that $r, s \in \mathbb{N}$ and that $p \neq q$. We can also suppose that $p = p \oplus q$ for instance. Since $p <_{\mathbb{N}} q$, there exists $N \in \mathbb{N}$ such that $r+pk <_{\mathbb{N}} s+kq$ for every integer $k \geq N$. Let then $k \geq N$. Using iteratively (M) , we easily get

$$(M) \vdash r(pa)^* \oplus s(qa)^* \approx \left(\bigoplus_{i=0}^{k-1} ((r+ip) \oplus (s+iq)) a^i \right) \oplus a^k ((r+kp)(pa)^* \oplus (s+kq)(qa)^*) .$$

On the other hand, we can write

$$(P(p, q)) \vdash (r+kp)(pa)^* \oplus (s+kq)(qa)^* \approx (qa)^* ((r+kp)(pa)^* \oplus (s+kq)) \quad (3.3) .$$

But since $(r+kp) \oplus (s+kq) = r+kp$, we easily get

$$\begin{aligned} (M) \vdash (r+kp)(pa)^* \oplus (s+kq) &\approx ((r+kp) \oplus (s+kq)) \oplus (r+kp) \otimes (pa)(pa)^* \\ &\vdash (r+kp)(pa)^* \oplus (s+kq) \approx (r+kp)(0 \oplus (pa)(pa)^*) \\ &\vdash (r+kp)(pa)^* \oplus (s+kq) \approx (r+kp)(pa)^* \end{aligned} \quad (3.4) .$$

Hence it follows from relations (3.3) and (3.4) that

$$(M), (P(p, q)) \vdash (r+kp)(pa)^* \oplus (s+kq)(qa)^* \approx (r+kp)(qa)^*(pa)^* \approx (r+kp)(pa)^* .$$

Thus all our computations shows that

$$(M), (P(p, q)) \vdash r(pa)^* \oplus s(qa)^* \approx \left(\bigoplus_{i=0}^{k-1} ((r+ip) \oplus (s+iq)) a^i \right) \oplus (r+kp) a^k (pa)^* .$$

This ends therefore our proof. \blacksquare

COROLLARY 3.3 : Let $(r_i)_{i=1, M}$ and $(p_i)_{i=1, M}$ be two families of M elements of \mathcal{M} . Then there exists an integer $N \in \mathbb{N}$ such that we have for every $k \geq N$

$$(M), (P(p, q))_{p, q \in \mathcal{M}} \vdash \bigoplus_{i=1}^M r_i (p_i a)^* \approx P_k(a) \oplus t a^k (ma)^*$$

where $t, m \in \mathcal{M}$ and where $P_k(a)$ is a polynomial of $\mathcal{M}[a]$ of degree $< k$.

Proof : We argue by induction on M . The case $M = 1$ is easy and the case $M = 2$ is given by proposition 3.2. Let us now suppose that our result holds at order $M-1$ with $M \geq 3$. Applying the induction hypothesis, we obtain an integer K such that

$$(M), (P(p, q))_{p, q \in \mathcal{M}} \vdash \bigoplus_{i=1}^{M-1} r_i(p_i a)^* \approx P_k(a) \oplus t a^k (ma)^*$$

holds for every $k \geq N$ under the conditions of proposition 3.2. Hence, using iteratively (M) , it follows that we can write for every $k \geq K$

$$(M), (P(p, q))_{p, q \in \mathcal{M}} \vdash \bigoplus_{i=1}^M r_i(p_i a)^* \approx Q_k(a) \oplus a^k (t(ma)^* \oplus (r_m + kp_m)(p_m a)^*)$$

where we set $Q_k(a) = P_k(a) \oplus r_m \otimes (0 \oplus p_m a \oplus \dots \oplus (k-1)p_m a^{k-1})$ which is a polynomial of $\mathcal{M}[a]$ of degree $< k$. But proposition 3.2 shows that there exists N such that

$$(M), ((P(m, p_m)) \vdash t(ma)^* \oplus (r_m + kp_m)(p_m a)^* \approx R_n(a) \oplus p a^n (qa)^*$$

holds for every $n \geq N$, where R_n is a polynomial of degree $< n$ of $\mathcal{M}[a]$ and where p, q belongs to \mathcal{M} . It is now easy to conclude to our corollary. ■

We can also give the following result.

PROPOSITION 3.4 : Let $p, q \in \mathcal{M}$. Then we have

$$(M), (P(p, q)) \vdash (pa)^* \oplus (qa)^* \approx ((p \oplus q)a)^* .$$

Proof : Let us suppose for instance that $p = p \oplus q$. Then we can clearly write that

$$(P(p, q)) \vdash (pa)^* \oplus (qa)^* \approx ((pa)^* \oplus 0)(qa)^* .$$

Using the same method as in the end of the proof of proposition 3.2, we easily get

$$(M), (P(p, q)) \vdash ((pa)^* \oplus 0)(qa)^* \approx (pa)^* (qa)^* \approx (pa)^* .$$

Our proposition follows now immediately from the two above deductions. ■

The following result will also be useful in the sequel.

PROPOSITION 3.5 : Let $p, q \in \mathcal{M}$ and let $i, j \in \mathbb{N}$. Then there exists an element $r \in \mathcal{M}$, an integer $k \in \mathbb{N}$ and a polynomial $P \in \mathcal{M}[a]$ such that

$$(M), P(i), P(j), (P(jp, iq)) \vdash (pa^i)^* \otimes (qa^j)^* \approx P(a) (ra^k)^* .$$

Proof : Using $(P(j))$ and $(P(i))$, we can write :

$$P(j) \vdash (pa^i)^* \approx Q_j(pa^i) (jpa^{ij})^* \quad \text{and} \quad P(i) \vdash (qa^j)^* \approx Q_i(qa^j) (iqa^{ij})^*$$

where $Q_k(a)$ denotes for every $k \in \mathbb{N}$ the polynomial $Q_k = 1 \oplus a \oplus \dots \oplus a^{k-1}$. Using lemma 2.1, it follows immediately that

$$P(i), P(j), (M) \vdash (pa^i)^* \otimes (qa^j)^* \approx Q_j(pa^i) Q_i(qa^j) (jp a^{ij})^* (iq a^{ij})^*$$

from which, using $(P(jp, iq))$, we now easily get the result claimed by the lemma. ■

3.2 Normalized expressions

As an immediate corollary of proposition 3.5, we get the following result.

PROPOSITION 3.6 : The family of \mathcal{M} -rational expressions defined by

$$P(a) \oplus \bigoplus_{p \in \mathcal{M}, i \in \mathbb{N}} Q_{p,i}(a)(pa^i)^* \quad (3.5)$$

where P and $Q_{p,i}$ are polynomials in $\mathcal{M}[a]$ is additively and multiplicatively closed with respect to the identities (M) , $(P(p, q))_{p,q \in \mathcal{M}}$ and $(P(n))_{n \in \mathbb{N}}$.

Proof : Our family is clearly additively closed. It is also multiplicatively closed with respect to the above identities according to lemma 2.1 and proposition 3.5. ■

We can also easily obtain the following consequence of proposition 3.6.

COROLLARY 3.7 : The family of \mathcal{M} -rational expressions defined by

$$P(a) \oplus a^K \left(\bigoplus_{i=0}^{N-1} q_i a^i (p_i a^N)^* \right) \quad (3.6)$$

where $N, K \in \mathbb{N}$, where P is a polynomial of $\mathcal{M}[a]$ of degree $< K$ and where $(p_i)_{i=0, N-1}$ and $(q_i)_{i=0, N-1}$ are elements of \mathcal{M} with $q_0 \neq +\infty$, is additively and multiplicatively closed with respect to the identities (M) , $(P(p, q))_{p,q \in \mathcal{M}}$ and $(P(n))_{n \in \mathbb{N}}$.

Proof : According to proposition 3.6, it suffices to see that every \mathcal{M} -rational expression of type (3.5) can be rewritten in form (3.6) using the desired identities. Note first that using $(P(n))_{n \in \mathbb{N}}$, one can easily write any expression of type (3.5) as

$$R(a) \oplus \bigoplus_{i=0}^M R_i(a) (r_i a^N)^* \quad (3.7)$$

where R and every R_i is a polynomial of $\mathcal{M}[a]$, where $N, M \in \mathbb{N}$ and where $(r_i)_{i=0, M}$ are elements of \mathcal{M} . Applying now several times (M) that allows to write $(ra^N)^* \approx 0 \oplus ra^N(ra^N)^*$, we can easily rewrite an expression of form (3.7) as

$$Q(a) \oplus a^L \left(\bigoplus_{k=0}^{N-1} a^k \left(\bigoplus_{i=1}^{M_k} r_{i,k} (r_i a^N)^* \right) \right)$$

where $Q \in \mathcal{M}[a]$, where L and every M_k belong to \mathbb{N} and where every r_i and $r_{i,k}$ is in \mathcal{M} . Using now corollary 3.3, we can immediately conclude that the previous expression is equivalent to an expression of the form

$$P(a) \oplus a^K \left(\bigoplus_{k=0}^{N-1} q_k a^k (p_k a^N)^* \right)$$

with respect to (M) and $(P(p, q))_{p,q \in \mathcal{M}}$. It suffices now to use (M) in order to reduce the previous expression to an expression of the same form but with P of degree $< K$. Thus this ends our proof since we can clearly suppose that $q_0 \neq +\infty$. ■

According to corollary 3.7, we can give the following definition.

DEFINITION 3.1 : A one-letter \mathcal{M} -rational expression E is said to be *normalized* when E has the form (3.6).

The following proposition gives the main property of normalized expressions.

PROPOSITION 3.8 : Let E, F be two one-letter normalized \mathcal{M} -rational expressions such that $\epsilon(E) = \epsilon(F)$. Then we have

$$(M), (P(p, q))_{p, q \in \mathcal{M}}, (P(n))_{n \in \mathbb{N}} \vdash E \approx F .$$

Proof : Using the identities $(P(n))_{n \in \mathbb{N}}$, we can transform the two normalized expressions E and F into expressions of form (3.7) with the same N . Using the method involved in the proof of corollary 3.7, we can then rewrite E and F in normalized form but with the same N . Using iteratively the identity (M) , one can also choose the same K . Hence we showed that

$$(M), (P(n))_{n \in \mathbb{N}}, ((P(p, q))_{p, q \in \mathcal{M}} \vdash E \approx P(a) \oplus a^K \left(\bigoplus_{i=0}^{N-1} q_i a^i (p_i a^N)^* \right)$$

$$(M), (P(n))_{n \in \mathbb{N}}, ((P(p, q))_{p, q \in \mathcal{M}} \vdash F \approx Q(a) \oplus a^K \left(\bigoplus_{i=0}^{N-1} r_i a^i (s_i a^N)^* \right)$$

where the two above expressions are normalized. Since $\epsilon(E) = \epsilon(F)$, it is easy to see that we must have $P = Q$ and $p_i = s_i$ and $r_i = q_i$ for every $i \in [0, N - 1]$. Hence the identity $E \approx F$ can be deduced from the desired family of identities. ■

4 Commutative axiomatization

One-letter \mathcal{M} -rational expressions can be considered as *commutative* \mathcal{M} -rational expressions. This means that we work with respect to the axiom $ab = ba$ (see also [3] p. 91). Hence we can also study their commutative axiomatization. Let us first introduce the commutative identity

$$(C) \quad (a \oplus b)^* \approx a^* b^*$$

(which is only true in the commutative case) whose consistency follows from the boolean case (cf [3] p. 91). We can now give the following result.

PROPOSITION 4.1 : The system (M) , (S) , $(P(p, q))_{p, q \in \mathcal{M}}$, $(P(n))_{n \in \mathbb{N}}$ and (C) is a complete system of *commutative* identities for one-letter \mathcal{M} -rational expressions.

Proof : Note first that it suffices to prove that normalized one-letter \mathcal{M} -rational expressions are stable by star with respect to the above identities, in order to get our result. Indeed, it will then follow from corollary 3.7 that every one-letter \mathcal{M} -rational expression can be reduced to a normalized form using the desired identities since the letter a is normalized. It is then easy to conclude using proposition 3.8. Thus let

$$E = \bigoplus_{i=0}^{K-1} p_i a^i \oplus \bigoplus_{i=0}^{N-1} q_i a^{i+K} (r_i a^N)^*$$

be a normalized expression. Using (C) , we obtain

$$(C) \vdash E^* \approx \bigotimes_{i=0}^{K-1} (p_i a^i)^* \otimes \bigotimes_{i=0}^{N-1} (q_i a^{i+K} (r_i a^N)^*)^* \quad (4.1) .$$

However, using (M), we can clearly write

$$(M) \vdash (q_i a^{i+K} (r_i a^N)^*)^* \approx 0 \oplus q_i a^{i+K} (r_i a^N)^* (q_i a^{i+K} (r_i a^N)^*)^*$$

for every $i \in [0, N - 1]$. It follows immediately that

$$(M), (S) \vdash (q_i a^{i+K} (r_i a^N)^*)^* \approx 0 \oplus q_i a^{i+K} (q_i a^{i+K} \oplus r_i a^N)^*$$

and hence, using (C), we obtain

$$(M), (S), (C) \vdash (q_i a^{i+K} (r_i a^N)^*)^* \approx 0 \oplus q_i a^{i+K} (q_i a^{i+K})^* (r_i a^N)^* \quad (4.2)$$

for every $i \in [0, N - 1]$. It follows now from relations (4.1) and (4.2) and from corollary 3.7 that E^* can be reduced to a normalized form with respect to the identities involved in the statement of our result. Thus this ends our proof. ■

Note : We can easily adapt the proof of theorem 1 of [3] p. 92 in order to get a normal form (with respect to the identities involved in proposition 4.1) for every commutative \mathcal{M} -rational expression over an arbitrary alphabet A , as a finite sum of terms of type $k_w w (k_1 w_1)^* \dots (k_n w_n)^*$ where w, w_1, \dots, w_n are words of A^* and where k_w, k_1, \dots, k_n are elements of \mathcal{M} . In fact, it might also be possible to adapt the proof of Redko's theorem (see [14]) given by Conway (see [3] p. 93-95) in order to show that the system (M), (S), $(P(p, q))_{p, q \in \mathcal{M}}$, $(P(n))_{n \in \mathbb{N}}$ and (C) is a complete system of *commutative* \mathcal{M} -rational identities for every alphabet A .

5 Non-commutative axiomatization

In the sequel, (\mathcal{A}) always denote the system (M), (S), $(P(p, q))_{p, q \in \mathcal{M}}$ and $(P(n))_{n \in \mathbb{N}}$ of \mathcal{M} -rational identities. Let us now recall that, as we saw in the proof of proposition 4.1, the research of a complete system of \mathcal{M} -rational identities for one-letter \mathcal{M} -rational expressions can be reduced to the research of a system (\mathcal{B}) of \mathcal{M} -rational identities containing (\mathcal{A}) such that E^* can be reduced in a normalized form with respect to (\mathcal{B}) for every normalized one-letter \mathcal{M} -rational expression E . Thus let then

$$E = \bigoplus_{i=0}^{K-1} p_i a^i \oplus \bigoplus_{i=0}^{N-1} q_i a^{i+K} (r_i a^N)^* \quad (5.1)$$

be such a normalized one-letter \mathcal{M} -rational expression.

5.1 First reduction

Let then F denote the one-letter \mathcal{M} -rational expression

$$F = \bigotimes_{i=0}^{K-1} (p_i a^i)^* \otimes \bigotimes_{i=0}^{N-1} (0 \oplus q_i a^{i+K} (q_i a^{i+K})^* (r_i a^N)^*) .$$

Following the lines of the proof of proposition 4.1, but using lemma 2.2 instead of axiom (C), we can easily obtain that

$$(M), (S) \vdash F \leq E^* .$$

Observe also that the proof of proposition 4.1 shows that we have $\epsilon(F) = \epsilon(E^*)$. Using now corollary 3.7, we easily get a normalized one-letter \mathcal{M} -rational expression U such that $(\mathcal{A}) \vdash F \approx U$. Hence we have

$$(M), (S) \vdash U \leq E^* \quad (5.2)$$

where U is a normalized one-letter \mathcal{M} -rational expression such that $\epsilon(U) = \epsilon(E^*)$. Since every identity between normalized expressions can be deduced from (\mathcal{A}) according to proposition 3.8, we immediately get $(\mathcal{A}) \vdash E \leq U$ from which it follows that

$$(\mathcal{A}) \vdash E^* \leq U^* \quad (5.3) .$$

Thus, according to relations (5.2) and (5.3), we have

$$(\mathcal{A}) \vdash U \leq E^* \leq U^* \quad (5.4) .$$

Since $\epsilon(U) = \epsilon(E^*)$, it follows that $\epsilon(U) = \epsilon(U^*)$ (cf [3] p. 35). Hence we can reduce our initial problem to the research of a system of identities (\mathcal{B}) containing (\mathcal{A}) such that

$$(\mathcal{B}) \vdash U \approx U^* \quad (5.5)$$

for every normalized one-letter \mathcal{M} -rational expression U for which $\epsilon(U) = \epsilon(U^*)$. Indeed if (\mathcal{B}) is such a system, we have

$$(\mathcal{B}) \vdash E^* \approx U$$

according to relation (5.4). Hence (\mathcal{B}) is a system of identities with respect to which the star of every normalized one-letter \mathcal{M} -rational expression can be reduced to a normalized form, as desired.

5.2 Second reduction

Hence a system (\mathcal{B}) of \mathcal{M} -rational identities for which relation (5.5) holds under the required conditions, is necessarily complete. Let then

$$U = P(a) \oplus a^K V \quad \text{where } V = \bigoplus_{i=0}^{N-1} q_i a^i (r_i a^N)^* \quad (5.6)$$

be a normalized one-letter expression such that $\epsilon(U) = \epsilon(U^*)$.

LEMMA 5.1 : Under the previous assumptions, we have

$$\epsilon((a^K V)^*) = 0 \oplus \epsilon(a^K V) .$$

Proof : Note first that we clearly have

$$0 \oplus \epsilon(a^K V) \leq \epsilon(a^K V)^* \quad (5.7) .$$

Since $\epsilon(U) = \epsilon(U^*)$, we also have $\epsilon(U^k) = \epsilon(U)$ for every integer $k \geq 1$. Hence, using relation (5.6), we can write

$$P(a) \oplus \epsilon(a^K V) = (P(a) \oplus \epsilon(a^K V))^k = P(a)^k \oplus \epsilon((a^K V)^k) \oplus R_k \quad (5.8)$$

with some series $R_k \in \mathcal{M} \ll a \gg$ for every $k \geq 1$. Looking only on the terms of degree $\geq K$ in relation (5.8), we get that

$$\epsilon(a^K V) = \epsilon((a^K V)^k) \oplus S_k \quad (5.9)$$

with some series $S_k \in \mathcal{M} \ll a \gg$ for every $k \geq 1$. Adding all relations (5.9) for every $k \geq 1$, we immediately obtain

$$0 \oplus \epsilon(a^K V) = \epsilon((a^K V)^*) \oplus S \quad (5.10)$$

where S denotes the series of $\mathcal{M} \ll a \gg$ which is the sum of all the series S_k for $k \geq 1$. Hence relation (5.10) shows that

$$\epsilon((a^K V)^*) \leq 0 \oplus \epsilon(a^K V) \quad (5.11) .$$

The lemma follows now immediately from relations (5.7) and (5.11). \blacksquare

Let us now suppose that (\mathcal{B}) is a system of \mathcal{M} -rational identities that contains (\mathcal{A}) and such that

$$(\mathcal{B}) \vdash (a^K V)^* \approx 0 \oplus a^K V \quad (5.12).$$

Then we can give the following lemma.

LEMMA 5.2 : Under the previous assumptions and hypotheses, we have

$$(\mathcal{B}) \vdash U^* \approx U .$$

Proof : Since $\epsilon(U) = \epsilon(U^*)$, the constant term of U is 0. Hence if $P = +\infty$, we must have $K = 0$ and $U = V$ and it is then easy to deduce our lemma from relation (5.12). Let us now suppose that $P \neq +\infty$. We can then write $P = 0 \oplus a Q$ with some polynomial Q of $\mathcal{M}[a]$ of degree $< K - 1$. It follows that we have

$$(S) \vdash U^* = (0 \oplus a Q \oplus a^K V)^* \approx (a Q \oplus a^K V)^*$$

from which we immediately deduce

$$(S), (P(K)) \vdash U^* \approx \left(\bigoplus_{i=0}^{K-1} (a Q \oplus a^K V)^i \right) ((a Q \oplus a^K V)^K)^* \quad (5.13) .$$

But we clearly have

$$(a Q \oplus \epsilon(a^K V))^K \leq \epsilon(U^*) = 0 \oplus a Q \oplus \epsilon(a^K V) .$$

Considering only the elements of degree $\geq K$ in the previous inequality, we obtain

$$(a Q \oplus \epsilon(a^K V))^K \leq \epsilon(a^K V) .$$

Hence, since every identity between any product of normalized expressions (that can be normalized with respect to (\mathcal{A})) is deducible from (\mathcal{A}) according to proposition 3.8 and corollary 3.7, we get

$$(\mathcal{A}) \vdash (a Q \oplus a^K V)^K \leq a^K V \quad (5.14) .$$

It follows now from relations (5.13) and (5.14) that

$$(\mathcal{A}) \vdash U^* \leq \left(\bigoplus_{i=0}^{K-1} (a Q \oplus a^K V)^i \right) (a^K V)^* .$$

Hence, using hypothesis (5.12), we can write

$$(\mathcal{B}) \vdash U^* \leq \left(\bigoplus_{i=0}^{K-1} (a Q \oplus a^K V)^i \right) (0 \oplus a^K V) \quad (5.15) .$$

Let us denote by G the \mathcal{M} -rational expression that appears at the right member of relation (5.15). Observe that we have

$$\epsilon(G) \leq (aQ \oplus \epsilon(a^K V))^* (0 \oplus \epsilon(a^K V)) \leq (\epsilon(U^*))^2 = \epsilon(U^*) = \epsilon(U) .$$

Hence, using again proposition 3.8 and corollary 3.7, we get

$$(\mathcal{A}) \vdash G \leq U \quad (5.16) .$$

It follows now immediately from relations (5.15) and (5.16) that

$$(\mathcal{B}) \vdash U^* \leq U .$$

Since the converse inequality is an obvious consequence of (M) , the lemma follows now easily. This ends our proof. \blacksquare

Hence lemma 5.2 shows that we can reduce our problem to the research of systems of \mathcal{M} -rational identities (\mathcal{B}) containing (\mathcal{A}) such that relation (5.12) holds when V is a one-letter \mathcal{M} -rational expression of the form (5.6) for which relation (5.12) is consistent. Indeed we proved that such a system (\mathcal{B}) is complete.

5.3 Third reduction

Let now W be a one-letter \mathcal{M} -rational expression of the form

$$W = a^K \left(\bigoplus_{i=0}^{N-1} q_i a^i (r_i a^N)^* \right) \quad (5.17)$$

such that $\epsilon(W^*) = 0 \oplus \epsilon(W)$. We are now looking for a system of \mathcal{M} -rational identities that allows to deduce the identity $W^* \approx 0 \oplus W$ since such a system is complete according to our study. Let us then consider the set

$$M = \{0\} \cup \bigcup_{i \in [0, N-1], q_i \neq +\infty} \{K + i + nN, n \in \mathbb{N}\} \subset \mathbb{N} .$$

It is easy to deduce that M is a submonoid of \mathbb{N} from the fact that $\epsilon(W^*) = 0 \oplus \epsilon(W)$. Hence $M = F \cup (\delta\mathbb{N} + k\delta)$ where δ is a strictly positive integer, where $k \in \mathbb{N}$ and where F is some finite subset of $\delta\mathbb{N}$ (see exercice 5.1.2 of [4]). In particular, since $q_0 \neq +\infty$ by hypothesis, K and $K + N$ must be in $\delta\mathbb{N}$. Thus $N \in \delta\mathbb{N}$. The same method shows that $i \in \delta\mathbb{N}$ for every $i \in [0, N-1]$ such that $q_i \neq +\infty$. It follows now easily that we have

$$W = a^{\delta L} \left(\bigoplus_{i=0}^{M-1} q_{\delta i} a^{\delta i} (r_i a^{\delta M})^* \right)$$

with some integers L and M . Let us then consider the \mathcal{M} -rational expression

$$W_\delta = a^L \left(\bigoplus_{i=0}^{M-1} q_{\delta i} a^i (r_i a^M)^* \right) .$$

Since we clearly have $W(a) = W_\delta(a^\delta)$, we also get $\epsilon(W_\delta^*) = 0 \oplus \epsilon(W_\delta)$. As one can now immediately see, working with W_δ rather than W , we can suppose that $\delta = 1$. This is exactly equivalent to suppose that the set M associated with W is

$$M = F \cup (\mathbb{N} + k)$$

where $k \in \mathbb{N}$ and where F is some finite subset of $[0, k-1]$. In other words, this means equivalently that we can suppose that $q_i \neq +\infty$ for every $i \in [0, N-1]$.

5.4 Fourth reduction

Let us now write $K = kN + r$ with $0 \leq r < N$. Hence we get

$$W = a^{kN+r} \left(\bigoplus_{i=0}^{N-1} q_i a^i (r_i a^N)^* \right) \quad (5.18)$$

where q_i is different from $+\infty$ for every $i \in [0, N-1]$. We then have

$$W = a^{kN+r} \left(\bigoplus_{i=0}^{N-r-1} q_i a^i (r_i a^N)^* \right) \oplus a^{kN+r} \left(\bigoplus_{i=N-r}^{N-1} q_i a^i (r_i a^N)^* \right).$$

Using now (M), we deduce easily from this last relation that

$$\begin{aligned} (M) \vdash W &\approx P(a) \oplus a^{(k+1)N+r} \left(\bigoplus_{i=0}^{N-r-1} (q_i + r_i) a^i (r_i a^N)^* \right) \\ &\oplus a^{(k+1)N} \left(\bigoplus_{i=0}^{r-1} q_{i-r+N} a^i (r_i a^N)^* \right) \end{aligned} \quad (5.19)$$

where $P(a)$ denotes the polynomial of degree $< (k+1)N$ defined by

$$P(a) = a^{kN+r} \left(\bigoplus_{i=0}^{N-r-1} q_i a^i \right).$$

Reindexing the expression involved in relation (5.19), we get

$$(M) \vdash W \approx P(a) \oplus a^{(k+1)N} \left(\bigoplus_{i=0}^{N-1} q'_i a^i (r_i a^N)^* \right) \quad (5.20)$$

with some new non-infinite coefficients q'_i . Let now W' be the one-letter \mathcal{M} -rational expression which is defined by

$$W' = a^{(k+1)N} \left(\bigoplus_{i=0}^{N-1} q'_i a^i (r_i a^N)^* \right).$$

Using lemma 5.1, we obtain $\epsilon(W'^*) = 0 \oplus \epsilon(W')$. Moreover it follows easily from relation (5.20) and lemma 5.2 that we can reduce the research of a system (\mathcal{B}) of \mathcal{M} -rational identities such that $(\mathcal{B}) \vdash W^* \approx 0 \oplus W$ to the research of a system such that $(\mathcal{B}) \vdash W'^* \approx 0 \oplus W'$. Hence this proves that we can suppose that $r = 0$ in relation (5.18).

LEMMA 5.3 : Let W be a one-letter \mathcal{M} -rational expression of form (5.18) with $r = 0$ such that $\epsilon(W^*) = 0 \oplus \epsilon(W)$. Then we have $r_i = r_j$ for every $i, j \in [0, N-1]$.

Proof : Note first that we clearly have

$$(\epsilon(W) | a^{nN+i}) \simeq_{n \rightarrow +\infty} r_i n \quad (5.21)$$

for every $i \in [0, N-1]$. On the other hand, an easy computation using lemma 3.1 shows that we have

$$\epsilon(W^l) = a^{klN} \left(\bigoplus_{i_1, \dots, i_l=0}^{N-1} (q_{i_1} + \dots + q_{i_l}) a^{i_1 + \dots + i_l} (\min(r_{i_1}, \dots, r_{i_l}) a^N)^* \right) \quad (5.22)$$

for every integer $l \geq 1$. Hence we have in particular for every $i \in [0, N-1]$

$$\epsilon(W^2) = a^{2kN} \left((q_0 + q_i) a^i ((r_0 \oplus r_i) a^N)^* \oplus S_i \right)$$

where S_i is some series of $\mathcal{M} \ll a \gg$. Thus we asymptotically have

$$(\epsilon(W^2)|a^{nN+i}) \leq_{\mathbb{N}} (r_0 \oplus r_i)n \quad (5.23)$$

for every $i \in [0, N-1]$ when $n \rightarrow +\infty$. But $\epsilon(W^*) = 0 \oplus \epsilon(W) \oplus \epsilon(W^2) \oplus \dots = 0 \oplus \epsilon(W)$ by hypothesis. Hence we asymptotically have

$$(\epsilon(W)|a^{nN+i}) \leq_{\mathbb{N}} (\epsilon(W^2)|a^{nN+i}) \quad (5.24) .$$

It follows now easily from relations (5.21), (5.23) and (5.24) that $r_i \leq_{\mathbb{N}} r_0 \oplus r_i$ for every $i \in [0, N-1]$. Hence we proved that $r_i \leq_{\mathbb{N}} r_0$ for every $i \in [0, N-1]$.

On the other hand, relation (5.22) shows that we have

$$\epsilon(W^N) = a^{kN^2} (N q_i a^{Ni} ((r_i \oplus \dots \oplus r_i) a^N)^* \oplus S_i) = a^{kN^2} (N q_i a^{Ni} (r_i a^N)^* \oplus S_i)$$

with some series $S_i \in \mathcal{M} \ll a \gg$ for every $i \in [0, N-1]$. Using the same kind of argument than above, we easily asymptotically obtain

$$(\epsilon(W)|a^{nN}) \leq_{\mathbb{N}} (\epsilon(W^N)|a^{nN}) \leq_{\mathbb{N}} r_i n$$

when $n \rightarrow +\infty$ for every $i \in [0, N-1]$. It follows now easily from these last relations and from relation (5.21) that $r_0 \leq_{\mathbb{N}} r_i$ for every $i \in [0, N-1]$. Thus our study shows clearly that $r_0 = r_i$ for every $i \in [0, N-1]$. This ends our proof. \blacksquare

Let now (\mathcal{B}) be a system of \mathcal{M} -rational identities such that

$$(\mathcal{B}) \vdash W^* \approx 0 \oplus W \quad (5.25)$$

for every one-letter \mathcal{M} -rational expression W of type

$$W = a^{kN} \left(\bigoplus_{i=0}^{N-1} q_i a^i \right) (r a^N)^* \quad (5.26)$$

with every $q_i \neq +\infty$. Lemma 5.3 and our previous study show then that (\mathcal{B}) is a complete system for one-letter \mathcal{M} -rational expressions. On now on, we shall therefore focus on obtaining a system such that deduction (5.25) holds under assumption (5.26).

Note : In the boolean case, we would necessarily have $W = a^{kN} (1 + a + \dots + a^{N-1}) (a^N)^*$ at this step of our proof. Since W is equivalent to $W' = a^{kN} a^*$ with respect to the identity $(P(N))$, it is then easy to prove that $W^* \approx 1 + W$ with respect to (M) , (S) and $(P(N))$. Hence we obtained a new proof of the classical Redko's result that states that (M) , (S) and $(P(n))_{n \in \mathbb{N}}$ is a complete system of identities for usual one-letter boolean rational expressions (cf [3, 13]).

5.5 Analysis of relation (5.25)

Let us now study the \mathcal{M} -rational expressions of form (5.26) such that relation (5.25) holds. We first give the following result.

LEMMA 5.4 : Let W be a one-letter \mathcal{M} -rational expression of form (5.26). Then the two following assertions are equivalent

1. $\epsilon(W^*) = 0 \oplus \epsilon(W)$
2. $\epsilon(W^2) \leq 0 \oplus \epsilon(W)$.

Proof : Note first that $1 \implies 2$ is obvious. Let us suppose now that assertion 2 holds. It follows then by an easy induction on n that we have for every $n \geq 1$

$$\epsilon(W^n) \leq 0 \oplus \epsilon(W) .$$

Adding all these relations, we get $\epsilon(W^*) \leq 0 \oplus \epsilon(W)$. Assertion 1 follows now immediately since the converse inequality is obvious. This ends our proof. \blacksquare

COROLLARY 5.5 : Let W be a one-letter \mathcal{M} -rational expression of form (5.26). Then we have $\epsilon(W^*) = 0 \oplus \epsilon(W)$ iff the two following conditions hold

1. For every $l \in [0, N - 1]$, $q_l + kr \leq_{\mathbb{N}} \min_{\substack{i+j=l \\ i,j \in [0, N-1]}} (q_i + q_j)$
2. For every $l \in [0, N - 2]$, $q_l + (k + 1)r \leq_{\mathbb{N}} \min_{\substack{i+j=l+N \\ i,j \in [0, N-1]}} (q_i + q_j)$

Proof : Let us compute first $\epsilon(W^2)$. Using lemma 3.1, we easily get

$$\epsilon(W^2) = a^{2kN} \left(\bigoplus_{i=0}^{N-1} q_i a^i \right)^2 (r a^N)^* = a^{2kN} \left(\bigoplus_{i,j=0}^{N-1} (q_i + q_j) a^{i+j} \right) (r a^N)^* .$$

It follows therefore from the above identity that

$$\epsilon(W^2) = a^{2kN} \left(\bigoplus_{l=0}^{N-1} \min_{i+j=l} (q_i + q_j) a^l \right) (r a^N)^* \oplus a^{(2k+1)N} \left(\bigoplus_{l=0}^{N-2} \min_{i+j=l+N} (q_i + q_j) a^l \right) (r a^N)^* .$$

Thus the second condition of lemma 5.4 is clearly equivalent to the two conditions ³

1. For every $l \in [0, N - 1]$, $q_l + (l + k)r \leq_{\mathbb{N}} lr + \min_{i+j=l} (q_i + q_j)$
2. For every $l \in [0, N - 2]$, $q_l + (l + k + 1)r \leq_{\mathbb{N}} lr + \min_{i+j=l+N} (q_i + q_j)$.

Moreover these two last conditions are clearly equivalent to the two conditions of our corollary which follows now immediately from lemma 5.4. \blacksquare

When the two conditions of corollary 5.5 are satisfied for some $k = k_0$, they are also obviously satisfied for every $k \leq k_0$. This implies in particular that they are always satisfied with $k = 0$. Hence if X denotes the one-letter \mathcal{M} -rational expression

$$X = \left(\bigoplus_{i=0}^{N-1} q_i a^i \right) (r a^N)^* \quad (5.27) ,$$

which is such that $W = a^{kN} X$, we have $\epsilon(X^*) = 0 \oplus \epsilon(X)$ according to corollary 5.5.

5.6 Fifth reduction

Let us consider again the one-letter \mathcal{M} -rational expression W of relation (5.26). Two cases can occur : either $k = 0$ or $k \geq 1$. When $k \geq 1$, we can in fact always suppose that $k = 1$. Indeed, if we are in this case, we can write

³ When $k = 0$, condition 1 is obtained for $l = 0$ by looking on the coefficient of a^N of relation $\epsilon(W^2) \leq 0 \oplus \epsilon(W)$ and not on its constant term.

$$(P(k)) \vdash W \approx a^{kN} \left(\bigoplus_{i=0}^{N-1} q_i a^i \right) \left(\bigoplus_{j=0}^{k-1} jr a^{jN} \right) (kr a^{kN})^* .$$

Thus it follows immediately from the previous relation that

$$(P(k)) \vdash W \approx a^{kN} \left(\bigoplus_{l=0}^{Nk-1} \min_{i+Nj=l} (q_i + jr) a^l \right) (kr a^{kN})^* .$$

It follows now easily from this last relation that we can suppose that $k = 1$ when $k \geq 1$ in relation (5.26). Thus we can suppose that either $k = 0$ or $k = 1$ in relation (5.26).

5.7 Study of the case $k = 1$

In all this subsection, we suppose that $k = 1$ in relation (5.26). Then we have.

LEMMA 5.6 : Under the previous assumptions, $q_i \geq_{\mathbb{N}} r$ for every $i \in [0, N - 1]$.

Proof : Condition 1 of corollary 5.5 taken with $l = 0$ shows that $q_0 + q_0 \geq_{\mathbb{N}} q_0 + r$, hence that $q_0 \geq_{\mathbb{N}} r$. Let now $i \in [1, N - 1]$. Suppose first that $2i \geq_{\mathbb{N}} N$. Since $2i \leq_{\mathbb{N}} 2N - 2$, we can write $2i = N + j$ with $j \in [0, N - 2]$. Condition 2 of corollary 5.5 give us then

$$q_i + q_i \geq_{\mathbb{N}} q_j + 2r \geq_{\mathbb{N}} 2r$$

from which it immediately follows that $q_i \geq_{\mathbb{N}} r$. Let us now suppose that $2i <_{\mathbb{N}} N$. Let then l be the smallest integer such that $2^l i \geq_{\mathbb{N}} N$. Using the previous study, we obtain

$$q_{2^{l-1}i} \geq_{\mathbb{N}} r \quad (5.28) .$$

On the other hand, the first condition of corollary 5.5 shows that

$$q_i + q_i \geq_{\mathbb{N}} q_{2i} + r, \quad q_{2i} + q_{2i} \geq_{\mathbb{N}} q_{4i} + r, \quad \dots, \quad q_{2^{l-2}i} + q_{2^{l-2}i} \geq_{\mathbb{N}} q_{2^{l-1}i} + r .$$

It is now immediate to deduce from all these inequalities and from relation (5.28) that $q_i \geq_{\mathbb{N}} r$. This ends therefore our proof. ■

Hence lemma 5.6 shows that we can consider the \mathcal{M} -rational expression

$$Y = \left(\bigoplus_{i=0}^{N-1} (q_i - r) a^i \right) (r a^N)^* \quad (5.29) .$$

Moreover it is easy to deduce from the two conditions of corollary 5.5 that we have $\epsilon(Y^*) = 0 \oplus \epsilon(Y)$ since $k = 1$ here. We can now give the following result.

LEMMA 5.7 : Let now (\mathcal{B}) be a system of \mathcal{M} -rational identities that contains (\mathcal{A}) and such that $(\mathcal{B}) \vdash Y^* \approx 0 \oplus Y$. We have then $(\mathcal{B}) \vdash W^* \approx 0 \oplus W$.

Proof : Note first that we have in our case for every $i \in [0, N - 1]$

$$(\epsilon(Y)|a^{i+Nj}) = q_i + r(j - 1) \quad \text{and} \quad (\epsilon(W)|a^{i+Nj}) = q_i + r(j - 1)$$

respectively for every j and for every $j \geq 1$. Since $(\epsilon(W)|a^i) = +\infty$ for every $i \in [0, N - 1]$, it follows immediately from these computations that $\epsilon(W) \leq \epsilon(Y)$. Hence we get

$$(\mathcal{A}) \vdash W \leq Y \quad (5.30)$$

according to proposition 3.8. Using relation (5.30), we can write

$$(\mathcal{A}) \vdash W^* \approx 0 \oplus W \oplus W^2 W^* \leq 0 \oplus W \oplus W^2 Y^* .$$

Let now (\mathcal{B}) be a system of \mathcal{M} -rational identities as in the statement of our lemma. It follows then from the previous relation that we have

$$(\mathcal{B}) \vdash W^* \leq 0 \oplus W \oplus W^2(0 \oplus Y) \approx 0 \oplus W \oplus W^2 \oplus W^2 Y \quad (5.31) .$$

However since $k = 1$ here and since $\epsilon(W^2) \leq \epsilon(W^*) = 0 \oplus \epsilon(W)$, we clearly have $\epsilon(W^2) \leq \epsilon(W)$. Using again proposition 3.8, we obtain immediately from corollary 3.7 that $(\mathcal{A}) \vdash W^2 \leq W$. It follows then easily from relation (5.31) that

$$(\mathcal{B}) \vdash W^* \leq 0 \oplus W \oplus WY \quad (5.32) .$$

However, using relation (5.30), we can see that

$$\epsilon(WY) \leq \epsilon(Y^2) \leq \epsilon(Y^*) = 0 \oplus \epsilon(Y) .$$

Hence $\epsilon(WY) \leq 0 \oplus \epsilon(Y)$. Using now the fact that the only integers i such that $\epsilon(WY)$ has a non-infinite coefficient on a^i are necessarily $\geq N$ and the fact that $\epsilon(Y)$ and $\epsilon(W)$ have the same coefficients on every a^i with $i \geq N$ as shown at the beginning of this proof, we deduce easily from the previous inequality that $\epsilon(WY) \leq \epsilon(W)$. Using again proposition 3.8, we deduce immediately from corollary 3.7 that

$$(\mathcal{A}) \vdash WY \leq W .$$

Hence it follows now easily from relation (5.32) that

$$(\mathcal{B}) \vdash W^* \leq 0 \oplus W .$$

Since the converse inequality is an obvious consequence of (M) , it follows that the identity $W^* \approx 0 \oplus W$ is deducible from (\mathcal{B}) under our hypotheses. This ends our proof. \blacksquare

Hence lemma 5.7 shows that the case $k = 1$ can be in fact reduced to the case $k = 0$. According to the study of section 5.6, we can now suppose that $k = 0$ in relation (5.26).

5.8 Sixth reduction

Thus our study shows that if (\mathcal{B}) is a system of \mathcal{M} -rational identities such that

$$(\mathcal{B}) \vdash W^* \approx 0 \oplus W \quad (5.33)$$

for every one-letter \mathcal{M} -rational expression W of type

$$W = \left(\bigoplus_{i=0}^{N-1} q_i a^i \right) (r a^N)^* \quad (5.34)$$

with every $q_i \neq +\infty$ and such that relation (5.33) is consistent, then (\mathcal{B}) is a complete system of \mathcal{M} -rational identities for one-letter \mathcal{M} -rational expressions. Observe that identity (5.33) makes sense iff the following conditions are satisfied

1. For every $l \in [0, N - 1]$, $q_l \leq_{\mathbb{N}} \min_{\substack{i+j=l \\ i,j \in [0, N-1]}} (q_i + q_j)$
2. For every $l \in [0, N - 2]$, $q_l + r \leq_{\mathbb{N}} \min_{\substack{i+j=l+N \\ i,j \in [0, N-1]}} (q_i + q_j)$

according to corollary 5.5. It is easy to check that if the two above relations hold, they are also satisfied with $q_0 = 0$. Using again corollary 5.5, this shows that the \mathcal{M} -rational expression

$$Z = (0 \oplus \bigoplus_{i=1}^{N-1} q_i a^i) (r a^N)^* \quad (5.35)$$

satisfies to $\epsilon(Z^*) = 0 \oplus \epsilon(Z)$ and hence to $\epsilon(Z^*) = \epsilon(Z)$ since $\epsilon(Z) = 0 \oplus \epsilon(Z)$ because the constant term of $\epsilon(Z)$ is now 0. We can now give the following lemma.

LEMMA 5.8 : Let (\mathcal{B}) be a system of \mathcal{M} -rational identities that contains (\mathcal{A}) and such that $(\mathcal{B}) \vdash Z^* \approx Z$. Then we have $(\mathcal{B}) \vdash W^* \approx 0 \oplus W$.

Proof : Indeed, using (M) and (S) , it is easy to see that we can write

$$(M), (S) \vdash W \approx 0 \oplus WW^* \approx 0 \oplus \left(\bigoplus_{i=0}^{N-1} q_i a^i \right) (r a^N \oplus \bigoplus_{i=0}^{N-1} q_i a^i)^* .$$

Using now the fact that $q_0 \leq 0$, we get

$$(M), (S) \vdash W \leq 0 \oplus \left(\bigoplus_{i=0}^{N-1} q_i a^i \right) (r a^N \oplus 0 \oplus \bigoplus_{i=1}^{N-1} q_i a^i)^*$$

from which, using again (S) , we easily obtain

$$(M), (S) \vdash W \leq 0 \oplus \left(\bigoplus_{i=0}^{N-1} q_i a^i \right) (r a^N)^* Z^* = 0 \oplus WZ^* .$$

Using now our hypothesis on (\mathcal{B}) , we deduce that we have

$$(\mathcal{B}) \vdash W \leq 0 \oplus WZ \quad (5.36) .$$

However we can write

$$WZ = \left(\bigoplus_{i=0}^{N-1} q_i a^i \right) (r a^N)^* (0 \oplus \bigoplus_{i=1}^{N-1} q_i a^i) (r a^N)^* .$$

As $0 = 0 \oplus q_0$, it follows easily from the above relation that we have

$$WZ = \left(\bigoplus_{i=0}^{N-1} q_i a^i \right) (r a^N)^* (0 \oplus \bigoplus_{i=0}^{N-1} q_i a^i) (r a^N)^* .$$

Using now the deduction $(M), (S) \vdash a^* a^* \approx a^*$ (cf [3] p. 36), we get

$$(M), (S) \vdash WZ \approx \left(\bigoplus_{i=0}^{N-1} q_i a^i \right) (r a^N)^* (0 \oplus \bigoplus_{i=0}^{N-1} q_i a^i) (r a^N)^* \approx W \oplus W^2$$

Hence we proved that $(M), (S) \vdash WZ \leq W \oplus W^2$. Using now relation (5.36), we get

$$(\mathcal{B}) \vdash W^* \leq 0 \oplus W \oplus W^2 .$$

The converse inequality being an obvious consequence of (M) , it follows that

$$(\mathcal{B}) \vdash W^* \approx 0 \oplus W \oplus W^2 \quad (5.37) .$$

Hence $0 \oplus \epsilon(W) = 0 \oplus \epsilon(W) \oplus \epsilon(W^2)$. Using proposition 3.8, it follows from corollary 3.7 that $(\mathcal{A}) \vdash 0 \oplus W \approx 0 \oplus W \oplus W^2$. We can now immediately conclude with this deduction and relation (5.36). This ends our proof. \blacksquare

The previous lemma shows that we can suppose that $q_0 = 0$ in relation (5.34). Indeed if (\mathcal{B}) is a system of \mathcal{M} -rational identities such that

$$(\mathcal{B}) \vdash Z^* \approx Z \quad (5.38)$$

for every one-letter \mathcal{M} -rational expression Z of type

$$Z = (0 \oplus \bigoplus_{i=1}^{N-1} q_i a^i) (r a^N)^* \quad (5.39)$$

with every $q_i \neq +\infty$ and such that relation (5.38) is consistent, then (\mathcal{B}) is a complete system of \mathcal{M} -rational identities for one-letter \mathcal{M} -rational expressions.

5.9 A new family of \mathcal{M} -rational identities

Let us now consider a family $\underline{q} = (q_i)_{i=1, N}$ of non-infinite elements of \mathcal{M} that satisfies to the conditions

1. For every $l \in [1, N-1]$, $q_l \leq_{\mathbb{N}} \min_{\substack{i+j=l \\ i, j \in [1, N-1]}} (q_i + q_j)$
2. $q_N \leq_{\mathbb{N}} \min_{\substack{i+j=N \\ i, j \in [1, N-1]}} (q_i + q_j)$
3. For every $l \in [1, N-2]$, $q_l + q_N \leq_{\mathbb{N}} \min_{\substack{i+j=l+N \\ i, j \in [1, N-1]}} (q_i + q_j)$

Note that these conditions are exactly the conditions given by corollary 5.5 for relation (5.38) to be consistent when $q_N = r$. We associate then with such a family \underline{q} the following \mathcal{M} -rational identity

$$(St(\underline{q})) \quad \left(\bigoplus_{i=1}^N q_i a^i \right)^* \approx \left(0 \oplus \bigoplus_{i=1}^{N-1} q_i a^i \right) (q_N a^N)^*$$

whose consistency is given by the following lemma.

LEMMA 5.9 : Under the previous assumptions, $(St(\underline{q}))$ is a consistent identity .

Proof : Let us consider the \mathcal{M} -rational expression T defined by

$$T = \left(0 \oplus \bigoplus_{i=1}^{N-1} q_i a^i \right) (q_N a^N)^* .$$

Corollary 5.5 shows then that $\epsilon(T^*) = 0 \oplus \epsilon(T) = \epsilon(T)$ since the constant coefficient of $\epsilon(T)$ is 0. But we clearly have

$$T^* = \left(\left(0 \oplus \bigoplus_{i=1}^{N-1} q_i a^i \right) (q_N a^N)^* \right)^* ,$$

from which using (S) , it follows that

$$T^* \approx \left((q_N a^N)^* \right)^* \left(\left(\bigoplus_{i=1}^{N-1} q_i a^i \right) (q_N a^N)^* \left((q_N a^N)^* \right)^* \right)^* .$$

Using now star-star identity and the fact that $a^* a^* \approx a^*$ (cf [3] p. 36), we get

$$T^* \approx (q_N a^N)^* \left(\left(\bigoplus_{i=1}^{N-1} q_i a^i \right) (q_N a^N)^* \right)^* .$$

Identity (S) allows us then to deduce from this last relation that

$$T^* \approx \left(\bigoplus_{i=1}^N q_i a^i \right)^* .$$

The fact that $\epsilon(T^*) = \epsilon(T)$ is now clearly equivalent to the consistency of axiom ($St(\underline{q})$). Thus this ends our proof. ■

The importance of this new family of axioms comes from the following result that concludes all our study.

LEMMA 5.10 : Let us set $q_N = r$. Then we have

$$(M), (S), (St((q_i)_{i=1,N})) \vdash Z^* \approx Z .$$

Proof : Indeed we can write

$$(St((q_i)_{i=1,N})) \vdash Z \approx \left(\bigoplus_{i=1}^N q_i a^i \right)^* .$$

But it is easy to see that the proof of lemma 5.9 shows that

$$(M), (S) \vdash \left(\bigoplus_{i=1}^N q_i a^i \right)^* \approx \left(\left(0 \oplus \bigoplus_{i=1}^{N-1} q_i a^i \right) (q_N a^N)^* \right)^* = Z^* .$$

Our lemma follows now immediately from the two last relations. ■

The previous lemma shows therefore that $(\mathcal{A}) \cup (St(\underline{q}))_{q \in \mathcal{M}^n, n \in \mathbb{N}}$ is a system of \mathcal{M} -rational identities that satisfies to the desired property (5.38).

5.10 Conclusion

Hence it follows from lemma 5.10 that we have the following theorem that gives a complete system of \mathcal{M} -rational identities for one-letter \mathcal{M} -rational expressions.

THEOREM 5.11 : The following system of \mathcal{M} -rational identities

$$(M), (S), (P(n))_{n \in \mathbb{N}}, (P(p, q))_{p, q \in \mathcal{M}}, (St(\underline{p}))_{p \in \mathcal{M}^n, n \in \mathbb{N}}$$

is a *complete* system of identities for one-letter \mathcal{M} -rational expressions.

Notes : 1) One should notice the difference of difficulty between the commutative and the non-commutative axiomatization of one-letter \mathcal{M} -rational expressions.

2) The proof of theorem 5.11 shows in fact that every one-letter \mathcal{M} -rational expressions can be reduced in normalized form using the above identities.

Acknowledgements

Special thanks are due to the anonymous referee for his careful reading of the paper and for several valuable comments.

References

- [1] BACCELLI F., COHEN G., OLSDER G.J., QUADRAT J.P., *Synchronization and linearity – An algebra for discrete event systems*, Wiley, 1992
- [2] BERSTEL J., REUTENAUER C., *Rational series and their languages*, Springer Verlag, 1986
- [3] CONWAY J.H., *Regular algebra and finite machines*, Chapman and Hall, 1971
- [4] EILENBERG S., *Automata, languages and machines*, Volume A, Academic Press, 1974
- [5] HASHIGUSHI K., *Limitedness theorem on finite automata with distance functions*, J. Comput. Syst. Sci., **24**, (2), p. 233-244, 1982
- [6] HASHIGUSHI K., *Relative star-height, star-height and finite automata with distance functions*, [in "Formal properties of finite automata and applications", J.E. Pin (Ed.)], Lect. Notes in Comput. Sci., **386**, p. 74-88, Springer, 1989
- [7] KOZEN D., *A completeness theorem for Kleene algebras and the algebra of regular events*, Preprint (published in "Proceedings of LICS'91")
- [8] KROB D., *Expressions K-rationnelles*, Thèse, Université Paris 7, LITP Technical Report 88-23 , Paris, 1988
- [9] KROB D., *Complete systems of \mathcal{B} -rational identities*, Theor. Comput. Sci., **89**, (2), p. 207-343, 1991
- [10] KROB D., *Expressions K-rationnelles sur un anneau*, [in "Topics in invariant theory", M.P. Malliavin (Ed.)], Lect. Notes in Maths., **1478**, p. 215-143, Springer, 1991
- [11] KROB D., *Differentiation of K-rational expressions*, Int. Journ. of Alg. and Comput., **2**, (1), p. 57-87, 1992
- [12] KROB D., *The equality problem for rational series with multiplicities in the tropical semiring is undecidable*, [in "Proceedings of ICALP'92", W. Kuich (Ed.)], Lect. Notes in Comput. Sci., **623**, p. 101-112, Springer, 1992 (see also LITP Technical Report 92-63, Paris, 1992)
- [13] REDKO V.N., *On the determining totality of an algebra of regular events*, Ukrain. Mat. Z., **16**, p. 120-126, 1964 (in russian)
- [14] REDKO V.N., *On the algebra of commutative events*, Ukrain. Mat. Z., **16**, p. 185-195, 1964 (in russian)
- [15] SALOMAA A., SOITOLA M., *Automata-theoretic aspects of formal power series*, Springer, 1978
- [16] SIMON I., *Limited subsets of a free monoid*, [in "Proceedings 19th. Annual Symposium on Foundations of Computer Science"], IEEE, p. 143-150, 1978

- [17] SIMON I., *Recognizable sets with multiplicities in the tropical semiring*, [in "Proceedings of MFCS'88", M.P. Chytil et alii (Eds.)], Lect. Notes in Comput. Sci., **324**, p. 107-120, Springer, 1988