Direct and dual laws for automata with multiplicities

G. Duchamp, M. Flouret, É. Laugerotte and J-G. Luque
LIFAR, Faculté des Sciences et des Techniques,
76821 Mont-Saint-Aignan CEDEX France.

July 18, 2006

Abstract

We present here theoretical results coming from the implementation of the package called AMULT (automata with multiplicities in several noncommutative variables). We show that classical formulas are "almost every time" optimal, characterize the dual laws preserving rationality and also relators that are compatible with these laws.

Keywords: Automata with multiplicities; rational laws; dual laws; congruences; shuffle compatibility

1 Introduction

Noncommutative formal series (i.e. functions on the free monoid, with values in a - commutative or not - semiring) encode an infinity of data. Rational series can be represented by linear recurrences, corresponding to automata with multiplicities, and therefore they can be generated by finite state processes. Literature can be found on these "weighted automata" and their theoretical and practical (e.g. [13], [16], [11], [2], [15]) applications (recently one of us solved a conjecture in operator theory using these tools [4]). The theory was founded by Schützenberger in 1961 [18] where the link between recognizable and rational series is showed (see also [19]), extending to rings (and to semirings [1]) Kleene's result for languages [12] (corresponding to boolean coefficients). In 1974, for the case of fields, Fliess [6] extended the proof of the equivalence of minimal linear representations, using Hankel matrices. All these results allow us to construct an algorithmic processing for this series and their associated operations. In fact, classical constructions of language theory have multiplicity analogues which can be used in every domain where linear recurrences between words are handled. All these operations can be found in the package over automata with multiplicities (called AMULT). This package is a component of the environment SEA (Symbolic Environment for Automata) under development at the University of Rouen.

The structure of this paper is the following: In section 3 (the first section after introductory paragraphs), we recall the classical construction for simple rational laws $(+, ., *, \times)$ and make some remarks concerning in particular the non-commutative case. The compositions are based on polynomial formulas which has an important consequence on composition of automata choosen "at random". In fact, this first result says that the classical formulas are "almost everywhere" optimal (which is clear from experimental tests at random).

In section 4, we show that the three laws known to preserve rationality (Hadamard, shuffle and infiltration products) are of the same nature: they arise by dualizing alphabetic morphisms. Moreover, they are, up to a deformation, the only ones of this kind, which of course, shows immediately in the implemented formulas.

Section 5 is devoted to study the compatibility with relators. It was well known that, when coefficients are taken in a ring of characteristic 0, the only relators compatible with the shuffle were partial commutations ([3]). Here, we show that a similar result holds (up to the supplementary possibility of letters erasure) when K is a semiring which is not a ring. This implies the known case as a corollary. To end with, we give examples of some strange relators in characteristic 2.

2 Preamble

Let $K\langle\langle A\rangle\rangle$ be the set of noncommutative formal series with A a finite alphabet and K a semiring (commutative or not). A series denoted $S = \sum_{w\in A^*}\langle S|w\rangle w$ is recognizable iff there exists a row vector $\lambda \in K^{1\times n}$, a morphism of monoids $\mu : A^* \to K^{n\times n}$ and a column vector $\gamma \in K^{n\times 1}$, such that for all $w \in A^*$, one has $\langle S|w\rangle = \lambda\mu(w)\gamma$. Throughout the paper, we will denote by $S : (\lambda, \mu, \gamma)$ this property and say that (λ, μ, γ) is a linear representation of S, or an automaton with behaviour S. The integer n is called the *dimension* of the linear representation (λ, μ, γ) [6].

Let $K^{\rm rat}\langle\langle A\rangle\rangle$ be the set of rational noncommutative formal series, that is the set generated from the letters and the laws "." (concatenation or Cauchy product), $*$ (star operation, partially defined), $\times$ (external product) and $+$ (union or sum). The preceding four laws are called simple rational laws. The following important theorem for series [18] is the analogue of Kleene's theorem for languages (and in fact implies it).

Theorem 2.1 (Schützenberger, 1961) *A formal series is recognizable if and only if it is rational.*

Notice that, in the boolean case, $\times$ (the external product) is trivial, but it permits to take for granded that $L = \emptyset$ and then $\emptyset^* = 1$ are rational (see [12, 10]).

A reduced automaton (λ, μ, γ) is an automaton of minimal dimension among all the automata with behaviour S[1]. This minimum is called the *rank* of the series S [18]. In case K is a field, the rank of S is the dimension of the linear span of the shifts of S (see Sect. 3). It is the smallest number of nodes of an automaton with behaviour S. Here, minimization (up to an equivalence) is possible [18] (see also [1]). An explicit algorithm is given in full details in [9] (notice that this algorithm is valid as well for noncommutative multiplicities) as well as the construction of intertwining matrices.

Again, the specialisation of K to the boolean semiring $\mathbb{B}$ yields to the case of classical finite state automata.

3 Constructing usual laws

3.1 Operations on linear representations

We expound here universal formulas for constructing linear representations. They can be applied to any semiring K. For two representations of ranks n and m, it will be provided a representation of rank $r(n, m)$. Let us recall some classical facts. Classical operations on series are sum, external product and star (unary and partially defined). By definition, the sum of two series

[1] Existence is assumed by definition, unicity is proved in case K is $\mathbb{B}$ (for deterministic automata) or a (commutative or not) field [9] but is problematic in general.

R and S is

$$R+S=\sum_{w\in A^*}\big(\langle R|w\rangle+\langle S|w\rangle\big)w,$$

their concatenation (or Cauchy product)

$$R.S=\sum_{w\in A^*}\left(\sum_{uv=w}\langle R|u\rangle\langle S|v\rangle\right)w,$$

and the star of a series S

$$S^*=\sum_{n\geq 0}S^n=1+SS^*$$

if its constant term is zero (such a series is said to be proper). The preceding operations have polynomial counterparts in terms of linear representations. We gather them in the following proposition.

Proposition 3.1 *Let $R:\mathcal{A}_r=(\lambda^r,\mu^r,\gamma^r)$ (resp. $S:\mathcal{A}_s=(\lambda^s,\mu^s,\gamma^s)$) of rank n (resp. m). The linear representations of the sum, the concatenation and the star are respectively*
$R+S$:

$$\mathcal{A}_r\boxplus\mathcal{A}_s=\left(\begin{pmatrix}\lambda^r & \lambda^s\end{pmatrix},\left(\begin{array}{c|c}\mu^r(a) & 0_{n\times m}\\ \hline 0_{m\times n} & \mu^s(a)\end{array}\right)_{a\in A},\begin{pmatrix}\gamma^r\\ \gamma^s\end{pmatrix}\right)\quad,\tag{1}$$

$R.S$:

$$\mathcal{A}_r\boxdot\mathcal{A}_s=\left(\begin{pmatrix}\lambda^r & 0_{1\times m}\end{pmatrix},\left(\begin{array}{c|c}\mu^r(a) & \gamma^r\lambda^s\mu^s(a)\\ \hline 0_{m\times n} & \mu^s(a)\end{array}\right)_{a\in A},\begin{pmatrix}\gamma^r\lambda^s\gamma^s\\ \gamma^s\end{pmatrix}\right)\quad,\tag{2}$$

If $\lambda^s\gamma^s=0$, S^* :

$$\mathcal{A}_s{}^{\circledast}=\left(\begin{pmatrix}0_{1\times m} & 1\end{pmatrix},\left(\begin{array}{c|c}\mu^s(a)+\gamma^s\lambda^s\mu^s(a) & 0_{m\times 1}\\ \hline \lambda^s\mu^s(a) & 0\end{array}\right)_{a\in A},\begin{pmatrix}\gamma^s\\ 1\end{pmatrix}\right)\quad.\tag{3}$$

Proof Formula (1) is straightforward.
To prove formula (2), let $(\lambda,\mu,\gamma):=\mathcal{A}_r\boxdot\mathcal{A}_s$. One proves by induction that

$$\mu(w)=\begin{pmatrix}\mu^r(w) & \displaystyle\sum_{\substack{uw=w\\ v\neq 1}}\mu^r(u)\gamma^r\lambda^s\mu^s(v)\\ 0_{m\times n} & \mu^s(w)\end{pmatrix},$$

and then $\lambda\mu(w)\gamma = \sum_{uv=w} \lambda^r\mu^r(u)\gamma^r\lambda^s\mu^s(v)\gamma^s = \sum_{uv=w} \langle R|u\rangle\langle S|v\rangle$.
Concerning the formula (3), let $(\lambda^*, \mu^*, \gamma^*) := \mathcal{A}_s{}^{\circledast}$. Again,

$$\mu^*(w) = \begin{pmatrix} * & 0_{m\times 1} \\ \sum_{n=1}^{|w|} \sum_{\substack{u_1\cdots u_n=w \\ u_i\neq 1}} (\lambda_s\mu_s(u_1)\gamma_s)\cdots(\lambda_s\mu_s(u_{n-1})\gamma_s)(\lambda_s\mu_s(u_n)) & 0 \end{pmatrix},$$

that is

$$\begin{aligned} \lambda^*\mu^*(w)\gamma^* &= \sum_{n=1}^{|w|} \sum_{\substack{u_1\cdots u_n=w \\ u_i\neq 1}} (\lambda_s\mu_s(u_1)\gamma_s)\cdots(\lambda_s\mu_s(u_n)\gamma_s) \\ &= \sum_{n=1}^{|w|} \langle S^n|w|\rangle = \sum_{n\geq 0} \langle S^n|w|\rangle = \langle S^*|w\rangle . \square \end{aligned}$$

Remark 3.2 *1. Formulas (1) and (2) provide associative laws on triplets. They can be found explicitly in [2].*

2. Formula (3) makes sense even when $\lambda^s\gamma^s \neq 0$ (this fact will be used in the density result of Section 3.2).

3. Of course if $S : (\lambda, \mu, \gamma)$ and $\alpha \in K$ then $\alpha S := \alpha \times S : (\alpha\lambda, \mu, \gamma)$ and $S\alpha := S \times \alpha : (\lambda, \mu, \gamma\alpha)$.

4. For the sum $(\mathcal{A}_R \boxplus \mathcal{A}_S)$, $\mathcal{A}_R$ and $\mathcal{A}_S$ are just placed side by side.

The product $\mathcal{A}_R \boxdot \mathcal{A}_S$ has the following components

- **States:** *States of $\mathcal{A}_R$ and $\mathcal{A}_S$.*
- **Inputs:** *Inputs of $\mathcal{A}_R$.*
- **Transitions:** *Transitions of $\mathcal{A}_R$ and $\mathcal{A}_S$ and, for each letter a, each state r_i of $\mathcal{A}_R$ and each state s_j of $\mathcal{A}_S$, a new arc $r_i \xrightarrow{a} s_j$ is added with the coefficient $(\gamma_r)_i(\lambda_s\mu_s(a))_j$.*
- **Outputs:** *The scalar product $\lambda_s\gamma_s$ is computed once for all and there is an output on each q_i with the coefficient $(\gamma_r)_i\lambda_s\gamma_s$, the outputs of $\mathcal{A}_S$ being unchanged.*

For $\mathcal{A}^{\circledast}$, one adds a new state q_{n+1} with an input and an output bearing coefficient 1, every coefficient $\mu_{i,j}(a)$ is multiplied by $(1+\gamma_i\lambda_j)$ and new transitions $q_{n+1} \xrightarrow{a} q_i$ with coefficient $\sum_k \lambda_k\mu_{k,i}(a)$ (i.e. the "charge" of the state q_i after reading a) are added.

In the case $K = \mathbb{B}$, one recovers the classical boolean constructions.

3.2 Sharpness

Here we discuss the sharpness of the preceding constructions. Indeed, testing our package showed us that "almost everytime" the compound automata was minimal when the data were choosen at random. The crucial point in the proof of Theorem 3.5 is the fact that certain polynomial indicators are not trivial. For this, we use suited examples which are gathered in the following subsection.

a) Test automata

Let $\mathcal{B} = (S_i)_{1\leq i\leq n}$ be a finite sequence of series generating a stable module and $S = \sum_{i=1}^n \lambda_i S_i$. It is well known that the triplet

$$\left(\sum_{i=1}^n \lambda_i e_i,\ \left([\mu_{i,j}(a)]_{1\leq i,j\leq n}\right)_{a\in A},\ \sum_{i=1}^n \langle S_i|1\rangle e_i^*\right)$$

(where $e_i := (0,\cdots,1,\cdots 0)$ with the entry 1 at place i, e_i^* the transpose of e_i, and $a^{-1}S_i = \sum_{j=1}^n \big(\mu(a)\big)_{ij} S_j$ for any letter $a \in A$) is a linear representation of S. Here, to each series of one variable, $S = \sum_{p\geq 0} \alpha_p a^p$, of rank n, over a field K, we associate the triplet $\tau(S)$ given by $\mathcal{B} = (a^{-p}S)_{0\leq p\leq n-1}$.

Remark 3.3 *Of course, if $a \in A$ we consider that S belongs to $K\langle\langle A\rangle\rangle$ and this will neither affect the rank nor the following constructions.*

Lemme 3.4 *Let $S_{\alpha,n} = \dfrac{1}{(1-\alpha a)^n}$ and $T_n = \dfrac{a^{n-1}}{1-a^n}$ be $\mathbb{Q}$-series.*

1. *The rank of $S_{\alpha,n}$, $S_{\alpha,n} + S_{\beta,m}$ ($\alpha \neq \beta$), and $S_{\alpha,n}.S_{\alpha,m}$ are respectively n, $n+m$ and $n+m$.*

2. *The rank of T_n is n and that of T_n^* is $n+1$.*

Proof Straightforward. □

b) Density

The following theorem proves that, if the data are choosen "at random" in bounded domains, the compound automaton is almost surely minimal. More precisely:

Theorem 3.5 *Let A be a finite alphabet and $\mathcal{A}_i = (\lambda_i, \mu_i, \gamma_i)$ two automata of dimension n_i $(i = 1, 2)$, choosen "at random" within bounded non trivial disks of K $(K = \mathbb{R}$ or $\mathbb{C})$. Then the probability that the automaton $\mathcal{A}_1 \boxplus \mathcal{A}_2$ (resp. $\mathcal{A}_1 \boxdot \mathcal{A}_2$, $\mathcal{A}_1^{\circledast}$) be minimal is 1.*

Proof The proof rests on the following lemma.

Lemme 3.6 *There is a polynomial mapping $P : K^{|A| \times n^2 + 2n} \longrightarrow K^s$ such that $P(\lambda, \mu, \gamma) = 0$ iff (λ, μ, γ) (an automaton of dimension n) is not minimal.*

Proof of the lemma By a theorem of Schützenberger [18], the representation (λ, μ, γ) is minimal iff $\lambda\mu(K\langle A\rangle) = K^{1\times n}$ (resp. $\mu(K\langle A\rangle)\gamma = K^{n\times 1}$). As there is a prefix (resp. suffix) subset $U \subset A^*$ (resp. $V \subset A^*$) such that $\lambda\mu(U)$ (resp. $\mu(V)\gamma$) is a basis, we have $U \subset A^{<n}$ (resp. $V \subset A^{<n}$). Let $A^{<n} = \{w_1 := 1, w_2, \cdots, w_m\}$ $(m = (|A|^n - 1)/(|A| - 1))$, one constructs the $m \times n$ (resp. $n \times m$) matrix

$$L = \begin{pmatrix} \lambda\mu(w_1) \\ \lambda\mu(w_2) \\ \vdots \\ \lambda\mu(w_m) \end{pmatrix} \left(\text{resp. } M = \begin{pmatrix} \mu(w_1)\gamma & \cdots & \mu(w_m) \end{pmatrix} \right),$$

these matrices have polynomial entries in the data. In view of what precedes, minimality is equivalent to the non nullity of some $n \times n$-minor of L and of M. Sorting these minors as a vector, one get the desired polynomial mapping $K^{|A|\times n^2+2n} \longrightarrow K^s$ with $s = \binom{m}{n}$.□

The other steps go as follows.

1. For the two first operations, let $P_{\boxplus} = (\mathcal{A}_1 \boxplus \mathcal{A}_2)$, $P_{\boxdot} = P(\mathcal{A}_1 \boxdot \mathcal{A}_2)$, and prove that $P_{\boxplus}$ (resp. $P_{\boxdot}$) is not trivial using $\tau(S_{\alpha,n}) = \mathcal{A}_1$ and $\tau(S_{\beta,n}) = \mathcal{A}_2$, $\alpha \neq \beta$ (resp. $\tau(S_{\alpha,n}) = \mathcal{A}_1$ and $\tau(S_{\alpha,m}) = \mathcal{A}_2$) extended to the alphabet A in view of remark 3.3. For the star operation, prove that $P_{\circledast} = P(\mathcal{A}_1^{\circledast})$ is not trivial using $\tau(T_n) = \mathcal{A}_1$.

2. End of the proof: if $\phi : K^r \to K^s$ is polynomial and not trivial, let ν be the normalized uniform probability mesure on the product of disks, then the probability such that $\phi(\nu) \neq 0$ is 1 as $\phi^{-1}\{0\}$ is closed with empty interior.$\square$

4 Dual laws

4.1 Discussion

Let $a, b \in A$, $u, v \in A^*$, and $\odot_{\epsilon,q}$ be the law defined recursively by

$$\begin{cases} 1 \odot_{\epsilon,q} 1 = 1,\ a \odot_{\epsilon,q} 1 = 1 \odot_{\epsilon,q} a = \epsilon a, \\ au \odot_{\epsilon,q} bv = \epsilon\big(a(u \odot_{\epsilon,q} bv) + b(au \odot_{\epsilon,q} v)\big) + q\delta_{a,b}a(u \odot_{\epsilon,q} v) \end{cases}$$

with $\delta_{a,b}$ the Kronecker delta.

One immediately checks that this law is associative iff $\epsilon \in \{0, 1\}$. We get, here, the well-known shuffle ($\sqcup\!\sqcup = \odot_{1,0}$), infiltration ($\uparrow = \odot_{1,1}$) and Hadamard ($\odot = \odot_{0,1}$) products ([5], [14]). Then, $\odot_{1,q}$ is a continuous deformation between shuffle and infiltration. These laws can be called "dual laws" as they proceed from the same template that we now describe. We use an implementable realisation of the lexicographically ordered tensor product. Let us recall that the tensor product of two spaces U and V with bases $(u_i)_{i\in I}$ and $(v_j)_{j\in J}$ is $U \otimes V$, with basis $(u_i \otimes v_j)_{(i,j)\in I\times J}$, and for the sake of computation, we impose that the set $I \times J$ be lexicographically ordered.

Let $K\langle A\rangle \otimes K\langle A\rangle$ be the "double" non commutative polynomial algebra that is the set of finite sums $P = \sum_{u,v\in A^*} \langle P|u \otimes v\rangle u \otimes v$, the product being given by $(u_1 \otimes v_1)(u_2 \otimes v_2) = u_1u_2 \otimes v_1v_2$.
The construction of dual laws is based on the following pattern:

Let $c : K\langle A\rangle \to K\langle A\rangle \otimes K\langle A\rangle$, if for all $w \in A^*$, the set $\{w : \langle u\otimes v|c(w)\rangle \neq 0\}$ is finite (in which case c will be called *locally finite*), then the sum

$$u \;\square_\alpha\; v = \sum_{w\in A^*} \langle u \otimes v|c_\alpha(w)\rangle w$$

exists and defines a (binary) law $\square_\alpha$ on $K\langle A\rangle$, dual to c_α. Then, this extends to series by

$$\langle R \;\square_\alpha\; S|w\rangle := \langle R \otimes S|c_\alpha(w)\rangle \ .$$

One can show easily that the three laws $\odot$, $\sqcup\!\sqcup$ and $\uparrow$ come from coproducts defined on the words by

1. $c_\alpha(a_1a_2\cdots a_n) = c_\alpha(a_1)c_\alpha(a_2)\cdots c_\alpha(a_n)$,
2. $c_\odot(a) = a\otimes a$, $c_{\sqcup\!\sqcup}(a) = a\otimes 1 + 1\otimes a$, $c_\uparrow(a) = a\otimes 1 + 1\otimes a + a\otimes a$,

and generally $c_{\epsilon,q}(a) = \epsilon(a\otimes 1 + 1\otimes a) + qa\otimes a$.
The preceding computation scheme has an immediate consequence on the implementation of the laws.

Proposition 4.1 *Let $R : (\lambda^r, \mu^r, \gamma^r)$ and $S : (\lambda^s, \mu^s, \gamma^s)$. Then*

$$R \,\square_\alpha\, S : (\lambda^r \otimes \lambda^s, \mu^r \otimes \mu^s \circ c_\alpha, \gamma^r \otimes \gamma^s) \;.$$

Proof We verify it by duality. Indeed, for $w \in A^*$,

$$\begin{aligned}
\langle R\otimes S|c_\alpha(w)\rangle &= \textstyle\sum_{u,v\in A^*} \langle \lambda^r\otimes\lambda^s\,(\mu^r\otimes\mu^s(u\otimes v))\,\gamma^r\otimes\gamma^s \times u\otimes v|c_\alpha(w)\rangle \\
&= \textstyle\sum_{u,v\in A^*} \lambda^r\otimes\lambda^s\,(\mu^r\otimes\mu^s(u\otimes v))\,\gamma^r\otimes\gamma^s.\langle u\otimes v|c_\alpha(w)\rangle \\
&= \lambda^r\otimes\lambda^s\left(\textstyle\sum_{u,v\in A^*} \mu^r\otimes\mu^s\langle u\otimes v|c_\alpha(w)\rangle(u\otimes v)\right)\gamma^r\otimes\gamma^s \\
&= \lambda^r\otimes\lambda^s\left(\mu^r\otimes\mu^s \textstyle\sum_{u,v\in A^*}\langle u\otimes v|c_\alpha(w)\rangle(u\otimes v)\right)\gamma^r\otimes\gamma^s \\
&= \lambda^r\otimes\lambda^s\,(\mu^r\otimes\mu^s c_\alpha(w))\,\gamma^r\otimes\gamma^s.\square
\end{aligned}$$

Let us study among laws which ones are associative.

Proposition 4.2 *Let K be a field, and $c_\alpha : K\langle A\rangle \to K\langle A\rangle\otimes K\langle A\rangle$ the alphabetic morphism defined on the letters of A by*

$$c_\alpha(a) = \sum_{p,q\geq 0} \alpha_{p,q} a^p \otimes a^q$$

with $c_\alpha(1) = 1\otimes 1$ ($\alpha_{p,q} = \alpha_{p,q}(a)$ may vary from one letter to one another).

1. *The morphism c_α is locally finite iff $\alpha_{0,0} = 0$.*
2. *Providing $\alpha_{0,0} = 0$, the following assertions are equivalent.*
   (a) *The law $\square_\alpha$ defined by $\langle u \,\square_\alpha\, v|w\rangle := \langle u\otimes v|c_\alpha(w)\rangle$ ($u, v, w \in A^*$) is associative.*
   (b) *The coefficients $\alpha_{p,q}$ satisfy the relations $\alpha_{p,q} = 0$ for p or $q \geq 2$, $\alpha_{0,1}, \alpha_{1,0} \in \{0, 1\}$ and $\alpha_{0,1}\alpha_{1,1} = \alpha_{1,0}\alpha_{1,1}$.*

3. *Providing (2.2b), the element* 1_{A^*} *is a unit for* $\Box_\alpha$ *iff* $\alpha_{0,1} = \alpha_{1,0} = 1$.

Proof

1. We have $c_\alpha(a) = \alpha_{0,0} 1 \otimes 1 + \sum_{p+q \geq 1} \alpha_{p,q} a^p \otimes a^q$, and then for all $n \geq 0$, $c_\alpha(a^n) = \alpha_{0,0}^n 1 \otimes 1 + \sum_{p+q \geq 1} \beta_{p,q} a^p \otimes a^q$ for some $\beta_{p,q}$. If $\alpha_{0,0}$ were not zero, the term $1 \otimes 1$ would appear in an infinity of words, and then c_α would not be locally finite.
Conversely, if $\alpha_{0,0}(a) = 0$ (for every letter), then $c_\alpha(a) = \sum_{p+q \geq 1} \alpha_{p,q} a^p \otimes a^q$ and for all word $w = a_1 \cdots a_n \in A^*$,

$$c_\alpha(w) = \sum_{\substack{p_i + q_i \geq 1 \\ 1 \leq i \leq n}} \left(\prod_{i=1}^{n} \alpha_{p_i,q_i}(a_i) \right) a_1^{p_1} \cdots a_n^{p_n} \otimes a_1^{q_1} \cdots a_n^{q_n}.$$

As $p_i + q_i \geq 1$, we have $\sum_{i=1}^{n} (p_i + q_i) \geq n$, that is to say

$$\langle c_\alpha(w), u \otimes v \rangle \Rightarrow \begin{cases} w| \leq |u| + |v| \\ Alph(w) = Alph(u) \cup Alph(v) \end{cases}$$

where $u := a_1^{p_1} \cdots a_n^{p_n}$ and $v := a_1^{q_1} \cdots a_n^{q_n}$.
To summarize, the set

$$S = \{ w / \langle u \otimes v | c_\alpha(w) \rangle \neq 0 \}$$

has bounded lengths and its alphabet is finite, S is then finite.

2. First, remark that (2.2a) is equivalent to the condition

$$(Id \otimes c_\alpha) \circ c_\alpha = (c_\alpha \otimes Id) \circ c_\alpha. \tag{4}$$

The law $\Box_\alpha$ is associative iff for all words u_1, u_2, $u_3 \in A^*$, we have

$$(u_1 \Box_\alpha u_2) \Box_\alpha u_3 = u_1 \Box_\alpha (u_2 \Box_\alpha u_3)$$

that is to say that, for all $w \in A^*$,

$$\langle (u_1 \Box_\alpha u_2) \Box_\alpha u_3 | w \rangle = \langle u_1 \Box_\alpha (u_2 \Box_\alpha u_3) | w \rangle \ .$$

But one has

$$\begin{aligned} \langle (u_1 \Box_\alpha u_2) \Box_\alpha u_3 | w \rangle &= \langle (u_1 \Box_\alpha u_2) \otimes u_3 | c_\alpha(w) \rangle \\ &= \langle u_1 \otimes u_2 \otimes u_3 | (c_\alpha \otimes Id) \circ c_\alpha(w) \rangle \end{aligned}$$

and

$$\begin{aligned} \langle u_1 \Box_\alpha (u_2 \Box_\alpha u_3) | w \rangle &= \langle u_1 \otimes (u_2 \Box_\alpha u_3) | c_\alpha(w) \rangle \\ &= \langle u_1 \otimes u_2 \otimes u_3 | (Id \otimes c_\alpha) \circ c_\alpha(w) \rangle. \end{aligned}$$

As u_1, u_2, u_3, w are arbitrary, we get $(c_\alpha \otimes Id) \circ c_\alpha = (Id \otimes c_\alpha) \circ c_\alpha$.
To show the equivalence between (2.2b) and (4), suppose first that (4) holds. We endow $\mathbb{N}^k$ with the lexicographic order (reading from left to right for instance) which is compatible with addition and will be denoted $\prec$ (here, $k = 2, 3$). Then, if it is not zero, $c_\alpha(a)$ can be written

$$\alpha_{\overline{p},\overline{q}} a^{\overline{p}} \otimes a^{\overline{q}} + \sum_{(p,q) \prec (\overline{p},\overline{q})} \alpha_{p,q} a^p \otimes a^q \ ,$$

$(\overline{p}, \overline{q})$ being the highest couple of exponents in the support. Then,

$$\begin{aligned} (c_\alpha \otimes Id) \circ c_\alpha(a) &= \alpha_{\overline{p},\overline{q}} c_\alpha(a^{\overline{p}}) \otimes a^{\overline{q}} + \sum_{(p,q) \prec (\overline{p},\overline{q})} \alpha_{p,q} c_\alpha(a^p) \otimes a^q \\ &= \alpha_{\overline{p},\overline{q}}^{\overline{p}+1} a^{(\overline{p})^2} \otimes a^{\overline{pq}} \otimes a^{\overline{q}} + \sum_{(p,q,r) \prec (\overline{p}^2, \overline{pq}, \overline{q})} \beta_{p,q,r} a^p \otimes a^q \otimes a^r, \end{aligned}$$

but

$$\begin{aligned} (Id \otimes c_\alpha) \circ c_\alpha(a) &= \alpha_{\overline{p},\overline{q}} a^{\overline{p}} \otimes c_\alpha(a^{\overline{q}}) + \sum_{(p,q) \prec (\overline{p},\overline{q})} \alpha_{p,q} a^p \otimes c_\alpha(a^q) \\ &= \alpha_{\overline{p},\overline{q}}^{\overline{q}+1} a^{\overline{p}} \otimes a^{\overline{pq}} \otimes a^{(\overline{q})^2} + \sum_{(p,q,r) \prec (\overline{p}, \overline{pq}, \overline{q}^2)} \beta_{p,q,r} a^p \otimes a^q \otimes a^r. \end{aligned}$$

Necessarily, $\overline{p} = \overline{p}^2$ and $\overline{q} = \overline{q}^2$, which is only possible when $\overline{p} \in \{0, 1\}$ and $\overline{q} \in \{0, 1\}$ and then $\alpha_{p,q} = 0$ for p or $q \geq 2$. The equality now reads

$$\begin{gathered} \alpha_{1,0} a \otimes 1 \otimes 1 + \alpha_{0,1}^2 1 \otimes 1 \otimes a + \alpha_{0,1}\alpha_{1,1} a \otimes 1 \otimes a \\ = \\ \alpha_{1,0}^2 a \otimes 1 \otimes 1 + \alpha_{0,1} 1 \otimes 1 \otimes a + \alpha_{1,0}\alpha_{1,1} a \otimes 1 \otimes a, \end{gathered}$$

which implies (2.2b). The converse is a straightforward computation.

3. The condition 1_{A^*} is a unit for $\Box_\alpha$ implies that, for $a \in A$, we have
$$\begin{aligned} 1\Box_\alpha a = a\Box_\alpha 1 = a \quad &\Leftrightarrow \quad \langle 1\Box_\alpha a|a\rangle = \langle a\Box_\alpha 1|a\rangle = 1 \\ &\Leftrightarrow \quad \langle 1\otimes a|c_\alpha(a)\rangle = \langle a\otimes 1|c_\alpha(a)\rangle = 1 \\ &\Leftrightarrow \quad \begin{cases} \langle 1\otimes a|\sum_{p,q\geq 0}\alpha_{p,q}a^p\otimes a^q\rangle = 1 \\ \langle a\otimes 1|\sum_{p,q\geq 0}\alpha_{p,q}a^p\otimes a^q\rangle = 1 \end{cases} \\ &\Leftrightarrow \quad \alpha_{0,1} = \alpha_{1,0} = 1. \end{aligned}$$
Conversely, the latter implies that, for each $w \in A^*$, $1\Box_\alpha w = w\Box_\alpha 1 = w$. $\Box$

Remark 4.3 *1. For just a commutative law the condition $\alpha_{p,q} = \alpha_{q,p}$ is sufficient. Moreover, the condition (2.2b) implies $\alpha_{0,1}, \alpha_{1,0} \in \{0,1\}$.*

2. *If $\alpha_{11} \neq 0$, the only dual laws which are associative ones are*

$$c_{\epsilon,q}(a) = \epsilon(a\otimes 1 + 1\otimes a) + qa\otimes a$$

with parameters $\epsilon \in \{0,1\}$ and $q \in K^\times$. Notice that in this case they are all commutative.

3. *If $\alpha_{11} = 0$, we get two degenerate laws (opposite between theimselves) which are not in the familly $(\Box_{\epsilon,q})$ with $\epsilon \in \{0,1\}$ and $q \in K$ corresponding to $\alpha_{10} = 1$ and $\alpha_{10} = 0$ (resp. $\alpha_{01} = 0$ and $\alpha_{10} = 1$). This laws are not commutative when $A \neq \emptyset$.*

4.2 Usual dual laws

a) Shuffle and infiltration product ($\epsilon = 1$, $q \in \{0,1\}$)

Proposition 4.4 *Let $R : (\lambda_1, \mu_1, \gamma_1)$ (resp. $S : (\lambda_2, \mu_2, \gamma_2)$) with rank n (resp. m).*

1. *Automata corresponding to shuffle and infiltration products are respectively*

$$R⧢S : \left(\lambda_1\otimes\lambda_2, (\mu_1(a)\otimes I_2 + I_1\otimes\mu_2(a))_{a\in A}, \gamma_1\otimes\gamma_2\right) , \quad (5)$$

and

$$R\uparrow S : \left(\lambda_1\otimes\lambda_2, (\mu_1(a)\otimes I_2 + I_1\otimes\mu_2(a) + \mu_1(a)\otimes\mu_2(a))_{a\in A}, \gamma_1\otimes\gamma_2\right) . \quad (6)$$

2. *The bound nm is sharp in both cases.*

3. *The density result of theorem 3.5 holds.*

Proof Concerning point (2), an example reaching the bound for any rank is to consider the families of series $S_n = a^{n-1}$ and $T_n = b^{n-1}$ of rank n. The shuffle product $S_n \sqcup\!\sqcup S_m = a^{n-1} \sqcup\!\sqcup b^{m-1}$ $(a \neq b \in A)$ has a minimal linear representation of rank nm. The same example is valid for the infiltration product as, for $a \neq b$, $a^n \uparrow b^m = a^n \sqcup\!\sqcup b^m$. $\square$

The proposition yields the following.

Definition 4.5 *Let $\mathcal{A}_i = (\lambda_i, \rho_i, \gamma_i)$ with $i = 1, 2$ then we define $\mathcal{A}_1 \sqcup\!\sqcup \mathcal{A}_2$ and $\mathcal{A}_1 \Uparrow \mathcal{A}_2$ by the formulas 5 and 6.*

Remark 4.6 *These laws are already associative at the level of automata.*

b) Hadamard product ($\epsilon = 0$, $q = 1$)

We recall that the Hadamard product ([7], [19]) of two series is the pointwise product of the corresponding functions (on words). We can use the machinery above to describe an automata for it.

Proposition 4.7 *Let $R : (\lambda^r, \mu^r, \gamma^r)$ (resp. $S : (\lambda^s, \mu^s, \gamma^s)$) with rank n (resp. m). A representation of the Hadamard product is*

$$R \odot S : \left(\lambda^r \otimes \lambda^s, (\mu^r(a) \otimes \mu^s(a))_{a \in A}, \gamma^r \otimes \gamma^s\right) \quad ,$$

and the bound is asymptotically sharp.

Proof Let $\beta(n, m) := sup_{\substack{rank(R)=n \\ rank(S)=m}} rank(R \odot S)$. We claim that

$$\limsup_{n,m \to +\infty} \frac{\beta(n, m)}{nm} = 1 \quad ,$$

(what we mean by "asymptotically sharp").
Indeed, let us consider the Hadamard product of two series of the family

$$S_n = \sum_{k \geq 0} a^{nk} = \frac{1}{(1 - a^n)} \quad .$$

The rank of S_n is n, and

$$\begin{aligned} S_n \odot S_m &= \textstyle\sum_{k \geq 0} a^{nk} \odot \sum_{k' \geq 0} a^{mk'} = \sum_{p \geq 0} \langle S_n | a^p \rangle \langle S_m | a^p \rangle a^p \\ &= \textstyle\sum_{k \geq 0} a^{lcm(n,m)k} = S_{lcm(n,m)} \quad . \end{aligned}$$

Thus, for n and m coprime, the rank of the product is nm, which proves the claim. $\square$

5 Shuffle of automata compatible with relators

In this section, we deal with automata whose actions can be coded by elements of a monoid defined by generators and relations. The first interesting case historically encountered is the trace monoid but, as we will see below, some results can be extended to the general case. To end with, we study the relators permitting the shuffle of automata.

5.1 Series over a monoid and automata

In the whole section $R \subset A^* \times A^*$ is a relator and $\equiv_R$ is the congruence relation generated by R.

Definition 5.1 *1. Let $f : A^* \to X$ (X a set) and $\equiv$ be a congruence on A^*, we will say that f is $\equiv -$compatible if*

$$u \equiv v \Rightarrow f(u) = f(v).$$

2. An automaton $\mathcal{A} = (\lambda, \mu, \gamma)$ is said $\equiv$-compatible if $\mu : A^* \to K^{n\times n}$ is.

Remarks 1 *1. The coarsest congruence compatible with a function f is known as the syntactic congruence of f. A non trivial result says that the syntactic congruence of all Greene's invariants is the plactic equivalence [17].*

2. If an automaton $\mathcal{A}$ is $\equiv$-compatible, then it is straigthforward to see that its behaviour is.

3. We can restate geometrically (2) of definition 5.1 as :

For each state q and $(u, v) \in R$ then $q.u = q.v$.

4. If $f : A^* \to M$ is a morphism of monoids (this is the case for the data μ of automata) compatibility has just to be tested on R, more precisely

$$(\forall (u, v) \in R)(f(u) = f(v)) \Rightarrow f \text{ is } \equiv \text{-compatible.}$$

5. *If S, T are $\equiv$-compatible, so is $S \odot T$ (which is by no means the case for $\sqcup\!\sqcup$ and $\uparrow$, see discussion below).*

The converse of remark 1(2) is true for minimal automata over fields as shown just below.

Proposition 5.2 *Suppose that K is a field (commutative or skew).*
Let $S : A^* \to K$ be a rational series, the following assertions are equivalent:

1. *S is $\equiv$-compatible.*

2. *The minimal automata of S are $\equiv$-compatible.*

Proof Let us first prove that (1)⇒(2). By the minimality of $\mathcal{A}$, it exists words $u_1, u_2, \ldots, u_n, v_1, v_2, \ldots v_n$ such that the column block matrix $L = (\lambda\mu(u_i))_{i\in[1,n]}$ and the line block matrix $R = (\mu(v_i)\gamma)_{i\in[1,n]}$ are invertible $n \times n$ matrices (K may not be commutative see [8]). Thus, if $w \equiv w'$ then

$$\begin{aligned} L\mu(w)R &= (\lambda\mu(u_i w v_j)\gamma)_{1\le i,j\le n} \\ &= (\langle S|u_i w v_j\rangle)_{1\le i,j\le n} \\ &= (\langle S|u_i w' v_j\rangle)_{1\le i,j\le n} \\ &= (\lambda\mu(u_i w' v_j)\gamma)_{1\le i,j\le n} \\ &= L\mu(w')R \end{aligned}$$

And thus, $\mu(w) = \mu(w')$.
The converse is straightforward from remark 1(4).□

It is clear that $\equiv$-compatibility is stable under linear combinations (i.e. if the series $(S_{i,j})_{(i,j)\in I\times J}$ are $\equiv$-compatible so is $\sum \alpha_i S_{i,j} \beta_j$). However, the Cauchy product of two compatible series may not be so, as shown by the example: $ab \equiv ba$, $S = a$ and $T = b$.

5.2 Study for general semirings

In case of a field, the compatibility of automata with shuffle product is equivalent to the compatibility of the coproduct with the congruence and its square. More precisely

Theorem 5.3 *1. Suppose that K is a field. Let $\equiv$ be a congruence with finite fibers*[2]*, the following assertions are equivalent.*

(a) If $\mathcal{A}_1$ and $\mathcal{A}_2$ are two $\equiv$-compatible automata so is $\mathcal{A}_1 ⧢ \mathcal{A}_2$.

(b) The coproduct respects $\equiv$ in the following sense:
For every $(u, v) \in A^* \times A^*$, we have

$$u \equiv v \Rightarrow c(u) \equiv^{\otimes 2} c(v).$$

where $\equiv^{\otimes 2}$ is the "square" of $\equiv$ defined as the kernel of the natural mapping

$$K\langle A\rangle \otimes K\langle A\rangle \to K[A^*/_{\equiv}] \otimes K[A^*/_{\equiv}].$$

2. The preceding conditions imply that if S and T are two $\equiv$-compatible series, so are $S ⧢ T$, $S \uparrow T$.

Proof To prove (1.1b) $\Rightarrow$ (1.1a), it suffices to remark that $\mu = (\mu_1 \otimes \mu_2) \circ c$ where μ_1, μ_2 and μ are respectively the associated morphisms of the automata $\mathcal{A}_1$, $\mathcal{A}_2$ and $\mathcal{A}_1 ⧢ \mathcal{A}_2$.
Now, we prove that (1.1a) $\Rightarrow$ (1.1b). We consider the (product order) relation on the multidegrees ($\alpha, \beta \in \mathbb{N}^{(A)}$):

$$(\alpha \leq \beta) \Leftrightarrow (\forall a \in A)(\alpha(a) \leq \beta(a)).$$

Let w be a word. In the sequel, we denote $[w]$ the mapping $(a \to |w|_a)$ its multidegree and $Cl(w)$ its equivalence class modulo $\equiv$. Let $w_1 \equiv w_2$ be two equivalent words. Consider

$$t_1 = \sup_{w \in Cl(w_1)} [w].$$

And let $\mathcal{C}_1 \ldots \mathcal{C}_k$ be the classes which contain at least a word whose multidegree is less than t_1, and we set

$$t_2 = \sup_{w \in \cup_{i=1}^k \mathcal{C}_i} [w]$$

(t_1 and t_2 are well defined due to the "finite fibers" hypothesis).
With $A^{\leq t_2} := \{w/[w] \leq t_2\}$, let us define the following truncation of $\equiv$ by

$$u \sim v \Leftrightarrow \begin{cases} Cl(u) \not\subseteq A^{\leq t_2} \text{ and } Cl(v) \not\subseteq A^{\leq t_2} \\ \text{or} \\ Cl(u) = Cl(v) \end{cases}$$

[2] i.e. the classes of $\equiv$ are finite sets.

The following lemma is easy.

Lemme 5.4 *1. The equivalence $\sim$ is a congruence coarser than $\equiv$.*

2. The classes of $\sim$ are $\mathcal{C}_1, \mathcal{C}_2, \dots, \mathcal{C}_k, \mathcal{C}_{k+1}, \dots \mathcal{C}_{p-1}$ and

$$\mathcal{C}_p = \bigcup_{Cl(w) \not\subseteq A^{\leq t_2}} Cl(w)$$

where $\mathcal{C}_1, \dots, \mathcal{C}_{p-1}$ are equivalence classes of $\equiv$ precisely the equivalence classes of $\equiv$ which are subsets of $A^{\leq t_2}$.

3. In particular $w_1 \sim w_2$ and $[w_i] \leq t_1$ implies $w_1 \equiv w_2$.

For every $a \in A$, we define $\mu(a)$ as the matrix (with respect to the basis $(\mathcal{C}_j)_{j\in[1,p]}$) of the linear transformation $\overline{u} \to \overline{a}.\overline{u} \in A^*/_\sim$, where $\overline{u}$ denotes the class of u for $\sim$. More explicitly

$$\mu(w) : \mathcal{C}_j \to \overline{w}.\mathcal{C}_j.$$

Then, μ is $\equiv$-compatible and hence the automata $\mathcal{A}_{i,j} = (e_{\mathcal{C}_i}, \mu, e^*_{\mathcal{C}_j})$ (with $(e_{\mathcal{C}_i})_{1\leq i\leq p}$ being the canonical basis of $K^{p\times 1}$) are $\equiv$-compatible. Then, by (1a) the p^4 automata

$$\mathcal{A}_{i_1,j_1} ⧢ \mathcal{A}_{i_2,j_2} = (e_{\mathcal{C}_{i_1}} \otimes e_{\mathcal{C}_{i_2}}, \mu \otimes I_p + I_p \otimes \mu, e^*_{\mathcal{C}_{j_1}} \otimes e^*_{\mathcal{C}_{j_2}})$$

are $\sim$-compatible. This, implies that the morphism $\nu : A^* \to K^{p^2\times p^2}$ defined by $\nu(a) = \mu(a) \otimes I_p + I_p \otimes \mu(a)$ for each $a \in A$, is $\sim$-compatible. Now, as $w_1 \equiv w_2$, one has

$$\begin{aligned}\textstyle\sum_{I+J=[1\dots n]} \mu(w_1[I]) \otimes \mu(w_1[J]) &= \nu(w_1)\\ &= \nu(w_2)\\ &= \textstyle\sum_{I+J=[1\dots n]} \mu(w_2[I]) \otimes \mu(w_2[J])\end{aligned}$$

which proves (evaluating this linear transformation on $1 \otimes 1$) that

$$\sum_{I+J=[1\dots n]} w_1[I] \otimes w_1[J] \sim^{\otimes 2} \sum_{I+J=[1\dots n]} w_2[I] \otimes w_2[J]$$

but, as $[w_i[I]], [w_i[J]] \leq t_1$ for $I, J \subset [1..n]$, lemma 5.4 implies $c(w_1) \equiv^{\otimes 2} c(w_2)$.

Now, we prove (1) $\Rightarrow$ (2). In fact we have, $\langle S \sqcup\!\sqcup T | w \rangle = \langle S \otimes T | c(w) \rangle$. As S and T are $\equiv$-compatible, the assertion (1.1b) implies the $\equiv$-compatibility of $S \sqcup\!\sqcup T$.$\square$

In fact (1.1b) can be formulated without the hypothesis over K and the fibers of $\equiv$ and then (1.1b) $\Rightarrow$ (1.1a) in the (very) general case.
According to this remark we can give the following definition.

Definition 5.5 *Let K be a semiring. A congruence will be said $K - \sqcup\!\sqcup$ compatible if (1.1b) is fullfilled.*

Partial commutations are $K - \sqcup\!\sqcup$ compatible for any K, so does , more generally, the relators $a^{p^{e_1}} b^{p^{e_2}} \equiv b^{p^{e_2}} a^{p^{e_1}}$ and $a^{p^{e_1}} = b^{p^{e_2}}$ for $K = \mathbb{Z}/p\mathbb{Z}$ with p prime.

In the next paragraph we completely solve the problem of $K - \sqcup\!\sqcup$ compatibility for semirings which are not rings.
The case when K is a ring of characteristic 0 is known (see [3]) but the tools developped below shows this again by a different argument.

5.3 Generalities

In the following we need some elementary properties.

Lemme 5.6 *Let $\phi : K_1 \to K_2$ be a morphism of semirings then*

1. *If $\equiv$ is $K_1 - \sqcup\!\sqcup$ compatible then it is $K_2 - \sqcup\!\sqcup$ compatible.*

2. *If ϕ is into, the converse is true.*

Proof Straightforward, remarking that the mapping $\mathbb{N}.1_{K_1} \xrightarrow{\phi} \mathbb{N}.1_{K_2}$ is surjective.$\square$

Remark 5.7 *This lemma implies that if a congruence is $\mathbb{N} - \sqcup\!\sqcup$ compatible then it is $K - \sqcup\!\sqcup$ compatible for each semiring K. In fact, a congruence is $K - \sqcup\!\sqcup$ compatible if and only if it is $\mathbb{N}.1_K - \sqcup\!\sqcup$ compatible.*

Let K be a semiring, in the following we discuss according to the subsemiring $K_0 = \mathbb{N}.1_K$. The semiring K_0 is entirely characterized by the monoid structure of $(K_0, +)$ which depends of the two following parameters:

$$m(K) = inf\{e \in \mathbb{N} / \exists r \in \mathbb{N}^*, e.1_k = (e+r).1_K\} \in \mathbb{N} \cup \{+\infty\}$$

and if $m(K) \neq \infty$

$$l(K) = inf\{r \in \mathbb{N}^*/m(K).1_K = (m(K)+r).1_K\} \in \mathbb{N}^*.$$

Lemme 5.8 *Let R be a relator on A^*. Then, $\equiv_R$ is $K - ⧢$ compatible if and only if for each pair $(w_1, w_2) \in R$ we have $c(w_1) \equiv_R^{\otimes 2} c(w_2)$.*

Proof The "if" part is straightforward considering the morphism

$$c : A^*/_{\equiv} \to K[A^*/_{\equiv}] \otimes K[A^*/_{\equiv}].$$

The converse is obvious.□

Lemme 5.9 *Each congruence generated by relators under the form $a \equiv b$ or $cd \equiv dc$ with $a, b, c, d \in A$ is $K - ⧢$ compatible.*

Proof According to lemma 5.8, it suffices to check that

$$c(a) = a \otimes 1 + 1 \otimes a \equiv^{\otimes 2} b \otimes 1 + 1 \otimes b = c(b)$$

for each $a \equiv b \in A$ and

$$\begin{array}{rl} c(cd) & = cd \otimes 1 + c \otimes d + d \otimes c + 1 \otimes cd \\ & \equiv^{\otimes 2} dc \otimes 1 + c \otimes d + d \otimes c + 1 \otimes dc \\ & = c(dc) \end{array}$$

for each pair of letters $(a, b) \in A^2$ such that $cd \equiv dc$.□

Lemme 5.10 *Let $B \subseteq A$ be a subalphabet. If $\equiv$ is $K - ⧢$ compatible then so is the congruence $\equiv_B := \equiv \cap B^2$.*

Proof Direct computation.□

The following general lemma will be used later.

Lemme 5.11 *Let $u \in A^+$ be a word and let n be the maximal integer such that u can be written under the form $u = u_1 a^n$ with $u_1 \in A^*$, $a \in A$ and $n \geq 1$ then*

$$\langle c(u) | u_1 \otimes a^n \rangle = 1.$$

Proof Suppose that $n = 1$ then it is easy to verify that $u_1 \otimes a$ appears only one times in the polynomial $c(u)$. By induction on n, we find the result.□

5.4 The case when $m(K) \neq 0$

a) The boolean case

We first consider the case where $K = \mathbb{B}$ is the boolean semiring. The $\mathbb{B} - \sqcup\!\sqcup$ compatible congruences are caracterised by the following result.

Proposition 5.12 *A congruence is $\mathbb{B} - \sqcup\!\sqcup$ compatible if and only if it is generated by the following relators*

$$\begin{cases} a \equiv 1 & (LE) \\ a \equiv b & (LI) \\ ab \equiv ba & (LC) \end{cases}$$

Proof Let us first prove that a congruence is $\mathbb{B} - \sqcup\!\sqcup$ compatible if it is generated by relators (LE), (LI) or (LC). According lemmas 5.8 and 5.9, it suffices to prove that the relators (LE) are $\mathbb{B} - \sqcup\!\sqcup$ compatible. In fact, we have

$$a \equiv 1 \Rightarrow c(a) = a \otimes 1 + 1 \otimes a \equiv^{\otimes 2} (1+1) \otimes 1 = c(1)$$

which proves the result.

Now, we prove the converse. Let $A' = \{a \in A / a \not\equiv 1\}$ and $S \subseteq A'$ be a section of $\equiv \cap A' \times A'$. It is clear that if (LE) is a list of couples $\{(a,1)\}_{a \in A - A'}$ and (LI) a list of couples $\{(a,b)\}_{x \equiv y, x \in S, y \in A' - S}$, then $\equiv$ is generated by $\equiv_S := \equiv \cap S^* \times S^*$, (LI) and (LE). So, it suffices to prove that $\equiv_S$ is generated by (LC) relators. Let us prove first, that $\equiv_S$ is multihomogeneous. Let $\equiv_m$ be the multihomogeneous part of $\equiv_S$ (i.e. the congruence generated by the pairs $(u,v) \in \equiv_S$ such that $[u] = [v]$). Let (u,v) be a pair of words such that $u \equiv_S v$ and $u \not\equiv_m v$ with $|u|$ minimal. Suppose that $u = 1$, if $v \neq 1$ we can set $v = v_1 a$ with $a \in S$. Then, as by lemma 5.10 $\equiv_S$ is again $\mathbb{B} - \sqcup\!\sqcup$ compatible,

$$\langle \overline{v}_1 \otimes \overline{a} | c(\overline{1}) \rangle = 1$$

($\overline{w}$ denoting the class of w for $\equiv$), but $c(1) = 1 \otimes 1$ which implies $a \equiv_S 1$ and contradicts the construction of S. Then, $u \neq 1$ and we can write u under the form $u = u_1 a$ with $a \in S$. As $\langle c(u) | u_1 \otimes a \rangle = 1$, it exists two complementary subwords $v[I]$ and $v[J]$ of v such that $v[I] \otimes v[J] \equiv_S^{\otimes 2} u_1 \otimes a$. But, $v \equiv_S u_1 a \equiv_S v[I]v[J]$ which implies $v \equiv_m v[I]v[J]$ and proves $\equiv_S = \equiv_m$. Let $\equiv_\theta$ be the congruence generated by pairs (ab, ba) with $a, b \in S$ and $ab \equiv_S ba$.

Lemme 5.13 *Let $u \equiv_S v$ with $v \in S^* a$ then it exists $u_1 \equiv_\theta u$ with $u_1 \in S^* a$.*

Proof We have $[u] = [v]$ from what precedes and in particular $|u|_a \neq 0$. Let $u_1 = u_2 a u_2'$ be a word such that $u_1 \equiv_\theta u$, $|u_2'|_a = 0$ and $|u_2'|$ minimal. Suppose that $u_2' \neq 1$, then we can write $u_2' = bu_3$ with $b \in S$ and $u_3 \in S^*$. Let $a^q b = (u_1)_I$ be the subword of u_1 with q maximal ($q = |u_a|$, the word is unique but the equality has $|u_2'|_b$ solutions in I), it exists two complementary subwords $v[I]$ and $v[J]$ such that $a^q b \otimes w \equiv_S^{\otimes 2} v[I] \otimes v[J]$ where w is a subword of u complementary of $a^q b$. Then $a^q b \equiv_S v[I]$ and then, as $|v[I]|_a = |u|_a = |v|_a$, $v[I] = a^{q-i} b a^i$ with $i \geq 1$. This implies $ab \otimes a^{q-1} \equiv_m^{\otimes 2} ab \otimes a^{q-1} + ba \otimes a^{q-1}$. As $\equiv_S$ is multihomogeneous, we have necessarily $ab \equiv_S ba$. It follows $u \equiv_\theta u_2 abu_3 \equiv_\theta u_2 bau_3$ which contradicts the minimality of $|u_2'|$ and proves the result.□

End of the proof of proposition If $\equiv_S \neq \equiv_\theta$, let (u, v) be a couple of words such that $u \equiv_S v$ and $u \not\equiv_\theta v$ with $|u| + |v|$ minimal.
Let a be a letter such that $u \equiv_\theta u_1 a^k = u', v \equiv_\theta v_1 a^l = v'$ with $k, l \neq 0, k + l \geq 2$ maximal (the existence of a such letter follows from lemma 5.13). Without restriction we can suppose that $k \leq l$. We have $\langle u_1 \otimes a^k | c(u') \rangle = 1$ and then it exists two complementary subwords $v'[I]$ and $v'[J]$ of v' such that $u_1 \otimes a^k \equiv_S^{\otimes 2} v'[I] \otimes v'[J]$. Hence, the multihomogeneity of $\equiv_S$ gives $v'[J] = a^k$ and we can write $v'[I] = v_2 a^\alpha$ where v_2 is a subword of v_1. If $\alpha > 0$, we have $u_1 \equiv_S v_2 a^\alpha$ and by lemma 5.13, it would exist $u_2 \in S^*$ such that $u_1 \equiv_\theta u_2 a$. Hence, $u \equiv_\theta u_2 a^{k+1}$ which contradicts the maximality of $k + l$. Thus $\alpha = 0$ and $v'[I] \notin S^* a$ is a subword of v_1, we have thus $|u| - k = |u_1| = |v'[I]| \leq |v_1| = |v| - l$ but we had $k \leq l$ then $k = l$. Now $v_1 = v'[I]$ and then $u_1 \equiv_\theta v_1$ which implies

$$u \equiv_\theta u_1 a^k \equiv_\theta v_1 a^k \equiv_\theta v$$

a contradiction, this proves the result.□

b) Other semirings such that $m(K) \neq 0$

Theorem 5.14 *Let K be a semiring such that $m(K) \neq 0$. Then a congruence $\equiv$ is $K - \sqcup\!\sqcup$ compatible if and only if*

1. *If $1_K + 1_K = 1_K$, it is generated by relators (LE), (LI) and (LC).*

2. *If $1_K + 1_K \neq 1_K$, it is generated by relators (LI) and (LC).*

In the two cases, $A^*/\equiv$ is a partially commutative monoid.

Proof The assertion (1) can be easily proved using lemma 5.6 and proposition 5.12. Let us show the assertion (2). Let K be a semiring such that $m(K) \neq 0$ and $1_K + 1_K \neq 1_K$, then it exists a morphism from K onto $\mathbb{B}$ (this morphism sends 0 on 0 and $x \neq 0$ on 1). Let $\equiv$ be a $K - \sqcup\!\sqcup$ compatible congruence, by lemma 5.6 $\equiv$ is so $\mathbb{B} - \sqcup\!\sqcup$ compatible and then it is generated by (LE), (LI) or (LC) relators. A fast computation shown that the only possibilities are (LI) and (LC). Which gives the result.□

Corollary 5.15 *[3] Let K be a ring of characteristic 0. A congruence is $K - \sqcup\!\sqcup$ compatible if and only if it is generated by relators of the type (LI) and (LC).*

Example 5.16 *Let $\mathbb{N}_{max} = (\mathbb{N} \cup \{-\infty\}, max, +)$ be the tropical semiring and $A = \{a, b, c, d\}$, the congruence generated by $\{(a, 1), (a, b), (cd, dc)\}$ is $\mathbb{N}_{max} - \sqcup\!\sqcup$ compatible.*

c) Other examples in characteristic 2

We consider here the field $K = \mathbb{Z}/2\mathbb{Z}$, and the relators

$$R = \{(ab^2, b^2a), (a^2b, ba^2), (abab, baba)\}.$$

It is obvious to see that the congruence generated by the set $\{(ab^2, b^2a), (a^2b, ba^2)\}$ is $\mathbb{Z}/2\mathbb{Z} - \sqcup\!\sqcup$ compatible. Furthermore, we have

$$\begin{array}{rcl} c(abab) & = & abab \otimes 1 + aba \otimes b + a^2b \otimes b + ab^2 \otimes a + bab \otimes a + ba \otimes ab \\ & + & va^2 \otimes b^2 + ab \otimes ba + b^2 \otimes a^2 + b \otimes aba + b \otimes a^2b + a \otimes b^2a \\ & + & a \otimes bab + 1 \otimes abab \\ & \equiv_R^{\otimes 2} & baba \otimes 1 + aba \otimes b + ba^2 \otimes b + b^2a \otimes a + bab \otimes a + ba \otimes ab \\ & + & a^2 \otimes b^2 + ab \otimes ba + b^2 \otimes a^2 + b \otimes aba + b \otimes ba^2 + a \otimes ab^2 \\ & + & a \otimes bab + 1 \otimes baba \\ & = & c(baba) \end{array}$$

which implies the $\mathbb{Z}/2\mathbb{Z} - \sqcup\!\sqcup$ compatibility of $\equiv_R$.
We can remark that this property does not occur if K is not a field or if $2_K \neq 0_K$.
In the same way, the congruence generated by the relators

$$R = \{(a^8b^2, b^2a^8), (a^4b^4, b^4a^4), (a^4b^2a^4b^2, b^2a^4b^2a^4)\}$$

is $\mathbb{Z}/2\mathbb{Z} - \sqcup\!\sqcup$ compatible.

6 Conclusion

Many computations over rational series can be lifted at the level of automata and these (classical) constructions has been proved to be genericaly optimal. The implementation of classical rational laws (shuffle, Hadamard, infiltration) has suggested us other laws (which also preserve rationality) and we have proved that, under some natural hypothesis, there is no other choice than a deformation of the classical case.
The study of the shuffle product over automata raises the question of the compatibility with relators. The answer is of course coefficient dependant and in classical cases (0 characteristic, boolean and proper semirings) it is interesting to observe that only dependance relations can occur. But the p-characteristic induces strange phenomena and opens some new and exciting questions.

References

[1] J. Berstel and C. Reutenauer, *Rational Series and Their Languages* (EATCS Monographs on Theoretical Computer Science, Springer-Verlag, Berlin, 1988).

[2] K. Culik II and J. Kari, Finite state transformations of images, *Proceedings of ICALP 95, Lecture Notes in Comput. Sci.* **944** (1995) 51-62.

[3] G. Duchamp and D. Krob, Partially commutative structures, *J. Algebra* **156** (1993) 318–361.

[4] G. Duchamp and C. Reutenauer, Un critère de rationalité provenant de la géométrie non-commutative, *Invent. Math.* **128** (1997) 613–622.

[5] S. Eilenberg, *Automata, languages and machines, Vol. A* (Acad. Press, New-York, 1974).

[6] M. Fliess, Matrices de Hankel, *J. Math. Pures et Appl.* **53** (1974) 197–224.

[7] M. Fliess, Sur divers produits de séries formelles, *Bull. Sc. Math.* **102** (1974) 181–191.

[8] M. Flouret, Contribution à l'algorithmique non commutative, *Ph.D. thesis, University of Rouen* (1999).

[9] M. Flouret and É. Laugerotte, Noncommutative minimization algorithms, *Inform. Process. Lett.* **64** (1997) 123–126.

[10] J. Hopcroft and D. Ullman, *Introduction to automata theory languages and computation* (Addison Wesley, 1979).

[11] T. Harju and J. Karhumäki, The equivalence problem of multitape finite automata, *Theoret. Comput. Sci.* **78** (1991) 347–355.

[12] S.C. Kleene, Representation of events in nerve nets and finite automata, *Automata Studies, Princeton Univ. Press* (1956) 3–42.

[13] W. Kuich and A. Salomaa, *Semirings, automata, languages* (EATCS Monographs on Theoret. Comput. Sci., Springer-Verlag, 1986).

[14] M. Lothaire, *Combinatorics on words* (Addison-Wesley, 1983).

[15] M. Mohri, F. Pereira and M. Riley, A rational design for a weighted finite-state transducer library, *Proceedings of WIA'97* (1997) 43–53.

[16] A. Salomaa and M. Soittola, *Automata-theoretic aspects of formal power series* (Springer-Verlag, 1978).

[17] M.P. Schützenberger, Communication to G. Duchamp.

[18] M.P. Schützenberger, On the definition of a family of automata, *Inform. and Contr.* **4** (1961) 245–270.

[19] M.P. Schützenberger, On a theorem of R. Jungen, *Proc. Amer. Soc.* **13** (1962) 885–890.