Table des matières

— ◦ —

Chapitre 6

Dérivation d'expressions rationnelles avec multiplicité

« C'est à la fois très simple et très compliqué ... »
Hergé, *Tintin au pays de l'or noir*

Dans le quatrième chapitre, au détour de la preuve du théorème d'Eggan, nous avons donné un algorithme qui permet de transformer une expression rationnelle en automate. Cet algorithme n'est pas des plus efficaces : le nombre d'états de l'automate engendré double chaque fois que l'on rencontre une étoile.

Pour une expression donnée, on peut construire des automates beaucoup plus petits. Si n est le nombre de lettres qui apparaissent dans l'expression, on peut construire un automate avec $n+1$ états qui reconnaît le langage. (Cette borne est optimale, il suffit de considérer une expression qui représente un mot de longueur n). On peut noter que ce n'est pas une borne optimale sur la taille de l'automate, puisque celui-ci peut alors avoir un nombre quadratique de transitions. J. Hromkovič, S. Seibert et T. Wilke [37] ont montré qu'on peut construire un automate avec seulement $n \log^2(n)$ transitions (voir aussi [28]).

Une première méthode pour construire un automate à $n+1$ états consiste à utiliser un algorithme dit « de position » dans lequel chaque état correspond à une occurence de lettre dans l'expression. En comptant un état initial qui ne correspond à aucune lettre, on obtient ainsi un automate qui a exactement $n+1$ états. Cette méthode a été initiée par Glushkov [27]; un algorithme efficace a été donné par Berry et Sethi [6]. Une preuve formelle de cet algorithme ainsi que ses relations avec les langages *locaux* ont été présentés par Berstel et Pin [7].

Une autre méthode est issue d'une approche algébrique. On a vu dans le chapitre introductif que l'ensemble des quotients à gauche d'un ensemble rationnel de A^* est fini : ce sont les états de l'automate minimal. Peut-on définir formellement une opération de *dérivation* sur les expressions rationnelles telle que la dérivation d'une expression E par une lettre soit une expression qui dénote le quotient du langage que représente E par la lettre ? Ceci a été fait par Brzozowski [9]. Il montre, de plus, que l'ensemble des dérivées d'une expression par tous les mots de A^* est fini, sous certaines conditions d'équivalences entre expressions (associativité, commutativité, idempotence). On peut donc construire un automate déterministe fini sur le modèle de l'automate minimal, qui reconnaît le langage. Ce ne sont plus les quotients qui étiquettent les états de l'automate, mais les dérivées de l'expression. Évidemment, on peut obtenir deux expressions différentes qui représentent le même langage, cet automate n'est donc pas nécessairement minimal. D'autre part, comme il s'agit d'un automate déterministe, il n'est pas étonnant que le nombre de ses états soit exponentiel par rapport à la taille de l'expression rationnelle qui, elle, peut être non-déterministe.

Antimirov [3] a repris l'idée de Brzozowski. Si $\mathcal{A}$ est un automate et $\mathcal{D}$ le déterminisé de $\mathcal{A}$, pour tout état X de $\mathcal{D}$, le futur de X est égal à l'union des futurs des éléments de X dans $\mathcal{A}$. Or, les futurs des états de $\mathcal{D}$ sont les quotients du langage. Les quotients du langages appartiennent donc à l'ensemble obtenu par clôture selon l'union, à partir de l'ensemble des futurs états de $\mathcal{A}$. Si on a l'esprit retors, et qu'on identifie l'union avec une somme booléenne, on peut dire que les quotients appartiennent au $\mathbb{B}$-semi-module engendré par les futurs de $\mathcal{A}$. L'algorithme d'Antimirov consiste, non plus à trouver des expressions qui représentent les quotients, mais des expressions qui représentent des générateurs de ce $\mathbb{B}$-semi-module. Il obtient ainsi un automate (non déterministe) qui a au plus $n+1$ états.

Les relations entre l'automate des positions donné par la première méthode et l'automate des dérivées d'Antimirov ont été étudiées par Champarnaud et Ziadi [13].

Les séries rationnelles sur un semi-anneau $\mathbb{K}$ peuvent elles aussi être dénotées par des expressions rationnelles avec des coefficients pris dans $\mathbb{K}$. Il paraît alors naturel d'adapter les algorithmes connus pour obtenir une méthode permettant de construire un automate avec multiplicité à partir d'une expression avec multiplicité. Caron et Flouret [11] ont ainsi donné un algorithme de position qui permet de construire un automate à $n+1$ états pour une expression comptant n lettres.

Généraliser le résultat de Brzozowski semble difficile. En effet, on sait que les quotients d'une série rationnelle peuvent être en nombre infini (considérer par exemple la série $a^*+(2a)^*$ sur $\mathbb{N}$, dont les quotients sont $\{a^* + 2^n(2a)^* \mid n \in \mathbb{N}\}$ qui est un ensemble infini de séries). En revanche, les quotients d'une série $\mathbb{K}$-rationnelle appartiennent à un $\mathbb{K}$-semi-module finiment engendré. Nous allons donc adapter la méthode d'Antimirov, de façon à calculer, à partir d'une expression rationnelle avec multiplicité, des expressions qui représentent des générateurs du $\mathbb{K}$-semi-module auquel appartiennent les quotients de la série. Nous verrons, que, de même que dans le cas booléen (c'est-à-dire dans le cas des langages), ceci permet de donner un automate à multiplicité avec au plus $n+1$ états.

— ∘ —

1 Expressions rationnelles

La définition des **expressions rationnelles sur A à multiplicité dans un semi-anneau** $\mathbb{K}$ se fait par récurrence.

DÉFINITION 6.1 *Soit* $\{0,1,+,\cdot,\star\}$ *un ensemble de symboles et* A *un alphabet.*

i) $\mathsf{0}$, $\mathsf{1}$, *et* a, *pour tout* a *appartenant à* A, *sont des expressions rationnelles (atomiques).*

ii) *Si* E *est une expression rationnelle, et* k *un élément de* $\mathbb{K}$, *alors* $(k\,\mathsf{E})$ *et* $(\mathsf{E}\,k)$ *sont des expressions rationnelles.*

iii) *Si* E *et* F *sont des expressions rationnelles, alors* $(\mathsf{E}{+}\mathsf{F})$, $(\mathsf{E}{\cdot}\mathsf{F})$ *et* $(\mathsf{E}^{\star})$ *aussi.*

Les symboles $\mathsf{0}$ et $\mathsf{1}$ sont donc des constantes, $+$ et $\cdot$ sont des opérateurs binaires; $\star$ est un opérateur unaire.
On note $\mathbb{K}\mathsf{RExp}A$ l'ensemble des expressions rationnelles sur A à multiplicité dans $\mathbb{K}$.

Exemple 24.1 Les semi-anneaux de coefficients qu'on manipule le plus souvent dans le cadre des séries formelles sont commutatifs : entiers, corps commutatifs, semi-anneaux « max ,+ »,*etc.* Toutefois, même si ce n'est pas la façon habituelle de considérer ces objets, les transductions rationnelles sur $A^* \times B^*$ ne sont rien d'autre que des séries rationnelles de $\mathcal{P}(B^*)\mathrm{Rat}\,A^*$. Dans cet exemple, $A = \{a,b\}$ et $B = \{\mathrm{x},\mathrm{y}\}$. On définit l'expression E_4 :

$$\mathsf{E}_4 = (\mathrm{y}((((\mathrm{x}(((a{\cdot}((\mathrm{y}b)^{\star})){\cdot})\mathrm{y}))+(((\mathrm{y}(b{\cdot}((\mathrm{x}a)^{\star}))){\cdot}b)\mathrm{x}))\mathrm{x})^{\star}))$$

On le voit, l'utilisation systématique de parenthèses, si elle permet d'éviter tout risque d'ambiguïté, rend, en revanche, l'expression difficilement lisible. C'est pourquoi on s'autorise à supprimer les parenthèses qui n'ôtent aucune ambiguïté. Pour cela, on fixe comme convention que tout produit ou somme de plusieurs facteurs est parenthésé par défaut à gauche et on utilise implicitement un certain nombre de règles qui seront détaillées plus tard. On obtient :

$$\mathsf{E}_4 = \mathrm{y}\Big(\mathrm{x}\big(a{\cdot}(\mathrm{y}\,b)^{\star}{\cdot}a\big)\,\mathrm{y}{+}\Big(\big(\mathrm{y}\,(b{\cdot}(a\,\mathrm{x})^{\star})\big){\cdot}b\Big)\,\mathrm{x}\Big)^{\star}$$

La complexité d'une expression rationnelle peut être évaluée de différentes façons. La longueur (littérale) de l'expression est le paramètre qui permet d'exprimer la taille de l'automate que nous construirons à la section 4. Toutefois, la plupart des preuves que nous allons effectuer sont par récurrence sur la profondeur des expressions rationnelles.

Définition 6.2 *La* ***longueur d'une expression*** E, *notée* $\ell(\mathsf{E})$ *est le nombre de lettres qui apparaissent dans l'expression :*

$$\begin{aligned}\ell(\mathsf{0}) = \ell(\mathsf{1}) &= 0,\\ \forall a \in A \qquad \ell(a) &= 1,\\ \ell((k\,\mathsf{E})) = \ell((\mathsf{E}\,k)) = \ell((\mathsf{E}^{\star})) &= \ell(\mathsf{E}),\\ \ell((\mathsf{E}\cdot\mathsf{F})) = \ell((\mathsf{E}+\mathsf{F})) &= \ell(\mathsf{E}) + \ell(\mathsf{F}).\end{aligned}$$

La ***profondeur d'une expression*** E, *notée* $\mathsf{d}(\mathsf{E})$ *est définie récursivement par :*

$$\begin{aligned}\mathsf{d}(\mathsf{0}) = \mathsf{d}(\mathsf{1}) &= 0,\\ \forall a \in A \qquad \mathsf{d}(a) &= 0,\\ \mathsf{d}((k\,\mathsf{E})) = \mathsf{d}((\mathsf{E}\,k)) = \mathsf{d}((\mathsf{E}^{\star})) &= 1 + \mathsf{d}(\mathsf{E}),\\ \mathsf{d}((\mathsf{E}\cdot\mathsf{F})) = \mathsf{d}((\mathsf{E}+\mathsf{F})) &= 1 + \mathsf{max}(\mathsf{d}(\mathsf{E}),\mathsf{d}(\mathsf{F})).\end{aligned}$$

Définition 6.3 *Le **terme constant d'une expression rationnelle**[1] est défini par récurrence sur la profondeur de l'expression :*

$$\begin{gathered}
\mathsf{c}(0) = 0_{\mathbb{K}}\,, \quad \mathsf{c}(1) = 1_{\mathbb{K}}, \\
\forall a \in A \qquad \mathsf{c}(a) = 0_{\mathbb{K}}, \\
\mathsf{c}((k\,\mathsf{E})) = k \otimes \mathsf{c}(\mathsf{E})\,, \quad \mathsf{c}((\mathsf{E}\,k)) = \mathsf{c}(\mathsf{E}) \otimes k, \\
\mathsf{c}((\mathsf{E}+\mathsf{F})) = \mathsf{c}(\mathsf{E}) \oplus \mathsf{c}(\mathsf{F})\,, \quad \mathsf{c}((\mathsf{E}\cdot\mathsf{F})) = \mathsf{c}(\mathsf{E}) \otimes \mathsf{c}(\mathsf{F}) \\
\text{et} \quad \mathsf{c}((\mathsf{E}^\star)) = \mathsf{c}(\mathsf{E})^* \quad \text{si le second membre est défini dans } \mathbb{K}.
\end{gathered}$$

Une expression rationnelle E est une formule. Une telle formule peut être une **expression rationnelle valide** et dénoter une série.

Définition 6.4 *Une expression rationnelle est **valide** si son terme constant est défini. La **série dénotée par une expression valide** E, qu'on désigne par $|\mathsf{E}|$, est elle aussi définie par récurrence sur la profondeur de l'expression E :*

$$\begin{gathered}
|0| = 0_{\mathbb{K}}\,, \quad |1| = 1_{A^*}\,, \quad |a| = a\,, \quad \text{pour tout } a \text{ dans } A\,, \\
|(k\,\mathsf{E})| = k \otimes |\mathsf{E}|\,, \quad |(\mathsf{E}\,k)| = |\mathsf{E}| \otimes k\,, \\
|(\mathsf{E}+\mathsf{F})| = |\mathsf{E}| \oplus |\mathsf{F}|\,, \quad |(\mathsf{E}\cdot\mathsf{F})| = |\mathsf{E}| \otimes |\mathsf{F}|\,, \\
\text{et} \quad |(\mathsf{E}^\star)| = |\mathsf{E}|^*.
\end{gathered}$$

*Deux expressions valides sont des **expressions équivalentes** si elles dénotent la même série.*

Remarquons que la définition du terme constant est bien cohérente. En effet, $\mathsf{c}(\mathsf{E})$ et $|\mathsf{E}|$ sont définis par la même induction et on a :

$$\begin{aligned}
\mathsf{c}(|0|) &= \mathsf{c}(0_{\mathbb{K}}) = 0_{\mathbb{K}} = \mathsf{c}(0), \\
\mathsf{c}(|1|) &= \mathsf{c}(1_{A^*}) = 1_{\mathbb{K}} = \mathsf{c}(1), \\
\forall a \in A^* \qquad \mathsf{c}(|a|) &= \mathsf{c}(a) = 0_{\mathbb{K}} = \mathsf{c}(a).
\end{aligned}$$

On obtient immédiatement que $\mathsf{c}(\mathsf{E})$ est égal à $\mathsf{c}(|\mathsf{E}|)$.

L'équation qui permet d'interpréter l'étoile est rendue consistante par la proposition 1.1 : $|(\mathsf{E}^\star)|$ est défini si et seulement si $\mathsf{c}(\mathsf{E})^*$ est défini, donc si et seulement si $(\mathsf{E}^\star)$ est valide.

Remarque 6.1 Il faut noter que la proposition 1.1 permet de définir l'étoile d'une série avec terme constant dénotée par une expression E. Toutefois, cette proposition ne donne aucune information sur la forme de l'expression dénotant la série propre. La proposition peut donc être appliquée aux séries mais ne devra pas être utilisée pour effectuer des récurrences sur les expressions.

1. Cette définition est distincte de celle de « terme constant d'une série » donnée en 1.28 page 29.

Exemple 25.1 On définit l'expression E_1 de $\mathbb{Q}\mathsf{RExp}\{a,b\}$:

$$\mathsf{E}_1 = (((\tfrac{1}{6}\, a^\star) + (\tfrac{1}{3}\, b^\star))^\star).$$

Soit l'expression $\mathsf{F}_1 = ((\frac{1}{6}\, a^\star) + (\frac{1}{3}\, b^\star))$. On a $\mathsf{c}(\mathsf{F}_1) = \frac{1}{2}$, et donc $\mathsf{c}(\mathsf{F}_1)^* = 2$, et bien que $|\mathsf{F}_1|$ ne soit pas propre, la série dénotée par E_1 est bien définie.

Exemple 26.1 On définit l'expression E_2 de $\mathbb{Z}\mathsf{RExp}\{a,b\}$:

$$\mathsf{E}_2 = (a\,b\,a + (a\,(a - b\,a))).$$

Afin d'alléger l'écriture des expressions, on se permet certaines licences et on note $a\,b$ pour $(a \cdot b)$, $a\,b\,a$ pour $((a \cdot b) \cdot a)$ ou encore $(a - b\,a)$ pour $(a + (-1_{\mathbb{K}}\,(b \cdot a)))$.

Exemple 27.1 On définit l'expression E_3 de $\mathbb{N}\mathsf{RExp}\{a,b\}$:

$$\mathsf{E}_3 = 5\,((2\,a\,b) + ((3\,b) \cdot (4\,(a\,b)^\star)))^\star$$

Cet exemple apparaît dans l'article [11]. Les étoiles s'appliquent dans cette expression à des sous-expressions propres. Avec la topologie usuelle, c'est la seule configuration pour laquelle l'étoile d'une série à coefficients entiers peut être définie.

— ∘ —

Identités triviales. Bien qu'on désire travailler formellement sur les expressions rationnelles, et que, pour cette raison, on refuse de recourir à des axiomes tels que l'associativité ou la commutativité, nous aurons besoin de définir une forme « normale » pour les expressions. C'est pourquoi nous définissons les règles de réécriture suivantes qui peuvent être appliquées localement aux expressions rationnelles.

$$(\mathsf{1}\,k) \equiv (k\,\mathsf{1})\,, \quad (a\,k) = (k\,a), \tag{1}$$

$$(k\,\mathsf{0}) \equiv (\mathsf{0}\,k) \equiv \mathsf{0}\,, \quad (0_{\mathbb{K}}\,\mathsf{E}) \equiv (\mathsf{E}\,0_{\mathbb{K}}) \equiv \mathsf{0}\,, \quad (\mathsf{0} \cdot \mathsf{E}) \equiv (\mathsf{E} \cdot \mathsf{0}) \equiv \mathsf{0}\,, \tag{2}$$

$$\mathsf{0} + \mathsf{E} \equiv \mathsf{E} + \mathsf{0} \equiv \mathsf{E}\,, \quad (1_{\mathbb{K}}\,\mathsf{E}) \equiv (\mathsf{E}\,1_{\mathbb{K}}) \equiv \mathsf{E}\,, \tag{3}$$

$$((k\,\mathsf{1}) \cdot \mathsf{E}) \equiv (k\,\mathsf{E})\,, \quad (\mathsf{E} \cdot (k\,\mathsf{1})) \equiv (\mathsf{E}\,k), \tag{4}$$

$$(k\,(k'\,\mathsf{E})) \equiv ([k \otimes k']\,\mathsf{E})\,, \quad ((\mathsf{E}\,k)\,k') \equiv (\mathsf{E}\,[k \otimes k'])\,, \quad ((k\,\mathsf{E})\,k') \equiv (k\,(\mathsf{E}\,k')). \tag{5}$$

L'identité (1) représente la commutativité des coefficients avec les expressions atomiques, les identités (2) reflètent le caractère absorbant du zéro; les identités (3) et (4) traduisent le fait que $0_{\mathbb{K}}$ et $1_{\mathbb{K}}$ sont des éléments neutres; l'identité (5) indique l'associativité du produit externe.

On vérifie immédiatement que l'interprétation de chaque membre de n'importe laquelle de ces identités est la même.

Noter que la commutativité des variables et des coefficients n'entraîne pas la commutativité des coefficients avec les expressions. Si $(\mathsf{E}\,k)$ est une expression, il est possible qu'un coefficient k' soit niché dans E et ne commute pas avec k. Dans ce cas $(k\,\mathsf{E})$ et $(\mathsf{E}\,k)$ risquent fort de ne pas commuter.

Les identités définies ci-dessus sont des propriétés locales et si chaque identité est considérée comme une règle de réécriture (dont le résultat est le membre droit), chaque expression rationnelle peut se réécrire en une **expression réduite** unique qui peut être calculée en temps proportionnel à la longueur de l'expression. Dans ce qui suit, on suppose qu'on applique systématiquement cette réduction.

Remarque 6.2 Les identités triviales ne reflètent en rien l'associativité ou la commutativité de l'addition et de la multiplication des séries. Ainsi, $(a + (b + c))$, $((a + b) + c)$ et $(a + (c + b))$ sont trois expressions réduites différentes qui dénotent la même série.

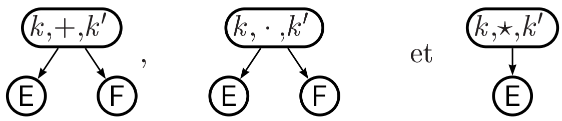
— ∘ —

2 Motivation de la dérivation

L'égalité (5) permet de voir les expressions rationnelles comme des arbres.

i) $\mathsf{0}$, k,1 et k,a sont des expressions.

ii) Si E et F sont des expressions, alors, pour tous k, k' dans $\mathbb{K}$,



sont des expressions.

On voit que dans cette définition, chaque opérateurs est doté systématiquement de coefficients. L'identité (3) permet, en l'absence de tels coefficients, de supposer qu'il s'agit de $1_{\mathbb{K}}$.

Exemple 24.2 L'arbre correspondant à l'expression E_4 est donné figure 1.

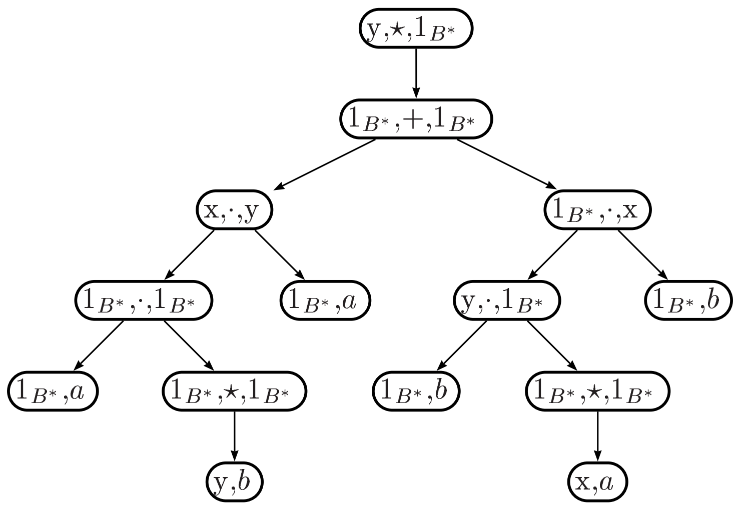


Fig. 1 – *L'arbre de l'expression* E_4.

Chaque nœud peut ensuite être « interprété ». La lecture d'un mot dans l'expression se fait de la façon suivante :

- Si le nœud est étiqueté par $+$, on explore *soit* le fils gauche, *soit* le fils droit, puis on remonte;
- si le nœud est étiqueté par $\cdot$, on explore le fils gauche, puis le fils droit, puis on remonte;
- si le nœud est étiqueté par $\star$, on explore le fils un nombre arbitraire de fois (éventuellement nul), puis on remonte;
- si le nœud est une feuille, on lit la constante qu'il contient puis on remonte;
- lorsqu'on descend, on prend en compte la multiplicité « d'entrée » du nœud.
- lorsqu'on remonte, on prend en compte la multiplicité « de sortie » du nœud.

La lecture se termine lorsqu'on essaie de remonter à partir de la racine.

Le comportement de chaque nœud peut être localement vu comme un automate :

$(k,+,k')$	$(k,\cdot,k')$	$(k,\star,k')$	(k,a)	$(k,1_{A^*})$	$\mathsf{0}$

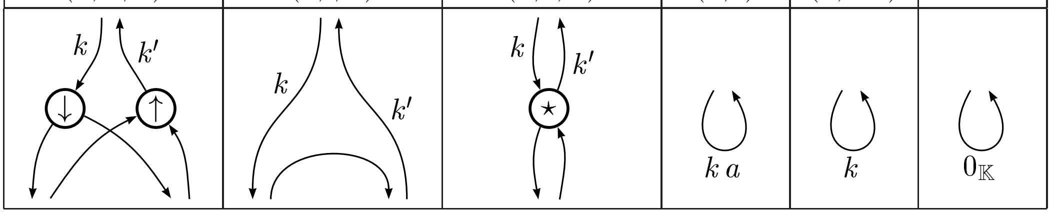


Fig. 2- L'interprétation des différents opérateurs rationnels.

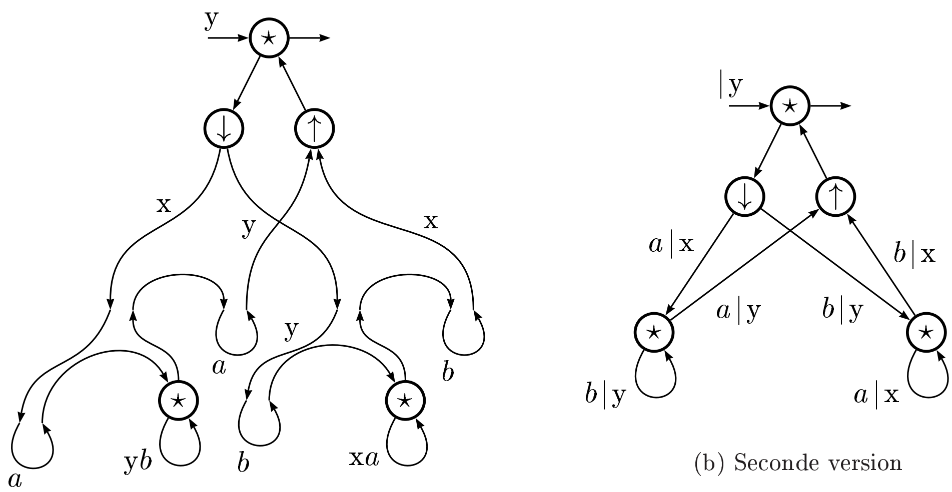
Le remplacement de chaque nœud de l'arbre de l'expression par la configuration indiquée ci-dessus donne un automate qui réalise la série dénotée par l'expression. Cet automate est généralisé; en effet, chaque transition est étiquetée par un mot, éventuellement vide.

La dérivation consiste à parcourir l'automate de l'expression. Le terme constant de l'expression est le poids total des chemins qui permettent de faire une boucle autour de la racine sans lire de lettre. La dérivée par rapport à une lettre est l'expression qui décrit l'endroit où l'on se trouve après avoir lu la lettre et le nombre de façons (comptées dans $\mathbb{K}$) de le faire. L'automate n'étant pas nécessairement déterministe, le résultat de la dérivation peut donner plusieurs expressions.

Ce procédé peut être systématisé et les dérivées calculées sur les expressions. C'est le propos du paragraphe suivant.

Exemple 24.3 En appliquant mécaniquement le remplacement des nœuds de l'arbre représentant l'expression E_4, on obtient l'automate présenté figure 3 a) qui se réécrit immédiatement en l'automate de la figure 3 b). Comme il s'agit d'un transducteur, on utilise la notations $a|\mathrm{x}$, plutôt que $\mathrm{x}\,a$.

— ∘ —



(a) Première version

(b) Seconde version

FIG. 3 – *L'automate issu de l'arbre de* E_4.

3 Dérivation et termes dérivés

On présente tout d'abord les « polynômes » d'expressions rationnelles. L'ensemble $\mathbb{K}\langle\mathbb{K}\mathsf{RExp}A\rangle$ des combinaisons linéaires d'expressions rationnelles, ou **polynômes d'expressions**, est un $\mathbb{K}$-semi-module (à gauche); l'addition y est commutative et la multiplication par un élément de $\mathbb{K}$ distributive :

$$k\,\mathsf{E} \oplus k'\,\mathsf{F} = k'\,\mathsf{F} \oplus k\,\mathsf{E} \qquad\qquad k\,\mathsf{E} \oplus k'\,\mathsf{E} = [k \oplus k']\mathsf{E}$$

Nous définissons de plus une loi de multiplication sur les monômes qui s'étend sur les polynômes par linéarité :

$$[k\,\mathsf{E}][k'\,\mathsf{F}] \equiv k\,(\mathsf{E}\cdot(k'\,\mathsf{F})), \tag{6}$$

$$\big([\mathsf{E}\oplus\mathsf{E}']\cdot\mathsf{F}\big) \equiv (\mathsf{E}\cdot\mathsf{F})\oplus(\mathsf{E}'\cdot\mathsf{F})\,, \quad \big(\mathsf{E}\cdot[\mathsf{F}\oplus\mathsf{F}']\big) \equiv (\mathsf{E}\cdot\mathsf{F}')\oplus(\mathsf{E}\cdot\mathsf{F}'). \tag{7}$$

$$\big([\mathsf{E}\oplus\mathsf{E}']\;k\big) \equiv (\mathsf{E}\,k)\oplus(\mathsf{E}'\cdot k)\,, \quad \big(k\;[\mathsf{E}\oplus\mathsf{E}']\big) \equiv (k\,\mathsf{E}')\oplus(k\,\mathsf{E}'). \tag{8}$$

Afin de différencier le plus possible les expressions des polynômes, nous essaierons de nous abstenir d'utiliser les parenthèses pour ces derniers. Ainsi, dans tout ce qui suit, $[k\,\mathsf{E}]$ ou $k\,\mathsf{E}$ désigne un monôme, alors que $(k\,\mathsf{E})$ représente une expression.

La série dénoté par un polynôme d'expressions rationnelles est obtenue par linéarité à partir de l'interprétation définie sur les expressions rationnelles (qui forment une base de $\mathbb{K}\langle\mathbb{K}\mathsf{RExp}A\rangle$).

REMARQUE 6.3 On pourrait être tenté de définir la multiplication des monômes par $[k\,\mathsf{E}][k'\,\mathsf{F}] \equiv [k\otimes k']\,(\mathsf{E}\cdot\mathsf{F})$; si $\mathbb{K}$ n'est pas commutatif, l'interprétation des membres gauche et droit peut alors être différente. C'est la raison pour laquelle on pose l'identité (6).

L'ensemble des polynômes d'expressions rationnelles n'est pas une semi-algèbre. En effet, la multiplication que nous avons définie n'est pas associative :

$$[[\mathsf{E}]\,[\mathsf{F}]]\;[\mathsf{G}] = ((\mathsf{E}\cdot\mathsf{F})\cdot\mathsf{G}) \neq (\mathsf{E}\cdot(\mathsf{F}\cdot\mathsf{G})) = [\mathsf{E}]\;[[\mathsf{F}]\,[\mathsf{G}]]$$

Ceci ne cause heureusement aucun problème pour traiter les dérivations.

— ∘ —

Derivation

DÉFINITION 6.5 *Soit* E *une expression de* $\mathbb{K}\mathsf{RExp}A$ *et* a *une lettre de* A*. La* ***dérivée de l'expression*** E ***par rapport à*** a*, notée* $\frac{\partial}{\partial a}\mathsf{E}$*, est un polynôme d'expressions rationnelles à coefficient dans* $\mathbb{K}$*, défini par récurence selon les formules suivantes :*

$$\frac{\partial}{\partial a}\mathsf{0} = \frac{\partial}{\partial a}\mathsf{1} = \mathsf{0}$$

$$\forall b \in A \qquad \frac{\partial}{\partial a} b = \begin{cases} \mathsf{1} & si\ b = a \\ \mathsf{0} & sinon \end{cases} \tag{9}$$

$$\frac{\partial}{\partial a}(k\,\mathsf{E}) = k\,\frac{\partial}{\partial a}\mathsf{E} \tag{10}$$

$$\frac{\partial}{\partial a}(\mathsf{E}\,k) = (\left[\frac{\partial}{\partial a}\mathsf{E}\right]\,k) \tag{11}$$

$$\frac{\partial}{\partial a}(\mathsf{E}{+}\mathsf{F}) = \frac{\partial}{\partial a}\mathsf{E} \oplus \frac{\partial}{\partial a}\mathsf{F} \tag{12}$$

$$\frac{\partial}{\partial a}(\mathsf{E}\cdot\mathsf{F}) = \left(\left[\frac{\partial}{\partial a}\mathsf{E}\right]\cdot\mathsf{F}\right) \oplus \mathsf{c}(\mathsf{E})\,\frac{\partial}{\partial a}\mathsf{F} \tag{13}$$

$$\frac{\partial}{\partial a}(\mathsf{E}^\star) = \mathsf{c}(\mathsf{E})^*\,\left(\left[\frac{\partial}{\partial a}\mathsf{E}\right]\cdot(\mathsf{E}^\star)\right) \tag{14}$$

La dérivation d'un polynôme d'expressions est évidemment définie en étendant linéairement la dérivation :

$$\frac{\partial}{\partial a}\left[\bigoplus_{i\in I} k_i\,\mathsf{E}_i\right] = \bigoplus_{i\in I} k_i\,\frac{\partial}{\partial a}\mathsf{E}_i \tag{15}$$

Les équations (10) à (14) sont sensiblement différentes de celles posées par Brzozowski [9]. En effet, l'opérateur (symbolique) « + » est remplacé, dans les équations (12) et (13), par l'opération « $\oplus$ ». Ceci est la généralisation de l'idée d'Antimirov; les langages rationnels sont en effet des séries rationnelles à multiplicité dans le semi-anneau de Boole et l'addition est alors l'union.

Les équations (10), (14) et (15) introduisent la prise en compte des multiplicités.

On peut relever que l'équation (14) n'est définie que si l'expression E est valide.

Le résultat de la dérivation d'une expression est donc un polynôme d'expressions à coefficients dans $\mathbb{K}$.

Contrairement au cas booléen, les polynômes obtenus en itérant la dérivation peuvent ne pas être en nombre fini. Le théorème 6.1 établira cependant que tous ces polynômes sont engendrés par un nombre fini d'expressions.

Définition 6.6 *La **dérivée d'une expression par rapport à un mot** u est définie par récurrence sur la longueur de u. Par convention, la dérivation par rapport au mot vide est l'identité.*

$$\forall u \in A^* \,, \quad \forall a \in A \qquad \frac{\partial}{\partial ua}\mathsf{E} = \frac{\partial}{\partial a}\left(\frac{\partial}{\partial u}\mathsf{E}\right) \tag{16}$$

— ∘ —

A présent que la dérivation est définie, il faut établir le sens qu'a cette opération syntaxique. Le lien entre les dérivées d'une expression et les quotients d'une série est exposé dans la proposition suivante :

Proposition 6.1 *L'interprétation de la dérivée d'une expression rationnelle par rapport à un mot est le quotient par rapport à ce mot de l'interprétation de l'expression :*

$$\forall u \in A^* \qquad |\frac{\partial}{\partial u}(\mathsf{E})| = u^{-1}|\mathsf{E}|$$

Ce résultat peut être montré directement, mais il apparaîtra comme un corollaire naturel de propriétés plus fines établies sur les dérivées.

Remarque 6.4 Il faut souligner dès à présent la différence de statut entre dérivée et quotient. Le quotient d'une série par un mot est un objet mathématique, la dérivée d'une expression est une représentation de cet objet. Ainsi, on peut obtenir plusieurs dérivées qui représentent le même quotient. Le fait que les quotients d'une série rationnelle appartiennent à un $\mathbb{K}$-semi-module finiment engendré n'implique pas qu'il en est de même pour les dérivées d'une expression qui la représente. Nous verrons d'ailleurs qu'il est possible qu'il existe des systèmes générateurs d'un $\mathbb{K}$-semi-module de quotients d'une série de cardinal strictement inférieur aux plus petits systèmes générateurs du $\mathbb{K}$-semi-module des dérivées d'une expression correspondant à la série.

La dérivée d'une expression par rapport à un mot est donnée explicitement par les formules suivantes :

Proposition 6.2 *Pour tout u dans A^+, pour tout couple (E,F) d'expressions,*

i)

$$\frac{\partial}{\partial u}(k\,\mathsf{E}) = k\,\frac{\partial}{\partial u}\mathsf{E}\,, \qquad \frac{\partial}{\partial u}(\mathsf{E}\,k) = (\left[\frac{\partial}{\partial u}\mathsf{E}\right]\,k),$$

ii)

$$\frac{\partial}{\partial u}(\mathsf{E}+\mathsf{F}) = \frac{\partial}{\partial u}\mathsf{E} \oplus \frac{\partial}{\partial u}\mathsf{F},$$

iii)

$$\frac{\partial}{\partial u}(\mathsf{E}\cdot\mathsf{F}) = \left[\frac{\partial}{\partial u}\mathsf{E}\right]\cdot\mathsf{F} \oplus \left[\bigoplus_{\substack{u=v\,w\\ v\in A^*,\, w\in A^+}} \mathsf{c}(\frac{\partial}{\partial v}\mathsf{E})\ \frac{\partial}{\partial w}\mathsf{F}\right],$$

iv)

$$\frac{\partial}{\partial u}(\mathsf{E}^\star) = \bigoplus_{\substack{u=v_1v_2\cdots v_n\\ v_1,v_2,\dots,v_n\in A^+}} \mathsf{c}(\mathsf{E})^*\,\mathsf{c}(\frac{\partial}{\partial v_1}\mathsf{E})\ \mathsf{c}(\mathsf{E})^*\cdots\mathsf{c}(\mathsf{E})^*\,\mathsf{c}(\frac{\partial}{\partial v_{n\text{-}1}}\mathsf{E})\ \mathsf{c}(\mathsf{E})^*\left([\frac{\partial}{\partial v_n}\mathsf{E}]\cdot(\mathsf{E}^\star)\right).$$

Démonstration. La preuve est par récurrence sur la longueur de u. Si u est de longueur 1, on vérifie que les formules données rejoignent celles de la définition 6.5. On suppose que u vérifie la proposition. Soit E et F deux expressions rationnelles et a une lettre de A. Posons

$$\frac{\partial}{\partial a}\mathsf{E} = \bigoplus k_i\,\mathsf{E}_i \text{ et } \frac{\partial}{\partial a}\mathsf{F} = \bigoplus k_j\,\mathsf{F}_j.$$

On obtient les égalités suivantes :

i)

$$\frac{\partial}{\partial au}(k\,\mathsf{E}) = \frac{\partial}{\partial u}\frac{\partial}{\partial a}(k\,\mathsf{E}) = \frac{\partial}{\partial u}\left[k\ \frac{\partial}{\partial a}\mathsf{E}\right] = k\ \frac{\partial}{\partial u}\left[\frac{\partial}{\partial a}\mathsf{E}\right] = k\ \frac{\partial}{\partial au}\mathsf{E}.$$

$$\begin{aligned}\frac{\partial}{\partial au}(\mathsf{E}\,k) = \frac{\partial}{\partial u}\frac{\partial}{\partial a}(\mathsf{E}\,k) = \frac{\partial}{\partial u}[\bigoplus k_i\,(\mathsf{E}_i\,k)] = \bigoplus k_i\ \frac{\partial}{\partial u}(\mathsf{E}_i\,k) &= \bigoplus k_i([\frac{\partial}{\partial u}\mathsf{E}_i]\,k)\\ &= \left([\bigoplus k_i\,\frac{\partial}{\partial u}\mathsf{E}_i]\,k\right) = \left(\frac{\partial}{\partial u}[\bigoplus k_i\mathsf{E}_i]\,k\right)\\ &= \left(\left[\frac{\partial}{\partial u}[\frac{\partial}{\partial a}\mathsf{E}]\right]\ k\right) = \left([\frac{\partial}{\partial au}\mathsf{E}]\,k\right).\end{aligned}$$

ii)

$$\frac{\partial}{\partial au}(\mathsf{E}{+}\mathsf{F}) = \frac{\partial}{\partial u}[\frac{\partial}{\partial a}\mathsf{E}\oplus\frac{\partial}{\partial a}\mathsf{F}] = \frac{\partial}{\partial u}[\frac{\partial}{\partial a}\mathsf{E}]\oplus\frac{\partial}{\partial u}[\frac{\partial}{\partial a}\mathsf{F}] = \frac{\partial}{\partial au}\mathsf{E}\oplus\frac{\partial}{\partial au}\mathsf{F}.$$

iii)

$$
\begin{aligned}
\frac{\partial}{\partial au}(\mathsf{E}{\cdot}\mathsf{F}) &= \frac{\partial}{\partial u}\left[\frac{\partial}{\partial a}(\mathsf{E}{\cdot}\mathsf{F})\right] = \frac{\partial}{\partial u}\left[\left([\frac{\partial}{\partial a}\,\mathsf{E}]\cdot\mathsf{F}\right)\oplus \mathsf{c}(\mathsf{E})\ \frac{\partial}{\partial a}\,\mathsf{F}\right] \\
&= \left(\frac{\partial}{\partial u}[\frac{\partial}{\partial a}\,\mathsf{E}]{\cdot}\mathsf{F}\right)\oplus\left[\bigoplus_{\substack{u=v\,w\\ v\in A^*,\,w\in A^+}} \mathsf{c}(\frac{\partial}{\partial v}[\frac{\partial}{\partial a}\,\mathsf{E}])\ \frac{\partial}{\partial w}\,\mathsf{F}\right]\oplus \mathsf{c}(\mathsf{E})\ \frac{\partial}{\partial au}\,\mathsf{F} \\
&= \left([\frac{\partial}{\partial au}\,\mathsf{E}]{\cdot}\mathsf{F}\right)\oplus\left[\bigoplus_{\substack{au=v\,w\\ v\in A^*,\,w\in A^+}} \mathsf{c}(\frac{\partial}{\partial v}\,\mathsf{E})\ \frac{\partial}{\partial w}\,\mathsf{F}\right]
\end{aligned}
$$

iv)

$$
\begin{aligned}
\frac{\partial}{\partial au}(\mathsf{E}^\star) &= \mathsf{c}(\mathsf{E})^*\ \frac{\partial}{\partial u}\left([\frac{\partial}{\partial a}\,\mathsf{E}]{\cdot}(\mathsf{E}^\star)\right) \\
&= \mathsf{c}(\mathsf{E})^*\ \left[\left([\frac{\partial}{\partial au}\,\mathsf{E}]{\cdot}(\mathsf{E}^\star)\right)\oplus \bigoplus_{\substack{au=v\,w\\ v\in A^*,\,w\in A^+}} [\mathsf{c}(\frac{\partial}{\partial av}\,\mathsf{E})\ \frac{\partial}{\partial w}(\mathsf{E}^\star)]\right] \\
&= \mathsf{c}(\mathsf{E})^*\ \left([\frac{\partial}{\partial au}\,\mathsf{E}]{\cdot}(\mathsf{E}^\star)\right)\oplus \\
&\quad \bigoplus_{\substack{au=v_0\,w\\ v_0\in A^*,\,w\in A^+}}\ \bigoplus_{\substack{w=v_1\ldots v_n\\ v_n\in A^+}} \mathsf{c}(\mathsf{E})^*\,\mathsf{c}(\frac{\partial}{\partial av_0}\,\mathsf{E})\ \mathsf{c}(\mathsf{E})^*\,\mathsf{c}(\frac{\partial}{\partial v_1}\,\mathsf{E})\ldots \mathsf{c}(\mathsf{E})^*\ \left([\frac{\partial}{\partial v_n}\,\mathsf{E}]{\cdot}(\mathsf{E}^\star)\right) \\
&= \bigoplus_{\substack{au=v_1\ldots v_n\\ v_n\in A^+}} \mathsf{c}(\mathsf{E})^*\ \mathsf{c}(\frac{\partial}{\partial v_1}\,\mathsf{E})\ldots \mathsf{c}(\frac{\partial}{\partial v_{n\text{-}1}}\,\mathsf{E})\ \mathsf{c}(\mathsf{E})^*\ \left([\frac{\partial}{\partial v_n}\,\mathsf{E}]{\cdot}(\mathsf{E}^\star)\right)
\end{aligned}
$$

$\square$

Exemple 25.2

$$\frac{\partial}{\partial a}\,\mathsf{E}_1 = \frac{\partial}{\partial a}(\mathsf{F}_1{}^\star) = 2\;\frac{\partial}{\partial a}\left(\tfrac{1}{6}\,a^\star\right)\cdot\mathsf{F}_1{}^\star \oplus 2\;\frac{\partial}{\partial a}\left(\tfrac{1}{3}\,b^\star\right)\cdot\mathsf{F}_1{}^\star = \tfrac{1}{3}\;(a^\star\cdot\mathsf{F}_1{}^\star)$$

$$\frac{\partial}{\partial b}\,\mathsf{E}_1 = 2\;\frac{\partial}{\partial b}\left(\tfrac{1}{3}\,b^\star\right)\cdot\mathsf{F}_1{}^\star = \tfrac{2}{3}\;(b^\star\cdot\mathsf{F}_1{}^\star)$$

$$\begin{aligned}\frac{\partial}{\partial aa}\,\mathsf{E}_1 &= \tfrac{1}{3}\;\frac{\partial}{\partial a}(a^\star\cdot\mathsf{F}_1{}^\star) = \tfrac{1}{3}\left(\frac{\partial}{\partial a}\,a^\star\right)\cdot\mathsf{F}_1{}^\star \oplus \tfrac{1}{3}\;\mathsf{c}(a)^*\;\frac{\partial}{\partial a}(\mathsf{F}_1{}^\star)\\ &= \tfrac{1}{3}\;(a^\star\cdot\mathsf{F}_1{}^\star)\oplus\tfrac{1}{9}\;(a^\star\cdot\mathsf{F}_1{}^\star) = \tfrac{4}{9}\;(a^\star\cdot\mathsf{F}_1{}^\star)\end{aligned}$$

$$\frac{\partial}{\partial ab}\,\mathsf{E}_1 = \tfrac{1}{3}\;\frac{\partial}{\partial b}(a^\star\cdot\mathsf{F}_1{}^\star) = \tfrac{1}{3}\left(\frac{\partial}{\partial b}\,a^\star\right)\cdot\mathsf{F}_1{}^\star \oplus \tfrac{1}{3}\;\mathsf{c}(a)^*\;\frac{\partial}{\partial b}(\mathsf{F}_1{}^\star) = \tfrac{2}{9}\;(b^\star\cdot\mathsf{F}_1{}^\star)$$

$$\frac{\partial}{\partial ba}\,\mathsf{E}_1 = \tfrac{2}{3}\;\frac{\partial}{\partial a}(b^\star\cdot\mathsf{F}_1{}^\star) = \tfrac{2}{3}\left(\frac{\partial}{\partial a}\,b^\star\right)\cdot\mathsf{F}_1{}^\star \oplus \tfrac{2}{3}\;\mathsf{c}(b)^*\;\frac{\partial}{\partial a}(\mathsf{F}_1{}^\star) = \tfrac{2}{9}\;(a^\star\cdot\mathsf{F}_1{}^\star)$$

$$\begin{aligned}\frac{\partial}{\partial bb}\,\mathsf{E}_1 &= \tfrac{2}{3}\;\frac{\partial}{\partial b}(b^\star\cdot\mathsf{F}_1{}^\star) = \tfrac{2}{3}\left(\frac{\partial}{\partial b}\,b^\star\right)\cdot\mathsf{F}_1{}^\star \oplus \tfrac{2}{3}\;\mathsf{c}(b)^*\;\frac{\partial}{\partial b}(\mathsf{F}_1{}^\star)\\ &= \tfrac{2}{3}\;(b^\star\cdot\mathsf{F}_1{}^\star)\oplus\tfrac{4}{9}\;(b^\star\cdot\mathsf{F}_1{}^\star) = \tfrac{10}{9}\;(b^\star\cdot\mathsf{F}_1{}^\star)\end{aligned}$$

Exemple 26.2

$$\frac{\partial}{\partial a}\,\mathsf{E}_2 = b\,a\oplus(a-b\,a) \qquad\qquad \frac{\partial}{\partial b}\,\mathsf{E}_2 = 0$$

$$\frac{\partial}{\partial aa}\,\mathsf{E}_2 = \frac{\partial}{\partial a}\,b\,a\oplus\frac{\partial}{\partial a}(a-b\,a) = 1$$

$$\frac{\partial}{\partial ab}\,\mathsf{E}_2 = \frac{\partial}{\partial b}\,b\,a\oplus\frac{\partial}{\partial b}(a-b\,a) = a\oplus(-1_{\mathbb{K}})\,a = 0$$

— ∘ —

Termes dérivés. Nous énonçons maintenant le théorème principal qui est une généralisation du résultat d'Antimirov.

Théorème 6.1 *Soit* E *une expression de* $\mathbb{K}\mathsf{RExp}A$*. Il existe un entier* m *inférieur à* $\ell(\mathsf{E})$*, et* m *expressions rationnelles* $\mathsf{K}_1, \mathsf{K}_2, \ldots, \mathsf{K}_m$ *telles que, pour tout mot* u *dans* A^+*, il existe* m *coefficients* $k_1^{(u)}, k_2^{(u)}, \ldots, k_m^{(u)}$ *de* $\mathbb{K}$ *tels que*

$$\frac{\partial}{\partial u}\,\mathsf{E} = \bigoplus_{i=1}^{i=m} k_i^{(u)}\,\mathsf{K}_i.$$

En fait, le théorème 6.1 est un corollaire de la proposition suivante. Celle-ci permet, en outre, de décrire un procédé plus proche de l'algorithme effectif présenté par la suite.

Proposition 6.3 *Soit* E *une expression de* $\mathbb{K}\mathsf{RExp}A$*. Il existe un entier* n *inférieur à* $\ell(\mathsf{E})$*, et* n *expressions rationnelles* $\mathsf{K}_1, \mathsf{K}_2, \ldots, \mathsf{K}_n$ *telles que, pour toute lettre* a *de* A*, il existe* n *coefficients* $k_1^{(a)}, k_2^{(a)}, \ldots, k_n^{(a)}$*, et* n^2 *coefficients* $\{z_{i,j}^{(a)}\}_{i,j\in[n]}$ *in* $\mathbb{K}$ *tels que*

i) $\dfrac{\partial}{\partial a} \mathsf{E} = \bigoplus_{i \in [n]} k_i^{(a)} \mathsf{K}_i$;

ii) $\forall i \in [n] \qquad \dfrac{\partial}{\partial a} \mathsf{K}_i = \bigoplus_{j \in [n]} z_{i,j}^{(a)} \mathsf{K}_j$

Les expressions K_i, dont l'existence est assurée par la proposition, sont appelés les **termes dérivés de** E.

Si $\mathbb{K}$ est le semi-anneau de Boole, ce sont exactement ce qu'Antimirov [3] appelle les « dérivées partielles » de E, avec la justification que ce sont des « parts » des dérivées de E. Comme le terme *dérivée partielle* évoque en mathématiques le fait de dériver selon seulement un paramètre (ici, une lettre), et que les dérivées telles que les définit Brzozowski sont, à cet égard, déjà partielles, nous préférons nous abstenir d'employer ce terme.

Exemple 25.3 Les termes dérivés de E_1 sont $(a^* \cdot \mathsf{F_1}^*)$ et $(b^* \cdot \mathsf{F_1}^*)$.

Il nous faut maintenant prouver la proposition.

Démonstration. La preuve est par récurrence sur la profondeur de l'expression E. L'énoncé est trivialement vrai pour les expressions atomiques $\mathsf{0}$, $\mathsf{1}$ et a (pour a dans A).

On prouve successivement que si le résultat est vrai pour deux expressions rationnelles E et F, il l'est pour :

a) $(k\,\mathsf{E})$ (pour k dans $\mathbb{K}$). En effet, d'après l'équation (10), les termes dérivés de $(k\,\mathsf{E})$ sont les mêmes que ceux de E.

b) $(\mathsf{E}\,k)$. Le nombre de termes dérivés est le même que celui de E, puisque d'après l'équation (11), il s'agit des $(\mathsf{K}_i\,k)$, où les K_i sont les termes dérivés de E.

c) $(\mathsf{E}+\mathsf{F})$. En effet, avec des notations évidentes,

$$\frac{\partial}{\partial a}(\mathsf{E}+\mathsf{F}) = \frac{\partial}{\partial a}\mathsf{E} \oplus \frac{\partial}{\partial a}\mathsf{F} = \bigoplus_{i \in [1;n]} k_i^{(a)} \mathsf{K}_i \oplus \bigoplus_{j \in [1;m]} l_j^{(a)} \mathsf{L}_j .$$

L'ensemble des termes dérivés de $(\mathsf{E}+\mathsf{F})$ est donc l'union de ceux de E et de ceux de F, ce qui répond à la proposition.

d) $(\mathsf{E} \cdot \mathsf{F})$. De la même façon,

$$\frac{\partial}{\partial a}(\mathsf{E} \cdot \mathsf{F}) = \left(\left[\frac{\partial}{\partial a}\mathsf{E}\right] \cdot \mathsf{F}\right) \oplus \mathsf{c}(\mathsf{E})\,\frac{\partial}{\partial a}\mathsf{F} = \bigoplus_{i \in [1;n]} k_i^{(a)} (\mathsf{K}_i \cdot \mathsf{F}) \oplus \bigoplus_{j \in [1;m]} \left(\mathsf{c}(\mathsf{E})\, l_j^{(a)}\right) \mathsf{L}_j$$

L'ensemble des termes dérivés de $(\mathsf{E}{\cdot}\mathsf{F})$ est donc l'union des $(\mathsf{K}_i{\cdot}\mathsf{F})_{i \in [1;n]}$ et des termes dérivés de F; on vérifie que cet ensemble est bien clos :

$$\frac{\partial}{\partial a}(\mathsf{K}_i \cdot \mathsf{F}) = \bigoplus_{p \in [1;n]} z_{i,p}^{(a)} (\mathsf{K}_p \cdot \mathsf{F}) \oplus \bigoplus_{j \in [1;m]} \left[\mathsf{c}(\mathsf{K}_i) \otimes l_j^{(a)}\right] \mathsf{L}_j$$

e) $(\mathsf{E}^\star)$. On calcule les termes dérivés :

$$\frac{\partial}{\partial a}(\mathsf{E}^\star) = \mathsf{c}(\mathsf{E})^* \left(\left[\frac{\partial}{\partial a}\mathsf{E}\right] \cdot (\mathsf{E}^\star)\right) = \bigoplus_{i \in [1;n]} \left[\mathsf{c}(\mathsf{E})^\star \otimes k_i^{(a)}\right] (\mathsf{K}_i \cdot \mathsf{E}^\star)$$

Le nombre des termes dérivés ne change pas, puisqu'il s'agit des $(\mathsf{K}_i \cdot \mathsf{E}^\star)_{i\in[1;n]}$. Cet ensemble est bien clos pour la dérivation :

$$\frac{\partial}{\partial a}(\mathsf{K}_i \cdot \mathsf{E}^\star) = \bigoplus_{j\in[n]} z_{i,j}^{(a)} (\mathsf{K}_j \cdot \mathsf{E}^\star) \oplus \bigoplus_{j\in[n]} \left[\mathsf{c}(\mathsf{K}_i) \otimes \mathsf{c}(\mathsf{E})^* \otimes k_j^{(a)}\right] (\mathsf{K}_j \cdot \mathsf{E}^\star)$$

□

La preuve du théorème 6.1 découle naturellement de la proposition et évite l'utilisation des formules lourdes introduites dans la propositions 6.2.

Démonstration du théorème 6.1. La preuve est par récurrence sur la longueur de u. Si u est réduit à une lettre, le théorème est équivalent à l'égalité i) de la proposition 6.3. Pour tout u dans A^+, et tout a dans A,

$$\frac{\partial}{\partial ua}\mathsf{E} = \frac{\partial}{\partial a}\left(\frac{\partial}{\partial u}\mathsf{E}\right) = \bigoplus_{i\in[1;n]} k_i^{(u)} \frac{\partial}{\partial a}\mathsf{K}_i$$

$$= \bigoplus_{i\in[1;n]} k_i^{(u)} \left[\bigoplus_{j\in[1;n]} z_{i,j}^{(a)} \mathsf{K}_j\right] = \bigoplus_{j\in[1;n]} \left[\bigoplus_{i\in[1;n]} \left[k_i^{(u)} \otimes z_{i,j}^{(a)}\right]\right] \mathsf{K}_j \tag{17}$$

□

Comme nous l'indique la preuve du théorème 6.1, les expressions qui apparaissent dans la dérivée d'une expression E par rapport à un mot sont toutes des termes dérivés de l'expression. Cependant, il se peut que tous n'apparaissent pas; les termes dérivés qui n'apparaissent dans aucun polynôme de l'ensemble $\{\frac{\partial}{\partial u}\mathsf{E} \mid u \in A^*\}$ sont appelés **termes dérivés fantômes**. Ils seront étudiés plus avant dans le paragraphe suivant.

Exemple 26.3 Les termes dérivés de E_2 sont $b\,a$, $(a - b\,a)$, a et 1, parmi lesquels $a = \frac{\partial}{\partial b}(a - b\,a)$ est un terme dérivé fantôme de E_2 (il n'apparaît pas dans l'exemple 26.2).

Remarque 6.5 La proposition 6.3 n'est pas seulement un lemme permettant de prouver le théorème 6.1; c'est aussi la description de l'algorithme le plus naturel pour calculer les termes dérivés de E. Ceux-ci sont calculés par dérivations successives jusqu'à ce que l'ensemble obtenu soit clos.

Le théorème suivant permet d'établir le lien entre le coefficient du mot u dans la série dénotée par une expression E et la dérivée de E par u.

Théorème 6.2 *Soit E une expression de $\mathbb{K}\mathsf{RExp}A$, et $\mathsf{K}_1, \mathsf{K}_2, \ldots, \mathsf{K}_m$ ses termes dérivés. Soit, pour tout mot u de A^+, $k_1^{(u)}, k_2^{(u)}, \ldots, k_m^{(u)}$ les coefficients définis dans le théorème 6.1. On a alors les égalités suivantes :*

$$\langle|\mathsf{E}|,u\rangle = \mathsf{c}(\frac{\partial}{\partial u}\mathsf{E}) = \bigoplus_{i=1}^{i=m} k_i^{(u)} \otimes \mathsf{c}(\mathsf{K}_i) \tag{18}$$

Démonstration. La preuve est par récurrence sur la profondeur de l'expression et utilise la proposition 6.2.

L'égalité est vraie pour les expressions $\mathsf{0}$ et $\mathsf{1}$; la dérivée par rapport à n'importe quel mot u de A^+ est nulle et le coefficient de u dans ces séries est effectivement nul.

De même, si l'expression est une lettre a de A, sauf si $u = a$, auquel cas la dérivée est égale à $\mathsf{1}$ et l'égalité est vraie.

Pour toute paire d'expressions (E,F) pour lesquelles l'égalité est vraie, pour tout k dans $\mathbb{K}$ et tout u dans A^+, on a les égalités suivantes :

$$\begin{aligned}
\langle|(k\,\mathsf{E})|,u\rangle &= k \otimes \langle|\mathsf{E}|,u\rangle = k \otimes \mathsf{c}(\frac{\partial}{\partial u}\,\mathsf{E}) = \mathsf{c}(\frac{\partial}{\partial u}(k\,\mathsf{E}))\\
\langle|(\mathsf{E}\,k)|,u\rangle &= \langle|\mathsf{E}|,u\rangle \otimes k = \mathsf{c}(\frac{\partial}{\partial u}\,\mathsf{E}) \otimes k = \mathsf{c}([\frac{\partial}{\partial u}\,\mathsf{E}]\,k) = \mathsf{c}(\frac{\partial}{\partial u}(\mathsf{E}\,k))\\
\langle|(\mathsf{E}+\mathsf{F})|,u\rangle &= \langle|\mathsf{E}|,u\rangle \oplus \langle|\mathsf{F}|,u\rangle\\
&= \mathsf{c}(\frac{\partial}{\partial u}\,\mathsf{E}) \oplus \mathsf{c}(\frac{\partial}{\partial u}\,\mathsf{F})\\
&= \mathsf{c}(\frac{\partial}{\partial u}(\mathsf{E}+\mathsf{F}))\\
\langle|(\mathsf{E}\cdot\mathsf{F})|,u\rangle &= \langle|(\mathsf{E})|,u\rangle \otimes \langle|(\mathsf{F})|,1_{A^*}\rangle\\
&\qquad \oplus \bigoplus_{\substack{u=v\,w\\ v\in A^*,\, w\in A^+}} \langle|(\mathsf{E})|,v\rangle \otimes \langle|(\mathsf{F})|,w\rangle\\
&= \mathsf{c}(\frac{\partial}{\partial u}\,E) \otimes \mathsf{c}(\mathsf{F}) \oplus \bigoplus_{\substack{u=v\,w\\ v\in A^*,\, w\in A^+}} \mathsf{c}(\frac{\partial}{\partial v}\,\mathsf{E}) \otimes \mathsf{c}(\frac{\partial}{\partial w}\,\mathsf{F})\\
&= \mathsf{c}\left(\left[\frac{\partial}{\partial u}\,E\right]\cdot\mathsf{F} \oplus \bigoplus_{\substack{u=v\,w\\ v\in A^*,\, w\in A^+}} \mathsf{c}(\frac{\partial}{\partial v}\,\mathsf{E})\,\frac{\partial}{\partial w}\,\mathsf{F}\right)\\
&= \mathsf{c}(\frac{\partial}{\partial u}(\mathsf{E}\cdot\mathsf{F}))
\end{aligned}$$

Toutes ces équations, ainsi que la seconde égalité du théorème, proviennent directement de la linéarité de $\mathsf{c}(\mathsf{E})$. Avant d'utiliser les mêmes arguments dans le but de prouver le résultat pour $\mathsf{E}^\star$, on utilise la proposition 1.1. Ceci permet d'éviter d'avoir à traiter une somme infinie; toutefois, on prend soin de revenir ensuite à la série non propre, puisque c'est la seule dont on connaît l'expression.

$$\begin{aligned}
\langle|(\mathsf{E}^\star)|,u\rangle &= \langle(\mathsf{c}(\mathsf{E})^* \otimes |\mathsf{E}|_p)^* \otimes \mathsf{c}(\mathsf{E})^*,u\rangle = \langle(\mathsf{c}(\mathsf{E})^* \otimes |\mathsf{E}|_p)^*,u\rangle \otimes \mathsf{c}(\mathsf{E})^*\\
&= \bigoplus_{\substack{u=v_1v_2\cdots v_n\\ v_1,v_2,\ldots,v_n\in A^+}} \langle\mathsf{c}(\mathsf{E})^* \otimes |\mathsf{E}|_p,v_1\rangle \otimes \ldots \otimes \langle\mathsf{c}(\mathsf{E})^* \otimes |\mathsf{E}|_p,v_n\rangle \otimes \mathsf{c}(\mathsf{E})^*\\
&= \bigoplus_{\substack{u=v_1v_2\cdots v_n\\ v_1,v_2,\ldots,v_n\in A^+}} \mathsf{c}(\mathsf{E})^* \otimes \langle|\mathsf{E}|_p,v_1\rangle \otimes \ldots \otimes \mathsf{c}(\mathsf{E})^* \otimes \langle|\mathsf{E}|_p,v_n\rangle \otimes \mathsf{c}(\mathsf{E})^*
\end{aligned}$$

Comme les v_i sont *tous différents du mot vide*, $\langle |\mathsf{E}|_p, v_i\rangle = \langle |\mathsf{E}|, v_i\rangle$.

$$
\begin{aligned}
\langle |(\mathsf{E}^\star)|, u\rangle &= \bigoplus_{\substack{u=v_1v_2\cdots v_n\\ v_1,v_2,\ldots,v_n\in A^+}} \mathsf{c}(\mathsf{E})^* \otimes \mathsf{c}(\frac{\partial}{\partial v_1}\mathsf{E}) \otimes \ldots \otimes \mathsf{c}(\mathsf{E})^* \otimes \mathsf{c}(\frac{\partial}{\partial v_n}\mathsf{E}) \otimes \mathsf{c}(\mathsf{E})^* \\
&= \mathsf{c}\left(\bigoplus_{\substack{u=v_1v_2\cdots v_n\\ v_1,v_2,\ldots,v_n\in A^+}} \mathsf{c}(\mathsf{E})^* \otimes \mathsf{c}(\frac{\partial}{\partial v_1}\mathsf{E}) \otimes \ldots \otimes \mathsf{c}(\mathsf{E})^* \left(\left[\frac{\partial}{\partial v_n}\mathsf{E}\right] \cdot (\mathsf{E}^\star)\right)\right) \\
&= \mathsf{c}(\frac{\partial}{\partial u}\mathsf{E}^\star)
\end{aligned}
$$

□

La proposition 6.1 apparaît alors comme un corollaire :

Démonstration de la proposition 6.1. Une preuve par récurrence immédiate montre que, pour tout couple de mots u et v de A^* et pour toute expression E,

$$\frac{\partial}{\partial uv}\mathsf{E} = \frac{\partial}{\partial v}\left[\frac{\partial}{\partial u}\mathsf{E}\right],$$

D'où, pour toute paire de mots u et v de A^*,

$$\langle u^{-1}|\mathsf{E}|, v\rangle = \langle |\mathsf{E}|, uv\rangle = \mathsf{c}(\frac{\partial}{\partial uv}\mathsf{E}) = \mathsf{c}\left(\frac{\partial}{\partial v}\left[\frac{\partial}{\partial u}\mathsf{E}\right]\right) = \langle |\frac{\partial}{\partial u}\mathsf{E}|, v\rangle$$

□

Remarque 6.6 La dérivation et le quotient sont deux actions à droite de A^* sur l'ensemble des polynômes d'expressions rationnelles et l'ensemble des séries respectivement. Le théorème 6.1 nous dit que l'orbite d'une expression rationnelle sous l'action de A^* appartient à un $\mathbb{K}$-semi-module finiment engendré. La fonction qui associe à chaque polynôme d'expressions P, la série rationnelle $|P|$ est un morphisme d'actions. Le théorème 6.1 implique donc que l'orbite d'une série rationnelle sous l'action de A^* appartient elle aussi à un $\mathbb{K}$-semi-module finiment engendré, ce qui donne une nouvelle preuve d'un résultat classique [8]. Soulignons que ce résultat n'est pas le but que nous poursuivons. Il s'agit avant tout de trouver un moyen effectif, en manipulant des expressions, de construire un automate.

— ∘ —

4 L'automate des termes dérivés

A toute expression avec multiplicité E de $\mathbb{K}\mathsf{RExp}A$, on associe un $\mathbb{K}$-automate de la façon suivante :

Définition 6.7 *Soit* $P = \{\mathsf{K}_1, \mathsf{K}_2, \ldots, \mathsf{K}_n\}$ *l'ensemble des termes dérivés de* E. *Soit* $\mathsf{K}_0 =$

*E et P_E l'union de P et de $\{\mathsf{K}_0\}$. L'**automate des termes dérivés** de E est le $\mathbb{K}$-automate $\mathcal{A}_\mathsf{E} = \langle P_\mathsf{E}, A, Z, I, T \rangle$ défini par :*

$$I_{\mathsf{K}_i} = \begin{cases} 1_\mathbb{K} & \textit{si} \quad \mathsf{K}_i = \mathsf{K}_0 \\ 0_\mathbb{K} & \textit{sinon} \end{cases}, \qquad Z_{\mathsf{K}_i,\mathsf{K}_j} = \bigoplus_{a \in A} z_{i,j}^{(a)}\, a\,, \qquad T_{\mathsf{K}_j} = \mathsf{c}(\mathsf{K}_j),$$

où les $z_{i,j}^{(a)}$ sont définis dans l'énoncé de la proposition 6.3.

Théorème 6.3 *Soit E une expression de $\mathbb{K}\mathsf{RExp}A$. La série réalisée par l'automate des termes dérivés de E est égale à la série dénotée par E.*

$$|\mathcal{A}_\mathsf{E}| = |\mathsf{E}|$$

Démonstration. La définition du $\mathbb{K}$-automate $\mathcal{A}_\mathsf{E}$ est en effet équivalente à celle d'une d'une $\mathbb{K}$-représentation linéaire (I,ζ,T). I et T sont vus respectivement comme des vecteurs ligne et colonne indicés par P_E, alors que ζ est un morphisme de A^* dans la semi-algèbre des matrices indicées par P_E défini par $(a)\zeta_{\mathbb{K}_i,\mathbb{K}_j} = (z_{i,j}^{(a)})$, pour tout a dans A.
La série réalisée par la représentation et par l'automate est :

$$|\mathcal{A}_\mathsf{E}| = \bigoplus_{f \in A^*} (I \cdot (f)\zeta \cdot T)\, f.$$

D'après l'équation 17, on obtient par récurence sur la longueur de f que

$$\forall f \in A^+\,, \quad \forall i \in [n] \qquad (I \cdot (f)\zeta)_i = k_i^{(f)},$$

d'où, pour tout mot f de A^+, d'après le théorème 6.3,

$$\langle |\mathcal{A}_\mathsf{E}|, f\rangle = \bigoplus_{i[n]} k_i^{(f)}\ \mathsf{c}(\mathsf{K}_i) = \langle |\mathsf{E}|, f\rangle.$$

Il suffit enfin de vérifier qu'on a une égalité similaire pour le mot vide :

$$\langle |\mathcal{A}_\mathsf{E}|, 1_{A^*}\rangle = \mathsf{c}(\mathsf{K}_0) = \mathsf{c}(\mathsf{E}).$$

□

Le passé et le futur d'un état de l'automate des termes dérivés dépendent directement du terme dérivé auquel cet état correspond.

Proposition 6.4 *Soit E une expression de $\mathbb{K}\mathsf{RExp}A$ et K un terme dérivé de E. Le passé et le futur de l'état K de l'automate $\mathcal{A}_\mathsf{E}$ des termes dérivés de E vérifient les égalités suivantes :*

$$\forall u \in A^* \qquad \langle \mathsf{Past}_{\mathcal{A}_\mathsf{E}}(\mathsf{K}), u\rangle = \langle \frac{\partial}{\partial u}\,\mathsf{E}, \mathsf{K}\rangle$$
$$\mathsf{Fut}_{\mathcal{A}_\mathsf{E}}(\mathsf{K}) = |\mathsf{K}|.$$

Démonstration. La preuve de la première égalité est par récurrence sur la longueur de u. Le résultat est vrai pour le mot vide, puisque chacun de ses membres est nul, sauf si $\mathsf{K} = \mathsf{E}$, auquel cas, chacun des membres vaut $1_{\mathbb{K}}$. On suppose le résultat vrai pour u. Alors, pour tout a dans A, pour tout terme dérivé K_j, d'après l'égalité (17),

$$\begin{aligned}
\langle \frac{\partial}{\partial ua}\,\mathsf{E}, \mathsf{K}_j\rangle &= \bigoplus_{i\in[1;n]} \left[k_i^{(u)} \otimes z_{i,j}^{(a)}\right] \\
&= \bigoplus_{i\in[1;n]} \langle \frac{\partial}{\partial u}\,\mathsf{E}, \mathsf{K}_j\rangle \otimes z_{i,j}^{(a)} \\
&= \bigoplus_{i\in[1;n]} \langle \mathsf{Past}_{\mathcal{A}_E d}(\mathsf{K}_i), u\rangle \otimes z_{i,j}^{(a)} \\
&= \bigoplus_{i\in[1;n]} \langle \mathsf{Past}_{\mathcal{A}_E d}(\mathsf{K}_i) Z_{\mathsf{K}_i,\mathsf{K}_j}, ua\rangle \\
&\langle \mathsf{Past}_{\mathcal{A}_\mathsf{E}}(\mathsf{K}_j), ua\rangle
\end{aligned}$$

L'autre égalité se démontre de la même façon que le théorème 6.3. Il suffit de prendre comme expression de départ non plus E mais K. On obtient un automate $\mathcal{A}_\mathsf{K}$ qui réalise la série $|\mathsf{K}|$ et qui est identique à l'automate $\mathcal{A}_\mathsf{E}$ en aval de l'état K. Le comportement de $\mathcal{A}_\mathsf{K}$ est donc exactement le futur de K dans $\mathcal{A}_\mathsf{E}$. □

— ∘ —

5 Les termes dérivés fantômes

La proposition 6.4 nous indique que le passé d'un état de l'automate des termes dérivés est lié à l'apparition de ce terme dans les dérivées de l'expression de départ par rapport aux mots de A^*. Comme nous l'avons déjà dit, il est possible que certains termes dérivés n'apparaissent dans aucune dérivée de E. Ce sont les termes dérivés fantômes.

D'après la proposition 6.4, le passé d'un état de l'automate des termes dérivés qui correspond à un terme fantôme est nul. On peut donc supprimer ces états sans modifier le comportement de l'automate. Encore faut-il les identifier !

Semi-anneaux positifs

Définition 6.8 *Un semi-anneau est **positif** si aucun n'élément n'a d'opposé (pour l'addition) et s'il est intègre, c'est-à-dire que le produit de deux éléments non nuls est non nul.*

De nombreux semi-anneaux courants sont positifs. Citons, bien sûr, le semi-anneau des entiers naturels, mais aussi tous les semi-anneaux $(\mathsf{max}\,,+)$ ou $(\mathsf{min}\,,+)$ construits à partir de sous-ensembles de $\mathbb{R}$. Le semi-anneau $\mathcal{P}(A^*)$ formé à partir du monoïde libre est aussi un semi-anneau positif.

PROPOSITION 6.5 *Aucun terme dérivé d'une série formelle s sur A^*, à coefficient dans un semi-anneau positif, n'est un terme dérivé fantôme.*

Démonstration. A partir de l'ágalité (17) page 163, on montre immédiatement par récurrence sur la longueur des mots, que, si u est un mot de A^+ longueur m, alors, pour tout i dans $[1;n]$, on a :

$$k_i^{(u)} = \bigoplus_{i_1,\dots,i_{m-1}\in[1;n]} k_{i_1}^{(u_1)} \otimes z_{i_1,i_2}^{(u_2)} \otimes z_{i_2,i_3}^{(u_3)} \otimes \dots \otimes z_{i_{m-1},i}^{(u_m)}. \tag{19}$$

Si un terme dérivé K existe, c'est qu'il existe une suite $\mathsf{K}_{i_0} = \mathsf{E}, \mathsf{K}_{i_1}, \dots, \mathsf{K}_{i_m} = \mathsf{K}$ de termes dérivés et un mot $u_1u_2\dots u_m$ tels que, pour tout j de $[1;m]$, $\langle \frac{\partial}{\partial u_j} \mathsf{K}_{i_{j-1}}, \mathsf{K}_{i_j}\rangle = z_{i_{j-1},i_j}^{(u_j)} \neq 0_{\mathbb{K}}$. Il y a donc, dans l'égalité (19), un produit de facteurs non nuls; comme le semi-anneau est positif, ce produit n'est pas nul et la somme dont il fait partie non plus, donc le terme dérivé K apparaît dans la dérivée de E par rapport à u. □

Comme le semi-anneau de Boole est un semi-anneau positif, il n'y a pas de termes dérivés fantômes dans le cadre des dérivations d'expressions sans multiplicité.

Semi-anneaux plongeables dans un corps. Dans ce cas, on peut voir apparaître des termes dérivés fantômes. C'est d'ailleurs ce qu'illustre l'exemple 26.3. On peut toutefois simplifier l'automate si des termes dérivés fantômes apparaissent. On utilise pour cela le « théorème d'égalité » (*cf.* [23] page 143) pour tester si le passé d'un état est nul.

Autres semi-anneaux. Dans le cas général, la décision dépend non seulement de la taille et de la structure de l'automate, mais aussi de la struture du semi-anneau.

EXEMPLE 28 Considérons l'expression rationnelle $\mathsf{E}_5 = (ya)\cdot(xb)^\star\cdot(ya)$ sur l'alphabet $\{a,b\}$ à coefficients dans un semi-anneau contenant deux éléments x et y. La dérivation de cette expression donne les termes dérivés $(xb)^\star\cdot(ya)$ et 1. L'automate qui en résulte est dessiné figure 4. On peut se demander si 1 est un terme dérivé fantôme. Sans autre rensei-

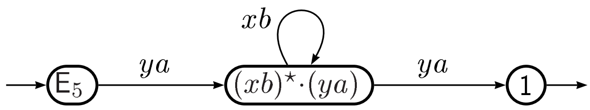


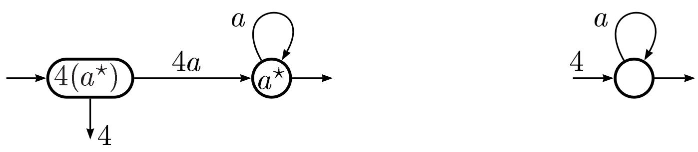
FIG. 4 – *L'automate des termes dérivés de E_5.*

gnement sur le semi-anneau, cette question est indécidable. En effet, pour tout k dans $\mathbb{N}$, la dérivée de E_5 par rapport à ab^ka est égale à $y \otimes x^k \otimes y\, 1$. Et pour tout N, il existe un semi-anneau et des éléments x et y tels que le plus petit k pour lequel cette quantité n'est pas nulle est N. (On peut par exemple prendre le semi-anneau des relations sur $[1; N+1]$, x égal à la rotation $(1,2,\dots,N+1)$ et y à la fonction partielle qui envoie 1 sur 2.)

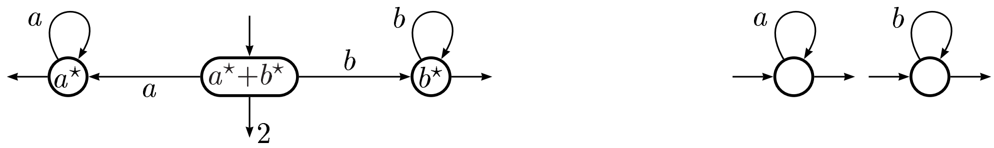
— ∘ —

6 Variations

On peut imaginer un certain nombres de variations dans la façon dont est définie la dérivation. On peut par exemple regretter que l'expression $4(a^\star)$ soit représentée par le premier de ces deux automates et non par le second :



De même pour l'expression $a^\star{+}b^\star$:



Nous allons voir que le comportement de l'algorithme, c'est-à-dire la portée de la dérivation, est très fortement conditionné par la dérivation par rapport au mot vide. Nous avons dit dans la définition 6.6 que la dérivation d'une expression par rapport au mot vide était l'identité. C'est cette convention que nous allons amender dans les paragraphes suivants.

Termes dérivés unitaires. Dans un premier temps, il apparaît souhaitable d'extraire le plus rapidement possible les coefficients de l'expression, par exemple lorsque l'expression a un coefficient principal gauche non trivial (c'est-à-dire lorsqu'il y a un coefficient gauche dans la racine de l'arbre de l'expression qui est différent de $1_{\mathbb{K}}$).

DÉFINITION 6.9 *Une expression est* ***unitaire*** *(gauche) si son coefficient principal à gauche est égal à $1_{\mathbb{K}}$. Toute expression E de $\mathbb{K}\mathsf{RExp}A$ peut s'écrire $(k\,\mathsf{F})$, où k est un élément de $\mathbb{K}$ et F est une expression unitaire gauche. Pour toute expression unitaire F, tout élément k de $\mathbb{K}$, on définit la* ***dérivée unitaire*** *de $(k\,\mathsf{F})$ par rapport au mot vide par :*

$$\frac{\partial_{\mathrm{u}}}{\partial_{\mathrm{u}} 1_{A^*}}(k\,\mathsf{F}) = k\,\mathsf{F}.$$

Par suite, la dérivée unitaire d'une expression E par rapport à une lettre a est définie par :

$$\frac{\partial_{\mathrm{u}}}{\partial_{\mathrm{u}} a}\,\mathsf{E} = \frac{\partial_{\mathrm{u}}}{\partial_{\mathrm{u}} 1_{A^*}}\left(\frac{\partial}{\partial a}\,\mathsf{E}\right),$$

et en remplaçant chaque dérivation par une dérivation unitaire dans les formules de la définition 6.5.

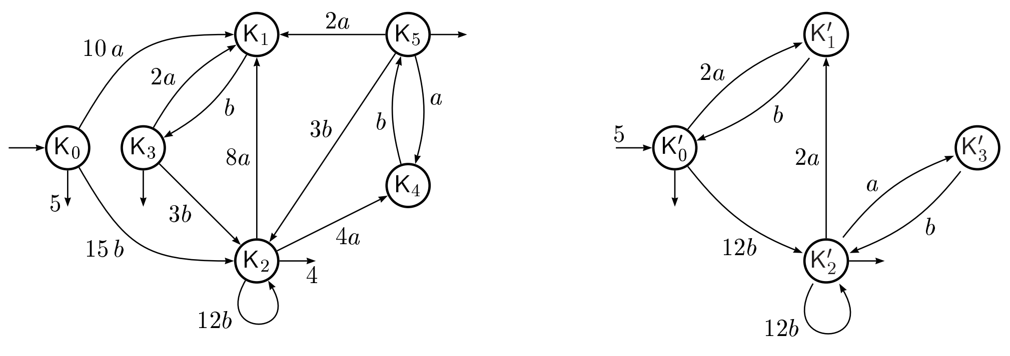
Les termes dérivés obtenus par une telle dérivation sont unitaires gauches.

On peut montrer que, de même que pour la dérivation « simple », le nombre de termes dérivés unitaires est inférieur à la longueur de l'expression. La borne sur la taille de l'automate obtenu est donc respectée. Mieux, il existe une fonction surjective des termes dérivés sur les termes dérivés unitaires, l'automate des termes dérivés unitaires est donc plus petit que celui des termes dérivés.

Exemple 27.2 Calculons les termes dérivés (colonne de gauche) et les termes dérivés unitaires de $\mathsf{E}_3 = (5((2ab) + ((3b) \cdot (4(ab)^*)))^*)$:

$$
\begin{aligned}
\mathsf{K}_0 &= \mathsf{E}_3 \\
\frac{\partial}{\partial a}\mathsf{K}_0 &= 10\,(b \cdot \mathsf{F}_3) = 10\,\mathsf{K}_1 \\
\frac{\partial}{\partial b}\mathsf{K}_0 &= 15\,((4\,(ab)^*) \cdot \mathsf{F}_3) = 15\,\mathsf{K}_2 \\
\frac{\partial}{\partial b}\mathsf{K}_1 &= \mathsf{F}_3 = \mathsf{K}_3 \\
\frac{\partial}{\partial a}\mathsf{K}_2 &= 4\,((b \cdot (ab)^*) \cdot \mathsf{F}_3) \oplus 8\,(b \cdot \mathsf{F}_3) \\
&= 4\,\mathsf{K}_4 \oplus 8\,\mathsf{K}_1 \\
\frac{\partial}{\partial b}\mathsf{K}_2 &= 12\,((4\,(ab)^*) \cdot \mathsf{F}_3) = 12\,\mathsf{K}_2 \\
\frac{\partial}{\partial a}\mathsf{K}_3 &= 2\,(b \cdot \mathsf{F}_3) = 2\,\mathsf{K}_1 \\
\frac{\partial}{\partial b}\mathsf{K}_3 &= 3\,\mathsf{K}_2 \\
\frac{\partial}{\partial b}\mathsf{K}_4 &= ((ab)^* \cdot \mathsf{F}_3) = \mathsf{K}_5 \\
\frac{\partial}{\partial a}\mathsf{K}_5 &= \mathsf{K}_4 \oplus 2\,\mathsf{K}_1, \quad \frac{\partial}{\partial b}\mathsf{K}_5 = 3\,\mathsf{K}_2 \\
\mathsf{c}(\mathsf{K}_0) &= 5, \mathsf{c}(\mathsf{K}_1) = \mathsf{c}(\mathsf{K}_4) = 0 \\
\mathsf{c}(\mathsf{K}_2) &= 4, \mathsf{c}(\mathsf{K}_3) = \mathsf{c}(\mathsf{K}_5) = 1
\end{aligned}
$$

$$
\begin{aligned}
\mathsf{K}'_0 &= \mathsf{F}_3 \qquad k_0 = 5 \\
\frac{\partial_{\mathrm{u}}}{\partial_{\mathrm{u}} a}\mathsf{K}'_0 &= 2\,(b \cdot \mathsf{F}_3) = 2\,\mathsf{K}'_1 \\
\frac{\partial_{\mathrm{u}}}{\partial_{\mathrm{u}} b}\mathsf{K}'_0 &= 12\,((ab)^* \cdot \mathsf{F}_3) = 12\,\mathsf{K}'_2 \\
\frac{\partial_{\mathrm{u}}}{\partial_{\mathrm{u}} b}\mathsf{K}'_1 &= \mathsf{F}_3 = \mathsf{K}'_0 \\
\frac{\partial_{\mathrm{u}}}{\partial_{\mathrm{u}} a}\mathsf{K}'_2 &= ((b \cdot (ab)^*) \cdot \mathsf{F}_3) \oplus 2\,(b \cdot \mathsf{F}_3) \\
&= \mathsf{K}'_3 \oplus 2\,\mathsf{K}'_1 \\
\frac{\partial_{\mathrm{u}}}{\partial_{\mathrm{u}} b}\mathsf{K}'_2 &= 12\,((ab)^* \cdot \mathsf{F}_3) = 12\,\mathsf{K}'_2 \\
\frac{\partial_{\mathrm{u}}}{\partial_{\mathrm{u}} b}\mathsf{K}'_3 &= ((ab)^* \cdot \mathsf{F}_3) = \mathsf{K}'_2 \\
\mathsf{c}(\mathsf{K}'_0) &= \mathsf{c}(\mathsf{K}'_2) = 1 \\
\mathsf{c}(\mathsf{K}'_1) &= \mathsf{c}(\mathsf{K}'_3) = 0
\end{aligned}
$$



(a) L'automate des termes dérivés de E_3 (b) L'automate des termes dérivés unitaires

Fig. 5 – *Deux* $\mathbb{K}$*-automates pour* E_3

La figure 5 a) représente l'automate des termes derivés de E_3 (qui est isomorphe à l'automate de Glushkov calculé dans [11]); b) représente l'automate des termes dérivés unitaires de E_3.

Exemple 24.4 On calcule l'automate des termes unitaires de E_4. Comme E_4, n'est pas une expression unitaire, ce choix semble s'imposer. On pose $\mathsf{E}_4 = \mathrm{y}\,\mathsf{F}_4$.

$$\frac{\partial_{\mathrm{u}}}{\partial_{\mathrm{u}} 1_{A^*}} \mathsf{E}_4 = \mathrm{y}\,\mathsf{F}_4 = \mathrm{y}\,\mathsf{K}_0$$

$$\frac{\partial_{\mathrm{u}}}{\partial_{\mathrm{u}} a} \mathsf{K}_0 = \mathrm{x}\,((((\mathrm{y}\,b)^\star \cdot a)\,\mathrm{y}) \cdot \mathsf{F}_4) = \mathrm{x}\,\mathsf{K}_1 \qquad \frac{\partial_{\mathrm{u}}}{\partial_{\mathrm{u}} b} \mathsf{K}_0 = \mathrm{y}\,((((\mathrm{x}\,a)^\star \cdot b)\,\mathrm{x}) \cdot \mathsf{F}_4) = \mathrm{y}\,\mathsf{K}_2$$

$$\frac{\partial_{\mathrm{u}}}{\partial_{\mathrm{u}} a} \mathsf{K}_1 = \mathrm{y}\,\mathsf{F}_4 = \mathrm{y}\,\mathsf{K}_0 \qquad \frac{\partial_{\mathrm{u}}}{\partial_{\mathrm{u}} a} \mathsf{K}_2 = \mathrm{x}\,((((\mathrm{x}\,a)^\star \cdot b)\,\mathrm{x}) \cdot \mathsf{F}_4) = \mathrm{x}\,\mathsf{K}_2$$

$$\frac{\partial_{\mathrm{u}}}{\partial_{\mathrm{u}} b} \mathsf{K}_1 = \mathrm{y}\,((((\mathrm{y}\,b)^\star \cdot a)\,\mathrm{y}) \cdot \mathsf{F}_4) = \mathrm{x}\,\mathsf{K}_1 \qquad \frac{\partial_{\mathrm{u}}}{\partial_{\mathrm{u}} b} \mathsf{K}_2 = \mathrm{x}\,\mathsf{F}_4 = \mathrm{x}\,\mathsf{K}_0$$

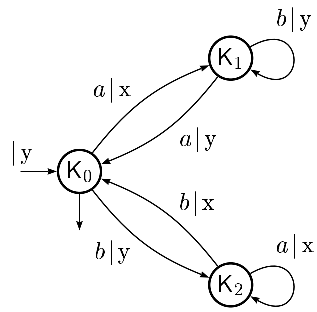


Fig. 6 – *Automate des termes unitaires de* E_4

— ∘ —

Dérivation cassante. Par ailleurs, on peut considérer que le symbole + d'une expression rationnelle est interprété directement lorsqu'il apparaît en dehors d'une expression « étoilée » ou d'un produit.

Définition 6.10 *Pour toutes expressions* E *et* F *de* $\mathbb{K}\mathsf{RExp}A$*, on définit la* ***dérivée cassante*** *de* $(\mathsf{E}+\mathsf{F})$ *par rapport au mot vide par :*

$$\frac{\partial_{\mathrm{c}}}{\partial_{\mathrm{c}} 1_{A^*}} (\mathsf{E}+\mathsf{F}) = \mathsf{E} \oplus \mathsf{F}.$$

Par suite, la dérivée cassante d'une expression E *par rapport à une lettre* a *est définie par :*

$$\frac{\partial_{\mathrm{c}}}{\partial_{\mathrm{c}} a} \mathsf{E} = \frac{\partial_{\mathrm{c}}}{\partial_{\mathrm{c}} 1_{A^*}} \left(\frac{\partial}{\partial a} \mathsf{E} \right),$$

et en remplaçant chaque dérivation par une dérivation unitaire dans les formules de la définition 6.5. De plus, on peut poser :

$$\frac{\partial_{\mathrm{c}}}{\partial_{\mathrm{c}} a} (\mathsf{E}\cdot\mathsf{F}) = \left(\frac{\partial_{\mathrm{c}}}{\partial_{\mathrm{c}} a} \mathsf{E} \cdot \frac{\partial_{\mathrm{c}}}{\partial_{\mathrm{c}} 1_{A^*}} \mathsf{F} \right) \oplus \mathsf{c}(\mathsf{E}) \, \frac{\partial_{\mathrm{c}}}{\partial_{\mathrm{c}} a} \mathsf{F}.$$

Cette nouvelle façon de faire permet d'obtenir sur l'exemple $a^\star + b^\star$ déjà cité un résultat plus proche de l'intuition. Cependant, cette méthode ne permet pas de garantir que le nombre d'états de l'automate obtenu sera linéaire en la longueur de l'expression.

— ∘ —

7 Le cas commutatif

L'hypothèse de commutativité du semi-anneau $\mathbb{K}$ simplifie quelque peu les choses. En effet, dans ce cas, pour toute expression rationnelle E et tout élément k de $\mathbb{K}$, les expressions $(k\,\mathsf{E})$ et $(\mathsf{E}\,k)$ sont équivalentes. On peut donc supposer que la multiplication d'une expression par un coefficient s'effectue toujours à gauche. La définition des expressions est alors la suivante :

i) $\mathsf{0}$, $\mathsf{1}$, et a, pour tout a appartenant à A, sont des expressions rationnelles (atomiques).

ii) Si E est une expression rationnelle, et k un élément de $\mathbb{K}$, alors $(k\,\mathsf{E})$ est une expression rationnelle.

iii) Si E et F sont des expressions rationnelles, alors $(\mathsf{E}+\mathsf{F})$, $(\mathsf{E}\cdot\mathsf{F})$ et (E^*) aussi.

Les identités triviales sur les expressions sont un tant soit peu plus simples :

$$\begin{gathered}(k\,\mathsf{0}) \equiv \mathsf{0}\,, \quad (0_{\mathbb{K}}\,\mathsf{E}) \equiv \mathsf{0}\,, \quad (\mathsf{0}\cdot\mathsf{E}) \equiv (\mathsf{E}\cdot\mathsf{0}) \equiv \mathsf{0}\,, \\ \mathsf{0}+\mathsf{E} \equiv \mathsf{E}+\mathsf{0} \equiv \mathsf{E}\,, \quad (1_{\mathbb{K}}\,\mathsf{E}) \equiv \mathsf{E}\,, \\ ((k\,\mathsf{1})\cdot\mathsf{E}) \equiv (\mathsf{E}\cdot(k\,\mathsf{1})) \equiv (k\,\mathsf{E})\,, \\ (k\,(k'\,\mathsf{E})) \equiv ([k\otimes k']\,\mathsf{E}).\end{gathered}$$

La représentation en arbre d'une expression est elle aussi simplifiée, puisqu'à chaque nœud n'est affecté qu'un coefficient. Les résultats, quant à eux, restent inchangés; la dérivation est définie de la même manière, si ce n'est qu'on ignore l'axiome $\frac{\partial}{\partial a}(\mathsf{E}\,k) = ([\frac{\partial}{\partial a}\,\mathsf{E}]\,k)$ qui n'a plus lieu d'être.

On peut définir la multiplication des monômes d'expressions de manière légèrement différente :

$$[k\,\mathsf{E}]\cdot[k'\,\mathsf{F}] = [k\otimes k']\,(\mathsf{E}\cdot\mathsf{F}).$$

Ceci permet, dans le cas de la dérivation unitaire, de définir la dérivée du produit :

$$\frac{\partial_{\mathrm{u}}}{\partial_{\mathrm{u}} a}(\mathsf{E}\cdot\mathsf{F}) = \left(\frac{\partial_{\mathrm{u}}}{\partial_{\mathrm{u}} a}\,\mathsf{E}\cdot\,\frac{\partial_{\mathrm{u}}}{\partial_{\mathrm{u}} 1_{A^*}}\,\mathsf{F}\right) \oplus \mathsf{c}(\mathsf{E})\;\frac{\partial_{\mathrm{u}}}{\partial_{\mathrm{u}} a}\,\mathsf{F}.$$

Cet aménagement n'aurait pas de sens dans le cas non commutatif car le coefficient qui peut « sortir » du second facteur serait immédiatement réenchâssé à cause de la multiplication des monômes.

— ◦ —

Table des exemples

Index

Bibliographie

[1] A. Ambainis et R. Freivalds, 1-way quantum finite automata: strengths, weaknesses and generalizations. In *39th Ann. Symposium on FOCS* (1998), 332–342.

[2] D. Angluin, Inference of reversible languages. *J. of the ACM* **29** (1982), 741–765.

[3] V. Antimirov, Partial derivatives of regular expressions and finite automaton constructions. *Theoret. Comput. Sci.* **155** (1996), 291–319.

[4] A. Arnold, A. Dicky, et M. Nivat, A note about minimal non-deterministic automata. *Bull ot the EATCS* **47** (1992), 166–169.

[5] M.-P. Béal, O. Carton, C. Prieur, et J. Sakarovitch, Squaring transducers. *Proc. of Latin 2000, Lect. Notes in Comp. Sci.* **1776** (2000), 397–406.

[6] G. Berry et R. Sethi, From regular expressions to deterministic automata, *Theoret. Comput. Sci.* **48** (1986), 117–126.

[7] J. Berstel et J.-E. Pin, Local languages and the Berry-Sethi algorithm, *Theoret. Comput. Sci.* **155** (1996), 439–446.

[8] J. Berstel et Ch. Reutenauer, *Les séries rationnelles et leurs langages.* Masson, 1984. Traduction: *Rational Series and their Languages.* Springer, 1986.

[9] J. A. Brzozowski, Derivatives of regular expressions. *J. Assoc. Comput. Mach.* **11** (1964), 481–494.

[10] A. Buchsbaum, R. Giancarlo, et J. Westbrook, On the Determinization of Weighted Finite Automata. *Proc. of ICALP'98, Lect. Notes in Comp. Sci.* **1443** (1998), 482–493.

[11] P. Caron et M. Flouret, Glushkov construction for multiplicities. *Pre-Proceedings of CIAA'00*, M. Daley, M. Eramian and S. Yu, eds, Univ. of Western Ontario, (2000), 52–61.

[12] O. Carton, Factorisations et matrice des facteurs. Manuscrit (1994).

[13] J.-M. Champarnaud et D. Ziadi, New finite automaton constructions based on canonical derivatives. *Pre-Proceedings of CIAA'00*, M. Daley, M. Eramian and S. Yu, eds, Univ. of Western Ontario, (2000), 36–43.

[14] Ch. Choffrut, Une caractérisation des fonctions séquentielles et des fonctions sous-séquentielles en tant que relations rationnelles. *Theoret. Comput. Sci.* **5** (1977), 325–337.

[15] M. Chrobak, Finite Automata and Unary Languages. *Theoret. Comput. Sci.* **47** (1986), 149–158.

[16] G. Cohen, P. Moller, J.-P. Quadrat, et M. Viot, Algebraic Tools for the Performance Evaluation of Discrete Event Systems. *IEEE Proc.: Special issue on D.E.S.* **77.1** (1989).

[17] R. Cohen, Star height of certain families of regular events. *J. Computer System Sci.* **4** (1970), 281–297.

[18] R. Cohen et J. A. Brzozowski, General properties of star height of regular events. *J. Computer System Sci.* **4** (1970), 260–280.

[19] J. H. Conway, *Regular algebra and finite machines.* Chapman and Hall, 1971.

[20] B. Courcelle, D. Niwinski, A. Podelski, A geometrical view of the dererminization ond minimization of finite-state automata. *Math. Systems Theory* **24** (1991), 117–146.

[21] F. Dejean et M.-P. Schützenberger, On a question of Eggan. *Inform. and Control* **9** (1966), 23–25.

[22] L. C. Eggan, Transition graphs and the star-height of regular events. *Michigan Mathematical J.* **10** (1963), 385–397.

[23] S. Eilenberg, *Automata, Languages and Machines, volume A.* Academic Press, 1974.

[24] S. Gaubert, Rational Series over Dioids and Discrete Event Systems. *Proc. of the 11th Conf. on Anal. and Opt. of Systems, Lect. Notes in Contr. and Inf. Sci.* **199** (1994).

[25] S. Gaubert, On the Burnside problem for Semigroups of Matrices in the $(\max,+)$ Algebra. *Semigroup Forum* **52** (1996), 271–292.

[26] S. Gaubert, Methods and applications of $(\max,+)$ linear algebra. *rapport de recherche INRIA* **3088** (1997).

[27] V. Glushkov, The abstract theory of automata. *Russian Mathematical Surveys 16* (1961), 1–53.

[28] Ch. Hagenah et A. Muscholl, Computing ε-Free NFA from regular expressions in $O(n\log^2(n))$ time. *R.A.I.R.O. Inf. Théorique* **34**, (2000), 257–277.

[29] T.E. Hall, Biprefix codes, inverse semigroups and syntactic monoids of injective automata. *Theoret. Comput. Sci.* **32** (1984), 201–213.

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

[31] K. Hashiguchi et N. Honda, The star height of reset-free events and strictly locally testable events. *Inform. and Control* **40** (1979), 267–284.

[32] K. Hashiguchi, Limitedness theorem on finite automata with distance functions. *J. of Comput. Syst. Sci.* **24** (1982), 233–244.

[33] K. Hashiguchi, Algorithms for determining relative star height and star height. *Inform. and Computation* **78** (1988), 124–169.

[34] K. Hashiguchi, Improved limitedness theorem on finite automata with distance functions. *Theoret. Comput. Sci.* **72** (1990), 27–38.

[35] P.-C. Héam, A lower bound for reversible automata. *Theoret. Informatics Appl.* **34** (2000), 331–341.

[36] P.-C. Héam, Contribution à l'algorithmique des automates : complexité et aspects topologiques. *Thèse de doctorat*, Université Paris 7, 2001.

[37] J. Hromkovič, S. Seibert, et T. Wilke, Translating regular expressions into small ε-free nondeterministic finite automata. *Proc. of STACS'97, Lect. Notes in Comp. Sci.* **1200** (1997), 55–66.

[38] D. Krob, Differentiation of K-rational expressions. *Int. J. of Algebra and Computation 2* (1992), 57–87.

[39] W. Kuich et A. Salomaa, *Semirings, Automata, Languages.* Springer, 1986.

[40] G. Lallement, *Semigroups and combinatorial applications.* Wiley, 1979.

[41] H. Leung, Limitedness theorem on finite automata with distance functions: an algebraic proof *Theoret. Comput. Sci.* **81** (1991), 137–145.

[42] S. Lombardy et J. Sakarovitch, On the star height of rational languages, a new presentation for two old results *Proc. of 3rd ICLWC, Kyoto* (2000) (M. Ito, ed.), World Scientific, *à paraître.*

[43] S. Lombardy et J. Sakarovitch, Star height of reversible languages and universal automata, *accepté à Latin'02.*

[44] S. Lombardy, Sequentialization and unambiguity of (max, +) rational series over one letter. *Pre-Proc. of Workshop on Max-plus algebra, Prague* (2001) (S. Gaubert, ed.).

[45] O. Matz et A. Potthoff, Computing small nondeterministic finite automata. *proc. of TACAS'95, BRICS Notes Series* (1995), 74–88.

[46] R. McNaughton et H. Yamada, Regular expressions and state graphs for automata. *IRE Trans. on electronic computers* **9** (1960), 39–47.

[47] R. McNaughton, The loop complexity of pure-group events. *Inform. and Control* **11** (1967), 167–176.

[48] Moebius, *Sur l'étoile.* Gentiane, 1983, Rééd. Casterman, 1990.

[49] M. Mohri, Finite-State Transducers in Language and Speech Processing. *Computat. Ling.* **23.2** (1997), 269–311.

[50] C. Nicaud, Étude du comportement en moyenne des automates finis et des langages rationnels. *Thèse de doctorat*, Université Paris 7, 2000.

[51] J.-E. Pin, On reversible automata. In *Proc. 1st LATIN Conf., (I. Simon, Ed.), Lecture Notes in Comput. Sci.* **583** (1992), 401–416.

[52] J.-E. Pin, Variétés de langages formels. Masson, 1984. Traduction: *Varieties of formal languages* North Oxford Acad. Pub., 1986.

[53] G. Raney, Sequential functions. *J. Assoc. Comput. Mach.* **5** (1958) 177–180.

[54] J. Sakarovitch, A construction on automata that has remained hidden. *Theoret. Comput. Sci.* **204** (1998), 205–231.

[55] J. Sakarovitch, *Éléments de théorie des automates.* Vuibert, *à paraître.*

[56] A. Salomaa, *Jewels of formal language theory.* Computer Science Press, 1981.

[57] P.V. Silva, On free inverse monoid languages. *Theoret. Informatics and Appl.* **30** (1996), 349–378.

[58] I. Simon, Recognizable sets with multiplicities in the tropical semiring. *Proc. of MFCS'88, Lect. Notes in Comp. Sci.* **324** (1988), 107–120.

[59] I. Simon, The non deterministic complexity of a finite automaton. *Mots (M. Lothaire)*, Hermès (1990) 384–400.

[60] I. Simon, On semigroups of matrices over the tropical semiring. *R.A.I.R.O. Inf. Théorique*, (1994), 277–294.

[61] N.J.A. Sloane, *The On-Line Encyclopedia of Integer Sequences.* `http://www.research.att.com/~njas/sequences/`

[62] J.B. Stephen, Presentations of inverse monoids. *J. Pure Appl. Alg.* **63** (1990), 81–112.

[63] M. Szalay, On the maximal order in S_n and S_n^*. *Acta arithm.* **37** (1980), 321–331.