Available online at www.sciencedirect.com
ScienceDirect
Theoretical Computer Science 400 (2008) 144–158
Theoretical Computer Science
www.elsevier.com/locate/tcs

Extension of Brzozowski's derivation calculus of rational expressions to series over the free partially commutative monoids

Jean Berstel[a], Christophe Reutenauer[b,*]

[a] *Institut Gaspard-Monge (IGM), Université Paris-Est, France*
[b] *LaCIM Université du Québec Montréal, Canada*

Received 28 June 2007; received in revised form 27 January 2008; accepted 24 February 2008

Communicated by B. Durand

Abstract

We introduce an extension of the derivatives of rational expressions to expressions denoting formal power series over partially commuting variables. The expressions are purely noncommutative, however they denote partially commuting power series. The derivations (which are so-called ϕ-derivations) are shown to satisfy the commutation relations.

Our main result states that for every so-called rigid rational expression, there exists a stable finitely generated submodule containing it. Moreover, this submodule is generated by what we call Words, that is by products of letters and of pure stars.

Consequently this submodule is free and it follows that every rigid rational expression represents a recognizable series in $K\langle\langle A/C\rangle\rangle$. This generalizes the previously known property where the star was restricted to mono-alphabetic and connected series.

Keywords: Rational expressions; Free partially commutative; Recognizable

1. Introduction

Nerode's criterion asserts that a formal language L is regular if and only if the set of its "derivatives" $u^{-1}L$ is finite (where by definition $u^{-1}L$ is the set of words w such that uw is in L). This leads us to consider the operators $L \mapsto u^{-1}L$ defined on the set of all languages, each word u defining an operator.

In [4], Brzozowski has proved that these operators may be lifted on the level of rational expressions. This is done basically by using the three formulas (see [4], page 483): $a^{-1}(EF) = (a^{-1}E)F \cup (E, 1)(a^{-1}F)$, $a^{-1}(E^*) = (a^{-1}E)E^*$, and $(uv)^{-1}(E) = v^{-1}(u^{-1}E)$. Here a is a letter and $(E, 1) = 1$ if the empty word appears in the language represented by E and $= \emptyset$ otherwise. These formulas are a translation, on the level of expressions, of what happens for languages.

One of the observations of Brzozowski is that the set of derivatives of a given rational expression E is finite. In this way, he gives an elegant proof of one part of Kleene's theorem, namely that a rational set is recognizable.

* Corresponding author. Tel.: +1 514 987 3000.
E-mail address: Christophe.Reutenauer@uqam.ca (C. Reutenauer).

0304-3975/$ - see front matter
doi:10.1016/j.tcs.2008.02.051

These considerations can be generalized to recognizable series ("languages with multiplicities") over a semiring, assumed to be commutative (for basic notions concerning formal power series, the reader may consult [3]. A new edition of the book is in preparation, and an electronic version may be viewed at the first author's homepage). Indeed, it follows from the work of Carlyle and Paz [6], Inagaki et al. [12], Fliess [11], or Jacob [13] that a series $S = \sum_{w\in A^*}(S, w)w$ is recognizable if and only if there exists a finitely generated K-module of series containing S and which is *stable*, that is closed under the action of the operators

$$S \mapsto u^{-1}S = \sum_{w\in A*} (S, uw)w.$$

As above, this leads to an elegant proof of one part of the Kleene-Schützenberger theorem, using the formulas $a^{-1}(ST) = (a^{-1}S)T + (S, 1)a^{-1}T$ and $a^{-1}(S^*) = (a^{-1}S)S^*$, see for instance [3], Lemma 6.2 and the proof of Theorem 6.1.

The operators $S \mapsto u^{-1}S$ may also be lifted to rational expressions with coefficients in K, see [14], and an analogous result can be proved, namely that the derivatives of a rational expression are contained in a K-module of finite type of rational expressions.

In [11], Fliess works in the enlarged framework of partially commutative free monoids (instead of free monoids) with an additional stronger hypothesis on the semiring K: this semiring is required to be a principal ring (in particular K can be a field). He then obtains the following more precise result: the series S is recognizable if and only if the K-module generated by the $u^{-1}S$ (which are, in his interpretation, the columns of the Hankel matrix of S) is finitely generated.

This motivates to consider the following operators. Given a partially commutative free monoid $A^*/\mathcal{C}$, and $a \in A$, we denote by D_a the operator from $K\langle\langle A/\mathcal{C}\rangle\rangle$ into itself defined for $w \in A^*/\mathcal{C}$ as follows: $D_a(w) = 0$ except if w can be written in $A^*/\mathcal{C}$ in the form $w = av$, in which case $D_a(w) = v$. The operator D_a is then extended by (infinite) linearity to series in $K\langle\langle A/\mathcal{C}\rangle\rangle$. Note that these operators have been considered in [8] and [16] where it is proved that they are derivations in the partially commutative free *shuffle* algebra. For the usual product in $K\langle\langle A/\mathcal{C}\rangle\rangle$ we are interested in here it is not very difficult to see that D_a, although it is not a derivation, is a ϕ_a-derivation, that is D_a satisfies the equation

$$D_a(ST) = D_a(S)T + \phi_a(S)T,$$

where $\phi_a(S)$ is obtained by mapping onto 0 the letter a and all letters which do not commute with a. This formula is easily verified on elements of $A^*/\mathcal{C}$ and then is extended to series by linearity.

There is also a formula for the star of a series, namely

$$D_a(S^*) = \phi_a(S^*)\, D_a(S)\, S^*.$$

Indeed, $S^* = \sum_{n\geq 0} S^n = 1 + SS^*$, and using the identities $D_a\phi_a = 0$ and $\phi_a^2 = \phi_a$

$$\begin{aligned} D_a(S^*) &= D_a(S)S^* + \phi_a(S)D_a(S^*) \\ &= D_a(S)S^* + \phi_a(S)(D_a(S)S^* + \phi_a(S)D_a(S^*)) \\ &= \dots \\ &= (1 + \phi_a(S) + \cdots + \phi_a(S)^n)D_a(S)S^* + \phi_a(S)^{n+1}D_a(S^*) \end{aligned}$$

which yields the formula by taking the limit, since S is assumed to have 0 constant term.

With these tools, the theorem of Fliess may be rephrased as follows: K being a principal ring, a series S in $K\langle\langle A/\mathcal{C}\rangle\rangle$ is recognizable if and only if the smallest K-module containing S and which is stable (that is closed for the D_a) is finitely generated.

In view of extending the result of Brzozowski to free partially commutative monoids, even in the case of arbitrary semirings, we show that the operations D_a may be lifted to rational expressions. We take the latter *noncommutative*.

This may seem surprising since we require no commutation on letters. However, it appears that the monoid generated by the D_a itself satisfies the underlying commutations, that is, it is isomorphic to $A^*/\mathcal{C}$.

Our main result states that for every *rigid* rational expression, there exists a stable submodule of finite type containing it. Moreover, this submodule is generated by what we call Words, that is by products of letters and of pure stars.

Consequently this submodule is free and it follows that every rigid rational expression represents a recognizable series in $K\langle\langle A/\mathcal{C}\rangle\rangle$. The converse also holds, and we obtain it as a consequence of the theorem of Droste–Gastin [7]. Thus recognizable series in $K\langle\langle A/\mathcal{C}\rangle\rangle$ are completely characterized by the fact that they admit a rigid rational expression.

Note that the property of the previous submodule to be free is essential to obtain the recognizability. The freeness follows from the generation by Words, and there are only finitely many of them which appear when one iteratively derivates a rational expression. This latter property is the analogue, in our approach, to the finiteness of "partial derivatives" of [1], see also [15].

Derivations, as considered here, appear at several places in the literature. First, usual left derivations in context-free grammars can be viewed as ϕ-derivations. Wechler [17] has used ϕ-derivations in his characterization of context-free formal power series, see also [2]. A more combinatorial use has been made by Dulucq in [10] and in his thesis [9].

In order to keep formulas simple to read, we write indistinctly $f(x)$ or fx for the value of a function f on the argument x.

2. Rational expressions

In this section, we recall the definition of rational expressions and sets of alphabets. Since we are not considering parsing of expressions, rational expressions are not viewed as syntax trees, but already modulo associativity and commutativity.

Rational expressions. Let K be a commutative semiring and let A be an alphabet. We define the semiring, denoted $\mathcal{E}$, of *rational expressions on A over K*. This semiring is the union of an increasing sequence of subsemirings $\mathcal{E}_n$ for $n \geq 0$. Each such subsemiring is of the form $\mathcal{E}_n = K\langle A_n\rangle$ for some (in general infinite) alphabet A_n; moreover, there is a semiring morphism $E \mapsto (E, 1)$ from $\mathcal{E}_n$ to K; the element $(E, 1)$ is the *constant term* of the rational expression E. Finally, we denote by $\mathcal{H}_n$ the set of elements $E \in \mathcal{E}_n$ with $E \neq 0$ and constant term $(E, 1) = 0$.

Now $A_0 = A$, $\mathcal{E}_0 = K\langle A\rangle$ and the constant term is the usual constant term. Suppose that we have defined A_{n-1}, $\mathcal{E}_{n-1} = K\langle A_{n-1}\rangle$, the constant term function on $\mathcal{E}_{n-1}$ and $\mathcal{H}_{n-1}$ for $n \geq 1$. Then

$$A_n = A_{n-1} \cup \{E^* \mid E \in \mathcal{H}_{n-1}\}.$$

Here E^* is a formal expression, obtained from E by putting $*$ as exponent. Now

$$\mathcal{E}_n = K\langle A_n\rangle.$$

Observe that $\mathcal{E}_{n-1} = K\langle A_{n-1}\rangle$ is a subsemiring of $\mathcal{E}_n$. The constant term function is obtained as follows: it is already defined on A_{n-1} (since $A_{n-1} \subset \mathcal{E}_{n-1}$), and we extend it to all of A_n by setting $(E^*, 1) = 1$ for $E \in \mathcal{H}_{n-1}$; now it is extended uniquely to a semiring morphism $\mathcal{E}_n : K\langle A_n\rangle \to K$ which is the identity on K.

We write $\mathcal{H} = \{E \mid E \in \mathcal{E} \setminus 0, (E, 1) = 0\}$.

Example. Let $A = \{a, b\}$. Then $ab \in \mathcal{E}_0$, $(ab)^* \in A_1$ and $1 + b(ab)^*a \in \mathcal{E}_1$. Next, since $a \in A_0$, one gets $a^* \in A_1$, $a^*b \in \mathcal{H}_1$, $(a^*b)^* \in A_2$, $(a^*b)^*a^* \in \mathcal{E}_2$. The constant term of $1 + b(ab)^*a$ is 1, and this holds also for $(a^*b)^*a^*$.

Let $\underline{A} = \cup_{n\geq 0} A_n$. It follows from the definition of $\mathcal{E}$ that $\mathcal{E} = K\langle\underline{A}\rangle$. In other words, each rational expression is uniquely a K-linear combination of products of elements of $\underline{A}$: we call *Word* such a product and *Letter* an element of $\underline{A}$ (we use initial capitals in order to emphasize the difference with words as elements of A^* and letters as elements of A). Note that a Letter is either a letter or a *pure star*, that is of the form E^* with E in $\mathcal{H}$. Hence each rational expression E is uniquely a K-linear combination of Words, that is of expressions of the form

$$E_1 \cdots E_k, \tag{1}$$

where E_i is either in A or is a pure star, and $k \geq 0$. The *Support* of E is the set of Words having nonzero coefficient in E. It is convenient to put $0^* = 1$. We therefore have a partial function $E \to E^*$ on $\mathcal{E}$, whose domain is the set of rational expressions E with $(E, 1) = 0$, that is $\mathcal{H} \cup \{0\}$.

Alphabet set of a rational expression. As usual, the *alphabet* of a word w in A^* is the set $\mathrm{alph}(w)$ of letters actually occurring in w. We now define recursively the *alphabet set* $\mathrm{Alph}(E)$ of a rational expression E.

If $E \in \mathcal{E}_0 = K\langle A\rangle$, then

$$\mathrm{Alph}(E) = \{\mathrm{alph}(w) \mid w \in \mathrm{supp}(E)\},$$

where $\mathrm{supp}(E)$ is as usual the set of words having nonzero coefficient in E (again we use initial capitals to distinguish supports from Supports). Note that $\mathrm{Alph}(0) = \emptyset$ and $\mathrm{Alph}(1) = \{\emptyset\}$. Now let $n \geq 1$. If $E \in A_n$, then either $E \in A_{n-1}$ and $\mathrm{Alph}(E)$ is already defined, or $E = H^*$ is a pure star. Then

$$\mathrm{Alph}(E) = \{B_1 \cup \cdots \cup B_k \mid k \geq 0,\ B_i \in \mathrm{Alph}(H)\}.$$

Finally, if E is a K-linear combination of distinct Words of the form (1), with nonzero coefficients, then $\mathrm{Alph}(E)$ is the union of the corresponding sets

$$\mathrm{Alph}(E_1 \cdots E_n) = \{B_1 \cup \cdots \cup B_n \mid B_i \in \mathrm{Alph}(E_i)\}.$$

Lemma 1. *For $E, F \in \mathcal{E}$, one has* $\mathrm{Alph}(EF) \subset \{B \cup C \mid B \in \mathrm{Alph}(E),\ C \in \mathrm{Alph}(F)\}$, $\mathrm{Alph}(E + F) \subset \mathrm{Alph}(E) \cup \mathrm{Alph}(F)$.

Proof. Both inclusions follow from the definition and from the observation that the Support of EF (resp. of $E + F$) is contained in the product (resp. the union) of the Support of E and that of F. □

Verbal submodules. A K-submodule of $\mathcal{E}$ is called *verbal* if it is generated by Words. Such a submodule is necessarily free, having as a basis over K the set of Words that it contains. Note that if a verbal submodule is finitely generated, then it is finitely generated by Words, hence it is a finitely generated free submodule.

Remark. Let us remark that in the case where the semiring K is positive, then

$$\mathrm{Alph}(E) = \{\mathrm{alph}(w) \mid w \in \mathrm{supp}(\mathrm{eval}(E))\},$$

where the evaluation function is the natural mapping into formal power series.

For general semirings, one may associate naturally to the expression E an expression E' over the Boolean semiring by replacing each nonnull coefficient by 1. Then

$$\mathrm{Alph}(E) = \{\mathrm{alph}(w) \mid w \in \mathrm{supp}(\mathrm{eval}(E'))\}.$$

3. Derivations

We introduce ϕ-derivations. In a first step, they are defined on polynomials, and then they are extended to rational expressions.

3.1. Derivations of polynomials

Let L be a semiring containing K in its center, and let ϕ be a semiring endomorphism of L. A *ϕ-derivation* of L is a K-linear endomorphism D of L such that for any $x, y \in L$

$$D(xy) = D(x)y + \phi(x)D(y),$$

and moreover $D(1) = 0$.

Lemma 2. *Let ϕ be an endomorphism of the K-algebra $K\langle A\rangle$. Then each mapping $D : A \to K\langle A\rangle$ has a unique extension to a ϕ-derivation of $K\langle A\rangle$.*

Proof. Recall that $K\langle A\rangle$ is the free associative K-algebra generated by A. In other words, each mapping μ from A into a K-algebra L has a unique extension to a K-algebra homomorphism $\bar{\mu} : K\langle A\rangle \to L$.

Given $D : A \to K\langle A\rangle$, we take for L the K-algebra $K\langle A\rangle^{2\times 2}$ and for μ the mapping $\mu(a) = \begin{pmatrix} a & 0 \\ Da & \phi a \end{pmatrix}$. The details are left to the reader. □

A useful identity is the following. Let $x_1, \ldots, x_n$ be in L and let D be a ϕ-derivation. Then

$$D(x_1 \cdots x_n) = \sum_{i=1}^{n} \phi(x_1 \cdots x_{i-1}) D(x_i) x_{i+1} \cdots x_n, \tag{2}$$

where as usually an empty product has to be interpreted as 1.

Commutation graph and associated ϕ-derivations. Let $\mathcal{C}$ be a finite undirected graph (without loops and multiple edges) called the *commutation graph*. Let A be its set of vertices. For $a \in A$, we denote by $\mathcal{C}(a)$ the set of neighbours in $\mathcal{C}$ of a. Thus $b \in \mathcal{C}(a)$ if and only if (a, b) is an edge in $\mathcal{C}$. Observe that $a \notin \mathcal{C}(a)$.

For $a \in A$, we define the K-algebra endomorphism $\phi_a : K\langle A\rangle \to K\langle A\rangle$ to be the projection onto $k\langle \mathcal{C}(a)\rangle$, that is, for $b \in A$,

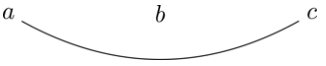
$$\phi_a(b) = \begin{cases} b & \text{if } b \in \mathcal{C}(a) \\ 0 & \text{if } b \notin \mathcal{C}(a) \end{cases}$$

Note that $\phi_a(a) = 0$. Now, we define the ϕ_a-derivation D_a of $K\langle A\rangle$ by

$$D_a(a) = 1 \text{ and } D_a(b) = 0 \text{ if } b \neq a.$$

This ϕ_a-derivation exists by Lemma 2. By Equation (2) applied to a product of letters, we see that D_a has the following combinatorial definition: for any word w in A^*, $D_a(w) = 0$ except if w has a factorization $w = uav$, with $u \in \mathcal{C}(a)^*$, and in this case $D_a(w) = uv$.

In the whole paper, we use the following running example. We take as graph $\mathcal{C}$ the graph



Thus $\mathcal{C}(a) = \{c\}, \mathcal{C}(b) = \emptyset, \mathcal{C}(c) = \{a\}$. Consequently, $\phi_a(w) = 0$ except if $w \in c^*$, in which case $\phi_a(w) = w$. A similar property holds for ϕ_c. Finally, $\phi_b(w) = 0$ except if w is the empty word, in which case $\phi_b(w) = w$.

We therefore have $D_a(c^n au) = c^n u$ and $D_a(w) = 0$ if w is not of this form. A similar property holds for D_c. Finally, $D_b(w) = 0$ except if $w = bu$ and then $D_b(w) = u$.

Commutation of the D_a. It is clear that the endomorphisms ϕ_a commute each to another.

Lemma 3. *Let (a, b) be an edge of $\mathcal{C}$. Then ϕ_a and D_b commute, and D_a and D_b commute.*

Proof. 1. First $\phi_a D_b(1) = 0 = D_b\phi_a(1)$. Next, if c is a letter distinct from b, then $\phi_a D_b(c) = 0$ and $D_b\phi_a(c) = D_b(c)$ or $= D_b(0)$ which evaluates to 0 in both cases. Furthermore, $\phi_a D_b(b) = \phi_a(1) = 1$ and $D_b\phi_a(b) = D_b(b) = 1$.

Let w be a word of length ≥ 2 and write $w = uv$, with u, v of smaller length. Then

$$\begin{aligned} \phi_a D_b(uv) &= \phi_a(D_b(u)v + \phi_b(u)D_b(v)) \\ &= \phi_a D_b(u)\phi_a(v) + \phi_a\phi_b(u)\phi_a D_b(v) \end{aligned}$$

and

$$\begin{aligned} D_b\phi_a(uv) &= D_b(\phi_a(u)\phi_a(v)) \\ &= D_b\phi_a(u)\phi_a(v) + \phi_b\phi_a(u)D_b\phi_a(v). \end{aligned}$$

Thus $\phi_a D_b(uv) = D_b\phi_a(uv)$, by induction and by the commutation of ϕ_a and ϕ_b.

2. It is enough to show that $D_a D_b$ and $D_b D_a$ coincide on words. So we may assume that K is a ring. We show that in this case the Lie bracket $E = D_a D_b - D_b D_a$ vanishes on the generators, and is a $\phi_a\phi_b$-derivation. Thus $E = 0$ by Lemma 2.

We check that $E(c) = 0$ for any letter c. This is easily verified for $c = a$, $c = b$ and for $c \neq a, b$, by using the fact that $D_x(1) = 0$ for each letter x.

We now show that, more generally, if ϕ and ψ are two commuting endomorphisms of a ring L (containing K in its center), and if D, E are a ϕ-derivation and a ψ-derivation respectively with $D\psi = \psi D$ and $E\phi = \phi E$, then $DE - ED$ is a $\phi\psi$-derivation.

Indeed,

$$\begin{aligned}(DE - ED)(xy) &= D(E(x)y + \psi(x)E(y)) - E(D(x)y + \phi(x)D(y)) \\ &= DE(x)y + \phi E(x)D(y) + D\psi(x)E(y) + \phi\psi(x)DE(y) \\ &\quad - ED(x)y - \psi D(x)E(y) - E\phi(x)D(y) - \psi\phi(x)ED(y) \\ &= (DE - ED)(x)y + \phi\psi(x)(DE - ED)(y)\end{aligned}$$

as was to be shown. □

Lemma 4. *If (a, b) is not an edge of $\mathcal{C}$, then $D_a\phi_b = 0$.*

Proof. This follows from the combinatorial definition of D_a, since $\phi_b(w)$ contains no occurrence of the letter a by hypothesis. □

Observe that in the lemma, ϕ_b and D_a do not commute, since $\phi_b D_a(a) = \phi_b(1) = 1$.

3.2. Derivations of rational expressions

Extension of ϕ_a and D_a to rational expressions. We first prove recursively that ϕ_a has an extension to each $\mathcal{E}_n$, and that $(E, 1) = (\phi_a E, 1)$ for any E in $\mathcal{E}_n$. This is clear if $n = 0$. Suppose $n \geq 1$ and let $E \in A_n$. If $E \in A_{n-1}$, then $\phi_a E$ is already defined and $(E, 1) = (\phi_a E, 1)$. Otherwise, $E = H^*$ for some $H \in \mathcal{H}_{n-1}$ and we define

$$\phi_a(E) = \phi_a(H)^*.$$

This is well defined since by induction $(\phi_a H, 1) = (H, 1) = 0$ and $\phi_a H \in \mathcal{E}_{n-1}$. Note that if $\phi_a H = 0$, then $\phi_a E = 1$ since by convention $0^* = 1$. Next, ϕ_a is extended uniquely to a K-algebra endomorphism of $\mathcal{E}_n = K\langle A_n\rangle$. Since $E \mapsto (E, 1)$ and $E \mapsto (\phi_a E, 1)$ are two homomorphisms $\mathcal{E}_n \to K$ which coincide on A_n, they are equal on $\mathcal{E}_n$. This proves the claim for ϕ_a.

Note that for any rational expression F such that F^* is defined, one has

$$\phi_a(F^*) = (\phi_a F)^*.$$

Thus, we may write $\phi_a F^*$ without ambiguity. Concerning D_a, we also proceed inductively. Let $E \in A_n$. If $E \in A_{n-1}$, then $D_a(E)$ is defined, and if $E = H^*$, then we put

$$D_a(E) = D_a(H^*) = \phi_a(H)^* \cdot D_a H \cdot H^*.$$

This defines D_a on A_n and we use now Lemma 2 to extend D_a to a ϕ_a-derivation on $\mathcal{E}_n = K\langle A_n\rangle$.

Commutation of the extensions.

Lemma 5. (i) *ϕ_a and ϕ_b commute on $\mathcal{E}$.*
(ii) *If (a, b) is an edge in $\mathcal{C}$, then ϕ_a and D_b commute, and D_a and D_b commute on $\mathcal{E}$.*

Proof. (i) Since ϕ_a, ϕ_b are K-algebra endomorphisms of $\mathcal{E}_n = K\langle A_n\rangle$, it is enough to show that they commute on A_n. This is true by definition for $n = 0$. Let $n \geq 1$. Let $E \in A_n$. If $E \in A_{n-1}$, then $\phi_a\phi_b E = \phi_b\phi_a E$ by induction. Otherwise $E = H^*$ for some $H \in \mathcal{H}_{n-1}$ and then

$$\phi_a\phi_b(E) = \phi_a\phi_b(H^*) = \phi_a(\phi_b(H)^*) = (\phi_a\phi_b(H))^*$$

and similarly $\phi_b\phi_a(E) = (\phi_b\phi_a(H))^*$. Since by induction $\phi_a\phi_b(H) = \phi_b\phi_a(H)$, the claim is proved.

(ii) By Lemma 3, $\phi_a D_b(E) = D_b\phi_a(E)$ for $E \in \mathcal{E}_0 = K\langle A\rangle$. Let $n \geq 1$. Suppose that ϕ_a and D_b commute on $\mathcal{E}_{n-1}$. Let $E \in A_n$. If $E \in A_{n-1}$, then $\phi_a D_b E = D_b\phi_a E$. Otherwise, $E = H^*$ for some $H \in \mathcal{H}_{n-1}$. Then

$$\phi_a D_b E = \phi_a(\phi_b H^* \cdot D_b H \cdot H^*) = \phi_a\phi_b H^* \cdot \phi_a D_b H \cdot \phi_a H^*$$

and

$$D_b\phi_a E = D_b(\phi_a H^*) = \phi_b\phi_a H^* \cdot D_b\phi_a H \cdot \phi_a H^*.$$

Hence, by induction and by (i), we have $\phi_a D_b E = D_b\phi_a E$. It follows by a computation already done in the proof of Lemma 3 that this formula holds for all E in $\mathcal{E}_n = K\langle A_n\rangle$.

We now consider D_a and D_b. By Lemma 3, they commute on $\mathcal{E}_0$. Let $n \geq 1$ and let $E \in A_n$. If $E \in A_{n-1}$, then D_a and D_b commute on E by induction. Otherwise $E = H^*$ for some $H \in \mathcal{H}_{n-1}$. Then, using (2),

$$\begin{aligned} D_a D_b E &= D_a(\phi_b H^* \cdot D_b H \cdot H^*) \\ &= D_a(\phi_b H^*) \cdot D_b H \cdot H^* + \phi_a \phi_b H^* \cdot D_a D_b H \cdot H^* \\ &\quad + \phi_a \phi_b H^* \cdot \phi_a D_b H \cdot D_a(H^*) \\ &= \phi_a \phi_b H^* \cdot D_a \phi_b H \cdot \phi_b H^* \cdot D_b H \cdot H^* + \phi_a \phi_b H^* \cdot D_a D_b H \cdot H^* \\ &\quad + \phi_a \phi_b H^* \cdot \phi_a D_b H \cdot \phi_a H^* \cdot D_a H \cdot H^*. \end{aligned}$$

Similarly, exchanging a and b,

$$\begin{aligned} D_b D_a E &= \phi_b \phi_a H^* \cdot D_b \phi_a H \cdot \phi_a H^* \cdot D_a H \cdot H^* \\ &\quad + \phi_b \phi_a H^* \cdot D_b D_a H \cdot H^* + \phi_b \phi_a H^* \cdot \phi_b D_a H \cdot \phi_b H^* \cdot D_b H \cdot H^* \end{aligned}$$

and we conclude that $D_a D_b E = D_b D_a E$ by induction on n and by the commutation rules that we have already established.

Now, in order to extend this latter formula to all of $\mathcal{E}_n = K\langle A_n \rangle$, it suffices to show that if it holds for E_1 and E_2, then it holds also for $E_1 E_2$. We have

$$\begin{aligned} D_a D_b(E_1 E_2) &= D_a(D_b E_1 \cdot E_2 + \phi_b E_1 \cdot D_b E_2) \\ &= D_a D_b E_1 \cdot E_2 + \phi_a D_b E_1 \cdot D_a E_2 + D_a \phi_b E_1 \cdot D_b E_2 \\ &\quad + \phi_a \phi_b E_1 \cdot D_a D_b E_2 \end{aligned}$$

and similarly

$$\begin{aligned} D_b D_a(E_1 E_2) &= D_b D_a E_1 \cdot E_2 + \phi_b D_a E_1 \cdot D_b E_2 + D_b \phi_a E_1 \cdot D_a E_2 \\ &\quad + \phi_b \phi_a E_1 \cdot D_b D_a E_2 \end{aligned}$$

and we may conclude. □

Lemma 6. *If (a, b) is not an edge of $\mathcal{C}$, then $D_a \phi_b = 0$.*

Proof. This holds on $\mathcal{E}_0$ by Lemma 4. Let $n \geq 1$. Let $E = H^*$ for some $H \in \mathcal{H}_{n-1}$ and assume by induction $D_a \phi_b H = 0$. Then

$$D_a(\phi_b(H)^*) = \phi_a \phi_b(H)^* \cdot D_a \phi_b H \cdot \phi_b(H)^* = 0.$$

Next

$$D_a \phi_b(E_1 E_2) = D_a(\phi_b E_1 \cdot \phi_b E_2) = D_a \phi_b E_1 \cdot \phi_b E_2 + \phi_a \phi_b E_1 \cdot D_a \phi_b E_2.$$

This formula shows that $D_a \phi_b = 0$ on $\mathcal{E}_n$. □

3.3. Free partially commutative monoid

Denote by $\sim_{\mathcal{C}}$ the congruence of the free monoid A^* generated by the relations $ab \sim_{\mathcal{C}} ba$ for each edge $(a, b) \in \mathcal{C}$. The monoid $A^*/\sim_{\mathcal{C}}$ or $A^*/\mathcal{C}$ for short is the *free partially commutative monoid* associated to $\mathcal{C}$. These have been introduced and studied in [5].

As we have seen, $ab \sim_{\mathcal{C}} ba$ implies $D_a D_b = D_b D_a$. Actually, there are no more relations among the D_a's.

Proposition 7. *The monoid generated by the mappings D_a, for $a \in A$, acting on $K\langle A \rangle$ (and a fortiori on $\mathcal{E}$), is isomorphic to the free partially commutative monoid $A^*/\mathcal{C}$.*

In fact, this result is only true when the mappings D_a are composed from left to right. Otherwise, "isomorphic" must be replaced by "anti-isomorphic" in the statement. For this reason, we write wD_a instead of $D_a w$ in the proof below (and only there), and we compose functions from left to right.

Proof. Write $D_u = D_{a_1} \cdots D_{a_n}$ if $u = a_1 \cdots a_n$ with $a_i \in A$. It suffices to show that the hypothesis $D_u = D_v$ implies $u \sim_{\mathcal{C}} v$. Using the combinatorial definition of D_v, we see that $vD_v = 1$. Thus $vD_u = 1$. Therefore, under

this hypothesis it is enough to show that $vD_u = 1$ implies $u \sim_{\mathcal{C}} v$. This in turn is done by induction on $|u|$. If $|u| = 0$, then $u = 1$ and D_u is the identity mapping. Thus $vD_u = v$ and $v = 1$. Next, if $|u| \geq 1$, write $u = aw$ with $a \in A$. Then $1 = vD_u = (vD_a)D_w$. By the combinatorial definition, there is a factorization $v = v_1 a v_2$ with $v_1 \in \mathcal{C}(a)^*$. Then $vD_a = v_1 v_2$ and consequently $1 = (v_1 v_2)D_w$. By induction, $w \sim_{\mathcal{C}} v_1 v_2$ and therefore $u = aw \sim_{\mathcal{C}} a v_1 v_2 \sim_{\mathcal{C}} v_1 a v_2 = v$. □

Remark. This result is related to, and extends Proposition 3.1 of [16]. It is proved there that, when K is a ring, the operators D_a on $K\langle A/\mathcal{C}\rangle$ (see the introduction) generate a Lie algebra which is isomorphic to the partially commutative free Lie algebra.

3.4. Words and sets of alphabets

Endomorphisms, Words, and sets of alphabets. The proofs of the following three lemmas are technical, but not really surprising.

Lemma 8. *Each endomorphism ϕ_a maps a Word onto a Word or* 0.

Proof. A Letter is either a letter or a pure star. The first is mapped by ϕ_a onto itself or 0, and the second is mapped onto a pure star or 1. The lemma follows. □

Lemma 9. *If $E \in \mathcal{E}$, then* $\mathrm{Alph}(\phi_a E) \subset \{B \in \mathrm{Alph}(E) \mid B \subset \mathcal{C}(a)\}$.

Proof. This is clear if $E \in \mathcal{E}_0 = K\langle A\rangle$ since ϕ_a maps each word w onto 0 except if $w \in \mathcal{C}(a)^*$, and in this case $\phi_a(w) = w$.

If $n \geq 1$, let $E = H^*$ with $H \in \mathcal{H}_{n-1}$. Arguing by induction, the result holds for H. Observe that $\phi_a(E) = \phi_a(H)^*$. Next, for any B in $\mathrm{Alph}(\phi_a(E))$, one has $B = B_1 \cup \cdots \cup B_k$ for some $k \geq 0$ and $B_i \in \mathrm{Alph}(\phi_a H)$. By induction, $B_i \in \mathrm{Alph}(H)$ and $B_i \subset \mathcal{C}(a)$. Hence $B \in \mathrm{Alph}(H^*) = \mathrm{Alph}(E)$ and $B \subset \mathcal{C}(a)$, what was to be shown.

Now, if E is a Word of the form (1), then $\phi_a(E) = \phi_a E_1 \cdots \phi_a E_n$. If $\phi_a(E) \neq 0$, let $B \in \mathrm{Alph}(\phi_a(E))$; then by Lemma 1, $B = B_1 \cup \cdots \cup B_k$ with $B_i \subset \mathrm{Alph}(\phi_a E_i)$. Hence $B_i \in \mathrm{Alph}(E_i)$ and $B_i \subset \mathcal{C}(a)$ by the previous arguments. Thus $B \in \mathrm{Alph}(E)$ and $B \subset \mathcal{C}(a)$.

Finally, let E be a linear combination of Words of the form (1), with nonzero coefficients. We conclude by the previous argument and Lemma 1. □

Remark. We do not have equality in the lemma. In our running example and for $E = (a + c)^* - (b + c)^*$, one has $\mathrm{Alph}(E) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, c\}, \{b, c\}\}$, and $\phi_a(E) = 0$, and therefore $\mathrm{Alph}(\phi_a(E)) = \emptyset$. However, $\{B \in \mathrm{Alph}(E) \mid B \subset \mathcal{C}(a)\}$ is equal to $\{\emptyset, \{c\}\}$.

ϕ-derivations and sets of alphabets.

Lemma 10. *For any $B \in \mathrm{Alph}(D_a E)$, one has $B \cup \{a\} \in \mathrm{Alph}(E)$.*

Proof. If $E \in \mathcal{E}_0 = K\langle A\rangle$, then there is some w in $\mathrm{supp}(D_a E)$ such that $B = \mathrm{alph}(w)$. By the combinatorial interpretation of D_a, there is a factorization $w = w_1 w_2$ such that $w_1 a w_2 \in \mathrm{supp}(E)$. Hence $B \cup \{a\} \in \mathrm{Alph}(E)$.

Suppose that the lemma is proved for $E \in \mathcal{E}_{n-1}$ and $n \geq 1$. Let $E \in \mathcal{E}_n$. Suppose first that $E = H^*$ with $H \in \mathcal{H}_{n-1}$. Then $D_a(H^*) = (\phi_a H)^* \cdot D_a H \cdot H^*$. By Lemma 1, there exist $B_1 \in \mathrm{Alph}(\phi_a H^*)$, $B_2 \in \mathrm{Alph}(D_a H)$, $B_3 \in \mathrm{Alph}(H^*)$ such that $B = B_1 \cup B_2 \cup B_3$. By induction, $B_2 \cup \{a\} \in \mathrm{Alph}(H)$. Now $\mathrm{Alph}(H^*)$ contains $\mathrm{Alph}(H)$ and is closed under union. Moreover by Lemma 9, $\mathrm{Alph}(\phi_a H^*) \subset \mathrm{Alph}(H^*)$. Hence $B \cup \{a\} \in \mathrm{Alph}(E)$. This proves the result for $E \in A_n$.

Now let E be a linear combination with nonzero coefficients of Words of the form (1). Then by (2) $D_a E$ is the corresponding linear combination of the elements

$$D_a E_1 \cdot E_2 \cdots E_n + \phi_a E_1 \cdot D_a E_2 \cdot E_3 \cdots E_n + \cdots + \phi_a(E_1 \cdots E_{n-1}) \cdot D_a E_n.$$

Since $B \in \mathrm{Alph}(D_a E)$, we have $B \in \mathrm{Alph}(\phi_a(E_1 \cdots E_{i-1}) \cdot D_a E_i \cdot (E_{i+1} \cdots E_n))$ for some i by Lemma 1. By the same lemma, we get a decomposition $B = B_1 \cup B_2 \cup B_3$ with $B_1 \in \mathrm{Alph}(\phi_a(E_1 \cdots E_{i-1}))$, $B_2 \in \mathrm{Alph}(D_a E_i)$, $B_3 \in \mathrm{Alph}(E_{i+1} \cdots E_n)$. By induction and the previous case, we have $B_2 \cup \{a\} \in \mathrm{Alph}(E_i)$ and in view of Lemma 9, $B_1 \in \mathrm{Alph}(E_1 \cdots E_{i-1})$. Since each E_i is a Letter, this implies that $B \cup \{a\} \in \mathrm{Alph}(E)$. □

4. Rigid rational expressions

This section contains the main result. We introduce the notion of a rigid expression and we prove that a rigid rational expression is contained in some finitely generated stable and verbal submodule of $\mathcal{E}$.

Rigid rational expressions. We define a subsemiring $\mathcal{E}'$ of $\mathcal{E}$ composed of *rigid* expressions (we don't use the word "connected" which may be misleading). For this, let $\bar{\mathcal{C}}$ be the complementary graph of $\mathcal{C}$. $\bar{\mathcal{C}}$ will be called the *non-commutation* graph. A pair (a, b) is an edge in $\bar{\mathcal{C}}$ if and only if (a, b) is not an edge in $\mathcal{C}$. A subset B of A (the set of vertices of $\mathcal{C}$) is *connected* if the subgraph $\bar{\mathcal{C}}|B$ is connected. In our running example, the connected subalphabets are all subsets of $\{a, b, c\}$ except $\{a, c\}$.

Let $E \in \mathcal{H}$ be a nonzero rational expression with $(E, 1) = 0$. We say that E^* is *rigid* if each B in $\mathrm{Alph}(E^*)$ is connected. Intuitively, $\mathcal{E}'$ is the set of all rational expressions involving only rigid stars. More formally, $\mathcal{E}'$ is the union of a chain of subsemirings $\mathcal{E}'_n$ defined recursively by $\mathcal{E}'_0 = \mathcal{E}_0 = K\langle A\rangle$ and $A'_0 = A$, and for $n \geq 1$, by

$$A'_n = A'_{n-1} \cup \{E^* \mid E \in \mathcal{E}'_{n-1}, E \in \mathcal{H}, \text{ and } E^* \text{ rigid }\}$$

and $\mathcal{E}'_n = K\langle A'_n\rangle$. It is convenient to set $\mathcal{H}'_n = \mathcal{E}'_n \cap \mathcal{H}$.

In our running example, $(ab + c)^*$ is a rigid rational expression, whereas $(ac)^*$, $(a + c)^*$ and $(b(ac)^*)^*$ are not rigid. The outer star in the last rational expression is rigid, but not the inner.

For sake of coherence, note that $\phi_a\mathcal{E}' \subset \mathcal{E}'$ and $D_a\mathcal{E}' \subset \mathcal{E}'$. This is proved inductively. We have clearly $\phi_a\mathcal{E}'_0 \subset \mathcal{E}'_0$ and $D_a\mathcal{E}'_0 \subset \mathcal{E}'_0$. For $n \geq 1$, and $E \in A'_n$, let $H \in \mathcal{H}'_{n-1}$ such that $E = H^*$. Then $\phi_a E = (\phi_a H)^*$. By Lemma 9, $\mathrm{Alph}(\phi_a H^*) \subset \mathrm{Alph}(H^*)$, showing that $\phi_a H^*$ is a rigid star and thus $\phi_a E \in \mathcal{E}'_n$. Moreover, $D_a E = \phi_a H^* \cdot D_a H \cdot H^*$. Then $\phi_a H^*$, $H^* \in \mathcal{E}'_n$ and $D_a H \in \mathcal{E}'_{n-1}$ by induction. Hence $D_a E \in \mathcal{E}'_n$. This proves the inclusions $\phi_a\mathcal{E}'_n \subset \mathcal{E}'_n$ and $D_a\mathcal{E}'_n \subset \mathcal{E}'_n$.

We say that a subset M of $\mathcal{E}$ is *stable* if $D_a M \subset M$ for all $a \in A$.

Theorem 11. *Let E be a rigid rational expression. Then there exists a finitely generated stable and verbal submodule of $\mathcal{E}$ containing E.*

From the algorithmic and computational point of view, this result may be rephrased as follows.

Corollary 12. *Let E be a rigid rational expression. Take the Words appearing in E, derivate them with respect to all D_a, and iterate. Then the set of Words obtained in this way is finite.*

Proof. This is because if E belongs to a verbal submodule, then all Words appearing in E belong to this submodule. □

Examples and counterexamples. Before going into the proof, here are some examples.

1. $E = (ab + c)^*$. Then there are the following derivations:

$$D_a E = \phi_a(E) D_a(ab + c)E = c^* bE := F, \text{ because } D_a(ab + c) = b.$$
$$D_b E = \phi_b(E) D_b(ab + c)E = 0, \text{ because } D_b(ab + c) = 0.$$
$$D_c E = \phi_c(E) D_c(ab + c)E = E, \text{ because } \phi_c(E) = 1 \text{ and } D_c(ab + c) = 1$$
$$D_a F = D_a(c^*)bE + \phi_a(c^*)D_a(b)E + \phi_a(c^*b)D_a(E) = 0$$
since $D_a(c^*) = \phi_a(c^*)D_a(c)c^* = 0$, $D_a(b) = 0$, $\phi_a(c^*b) = \phi_a(c^*)\phi_a(b) = 0$.
$$D_b F = D_b(c^*)bE + \phi_b(c^*)D_b(b)E + \phi_b(c^*b)D_b(E) = E$$
since $D_b(c^*) = 0$, $\phi_b(c^*) = \phi_b(c)^* = 0^* = 1$, $D_b(b) = 1$ and also $\phi_b(c^*b)$
$= \phi_b(c^*)\phi_b(b) = 0$.
$$D_c F = D_c(c^*)bE + \phi_c(c^*)D_c(b)E + \phi_c(c^*b)D_c(E) = F$$
since $D_c(c^*) = \phi_c(c^*)D_c(c)c^* = c^*$, $D_c(b) = 0$, $\phi_c(c^*b) = \phi_c(c^*)\phi_c(b) = 0$.

Thus E is contained in the stable submodule spanned by the two Words E and F.

2. Let $E = (ac)^*$ which is not rigid. Then

$$D_a((ac)^*) = \phi_a(ac)^* D_a(ac)(ac)^* = 0^* c(ac)^* = c(ac)^*.$$

Moreover,

$$D_a^2(ac)^* = D_a(c)(ac)^* + \phi_a(c)D_a(ac)^* = cD_a(ac)^* = c^2(ac)^*.$$

Inductively, $D_a^n(ac)^* = c^n(ac)^*$. Hence there is no finitely spanned stable and verbal submodule containing E, since the Words $c^n(ac)^*$ have unbounded length.

3. Let $E = (a + c)^*$ a nonrigid rational expression. Then a straightforward inductive computation shows that $D_a^n E = (c^*)^n E$ and we conclude as in the previous example.

4. $E = (b(ac)^*)^*$ is a nonrigid expression. One shows easily that $D_a^n D_b E = c^n(ac)^* E$ which allows us to conclude as before.

The Appendix contains a larger example.

Proof of the main result.

Lemma 13. *Let $\mathcal{W}$ be a set of Words spanning a stable submodule. Let $\mathcal{W}'$ be the closure of $\mathcal{W}$ under the ϕ_a for $a \in A$. Then $\mathcal{W}'$ spans a stable submodule. Moreover, if $\mathcal{W}$ is finite, then $\mathcal{W}'$ is finite.*

Proof. Each nonzero element in $\mathcal{W}'$ is a Word, by Lemma 8. Such a Word is of the form $\phi_1 \cdots \phi_n W$, where $W \in \mathcal{W}$ and $\phi_1, \ldots, \phi_n \in \{\phi_a \mid a \in A\}$. It suffices to show that $D_a\phi_i = \phi_i D_a$ or $D_a\phi_i = 0$, for each i. But this follows from Lemmas 5 and 6.

The last assertion follows from the fact that the ϕ_a are idempotent and commute. □

Proof of Theorem. 1. If $E \in \mathcal{E}'_0 = K\langle A\rangle$, we take for M the K-submodule spanned by all words appearing in E and their successive derivatives.

2. Now, let $n \geq 1$ and $E = H^*$. By induction, there is a finite set $\mathcal{W}$ of Words such that the K-submodule they span contains H and is closed under all D_a. By Lemma 13, we may assume that this submodule is closed under all ϕ_a. Hence, if $W \in \mathcal{W}$, then $\phi_a W \in \mathcal{W}$ or $\phi_a W = 0$.

3. Consider the set of all Words of the form

$$\phi_{B_k} H^* \cdot E_k \cdots \phi_{B_2} H^* \cdot E_2 \cdot \phi_{B_1} H^* \cdot E_1 \cdot \phi_{B_0} H^*, \tag{3}$$

where $k \geq 0$ and where there is a k-tuple $(A_k, \ldots, A_1)$ of *nonempty* subalphabets such that

- $B_i = A_1 \cup \cdots \cup A_i$ for $i = 0, \ldots, k$;
- $E_i \in \mathcal{W}$;
- $E_i = \phi_{B_{i-1}} E_i$ for $i = 1, \ldots, k$;
- $B \in \mathrm{Alph}(E_i)$ implies $B \cup A_i \in \mathrm{Alph}(H)$, for $i = 1, \ldots, k$.

Here we use the notation ϕ_B for

$$\phi_B = \prod_{b \in B} \phi_b.$$

Observe that $B_0 = \emptyset$ and $\phi_\emptyset = \mathrm{id}$.

4. We show that the set of expressions (3) is finite. It is enough to show that, under the hypothesis $B_{i-1} = B_i$, one has $E_i = 1 = \phi_{B_i} H^*$. Under this hypothesis, let $B \in \mathrm{Alph}(E_i)$. Note that such a B exists since E_i s a Word. Since $E_i = \phi_{B_{i-1}} E_i$, we have for any $a \in B_{i-1}$, $\phi_a E_i = \phi_a \phi_{B_{i-1}} E_i = \phi_{B_{i-1}} E_i = E_i$, hence by Lemma 9, $B \subset \mathcal{C}(a)$. Thus

$$B \subset \bigcap_{a \in B_{i-1}} \mathcal{C}(a) = \bigcap_{a \in B_i} \mathcal{C}(a) \subset \bigcap_{a \in A_i} \mathcal{C}(a).$$

Thus, if $B \neq \emptyset$, $B \cup A_i$ is not connected. But $B \cup A_i \in \mathrm{Alph}(H) \subset \mathrm{Alph}(H^*)$ and H^* is rigid. Hence $B = \emptyset$.

This shows simultaneously that $\mathrm{Alph}(E_i) = \{\emptyset\}$, hence $E_i = 1$ and that $A_i \in \mathrm{Alph}(H)$. By Lemma 9, if $B \in \mathrm{Alph}(\phi_{B_i} H^*)$, then

$$B \subset \bigcap_{a \in B_i} \mathcal{C}(a) \subset \bigcap_{a \in A_i} \mathcal{C}(a),$$

hence $B \cup A_i$ is not connected, except if B is empty. Since, by Lemma 9, $B \in \mathrm{Alph}(H^*)$ and since the latter is closed under union, we get $B \cup A_i \in \mathrm{Alph}(H^*)$. But H^* is rigid, hence $B = \emptyset$. Thus $\mathrm{Alph}(\phi_{B_i} H^*) = \{\emptyset\}$ and $\phi_{B_i} H^* = 1$ since $\phi_{B_i} H^*$ is a Word.

5. The expressions (3) are Words. Hence the submodule they span is verbal. It contains H^* (for $k = 0$). We now show that M is stable. If we apply the derivation D_a to (3) then, using (2), the result is a sum of terms of the form

$$\phi_a \phi_{B_k} H^* \cdot \phi_a E_k \cdots \phi_a E_{i+1} \cdot D_a \phi_{B_i} H^* \cdot E_i \cdot \phi_{B_{i-1}} H^* \cdots \phi_{B_0} H^* \tag{4}$$

for some $i = 0, \ldots, k$, or of the form

$$\phi_a \phi_{B_k} H^* \cdots \phi_a \phi_{B_i} H^* \cdot D_a E_i \cdot \phi_{B_{i-1}} H^* \cdots \phi_{B_0} H^* \tag{5}$$

for some $i = 1, \ldots, k$.

6. Consider a nonzero term of the form (4) (some $\phi_a E_j$ may be zero, and we discard the corresponding terms). We have

$$D_a \phi_{B_i} H^* = \phi_a \phi_{B_i} H^* \cdot D_a \phi_{B_i} H \cdot \phi_{B_i} H^*.$$

Moreover,

$$D_a \phi_{B_i} H = \sum_W \alpha_W W,$$

where the sum is over elements those W in $\mathcal{W}$ for which $\alpha_W \in K \setminus \{0\}$. By Lemmas 5 and 6, $\phi_{B_i} D_a \phi_{B_i} H = D_a \phi_{B_i} H$. Indeed, $D_a \phi_{B_i} H$ is either 0 or equal to $\phi_{B_i} D_a H$, and ϕ_{B_i} is idempotent. Thus

$$\sum \alpha_W W = \sum \alpha_W \phi_{B_i}(W),$$

and this shows, by the linear independence of $\mathcal{W}$, that $W = \phi_{B_i}(W)$ for any W appearing in the linear combination. If moreover $B \in \mathrm{Alph}(W)$, then $B \in \mathrm{Alph}(D_a \phi_{B_i} H)$ because $\alpha_W \neq 0$. Then by Lemma 9, and by Lemma 10

$$B \cup \{a\} \in \mathrm{Alph}(\phi_{B_i} H) \subset \mathrm{Alph}(H).$$

This shows that (4) is a linear combination of terms

$$\phi_a \phi_{B_k} H^* \cdot \phi_a E_k \cdots \phi_a E_{i+1} \cdot \phi_a \phi_{B_i} H^* \cdot W \cdot \phi_{B_i} H^* \cdot E_i \cdot \phi_{B_{i-1}} H^* \cdots \phi_{B_0} H^*$$

and that each of these terms is of the form (3), associated to the $(k+1)$-tuple of nonempty subalphabets $(A_k, \ldots, A_{i+1}, \{a\}, A_i, \ldots, A_1)$. The verification of the four conditions is left to the reader: the third follows from the idempotency of ϕ_a and the fourth is a consequence of Lemma 9.

7. We now consider a nonzero term of the form (5). As before,

$$D_a E_i = \sum_W \alpha_W W,$$

with the same conditions on the summation. Then (5) is a linear combination of terms

$$\phi_a \phi_{B_k} H^* \cdots \phi_a \phi_{B_i} H^* \cdot W \cdot \phi_{B_{i-1}} H^* \cdots \phi_{B_0} H^*.$$

Now, since $\phi_{B_{i-1}} E_i = E_i$, we have $D_a E_i = D_a \phi_{B_{i-1}} E_i = 0$ or $= \phi_{B_{i-1}} D_a E_i$ by Lemmas 5 and 6, and therefore $\phi_{B_{i-1}} D_a E_i = D_a E_i$. This implies that $\phi_{B_{i-1}} W = W$ for any W in the linear combination. Thus the term above is of the form (3), associated to the k-tuple $(A_k, \ldots, A_{i+1}, A_i \cup \{a\}, A_{i-1}, \ldots, A_1)$. Indeed, if $B \in \mathrm{Alph}(W)$, then $B \in \mathrm{Alph}(D_a E_i)$, hence $B \cup \{a\} \in \mathrm{Alph}(E_i)$ by Lemma 10, and therefore $B \cup \{a\} \cup A_i \in \mathrm{Alph}(H)$. The verification of the other conditions is left to the reader.

8. To conclude the proof, we must show that if E_1, E_2 are rigid rational expressions, with corresponding stable and verbal submodules M_1, M_2, which are finitely generated and contain E_1, E_2, then there exist submodules for $E_1 + E_2$ and E_1E_2.

For the sum, one takes $M_1 + M_2$, which is a stable, verbal, finitely generated submodule containing $E_1 + E_2$. For the product, we may assume, as in the previous part, that M_1 is closed under each ϕ_a. Then we take $M = M_1M_2$. It is a verbal, finitely generated submodule and contains E_1E_2. It is also stable since $D_a(F_1F_2) = D_aF_1 \cdot F_2 + \phi_aF_1 \cdot D_aF_2$. □

5. Application to recognizable series

There are natural semiring morphisms from the semiring $\mathcal{E}$ of rational expressions onto the semiring of rational power series in $K\langle\langle A\rangle\rangle$ and onto the semiring of rational series in $K\langle\langle A/\mathcal{C}\rangle\rangle$. These two morphisms are denoted eval and $\mathrm{eval}_{\mathcal{C}}$. They commute with the star operation and with the constant term function. Moreover, $\pi \circ \mathrm{eval} = \mathrm{eval}_{\mathcal{C}}$, where π denotes the natural morphism $K\langle\langle A\rangle\rangle \to K\langle\langle A/\mathcal{C}\rangle\rangle$.

Proposition 14. *The image of the semiring $\mathcal{E}'$ of rigid rational expressions under* $\mathrm{eval}_{\mathcal{C}}$ *is the semiring of recognizable series in $K\langle\langle A/\mathcal{C}\rangle\rangle$.*

Lemma 15. *Let M be a finitely generated free K-module, with a right action on $A^*/\mathcal{C}$ by endomorphisms of M, denoted $m \cdot w$ ($m \in M$, $w \in A^*/\mathcal{C}$). Let ϕ be some K-linear function $M \to K$ and $m_0 \in M$. Then*

$$S = \sum_{w \in A^*/\mathcal{C}} \phi(m_0 \cdot w)w \in K\langle\langle A/\mathcal{C}\rangle\rangle$$

is recognizable.

Proof. Let $m_1, \ldots, m_n$ be a basis of M. For each $a \in A$ and $i \in \{1, \ldots, n\}$, there exists a matrix $\mu a \in K^{n\times n}$ such that

$$m_i \cdot a = \sum_{1 \le j \le n} (\mu a)_{ij} m_j.$$

If $a \sim_{\mathcal{C}} b$, then $m_i \cdot ab = m_i \cdot ba$. Now

$$m_i \cdot ab = \Big(\sum_j (\mu a)_{ij} m_j\Big) \cdot b = \sum_{j,k} (\mu a)_{ij}(\mu b)_{jk} m_k$$

and similarly for $m_i \cdot ba$. Thus we have

$$\sum_{j,k} (\mu a)_{ij}(\mu b)_{jk} m_k = \sum_{j,k} (\mu b)_{ij}(\mu a)_{jk} m_k.$$

Since the m_k are linearly independent, we conclude that for any i and k,

$$\sum_j (\mu a)_{ij}(\mu b)_{jk} = \sum_j (\mu b)_{ij}(\mu a)_{jk}.$$

Hence $\mu a \mu b = \mu b \mu a$.

Thus the mapping $\mu : A \to K^{n\times n}$ extends to a linear representation from $A^*/\mathcal{C}$ to $K^{n\times n}$. It is easily seen by induction (compare with Lemma I.1.2 in [3]) that for any i and any w in $A^*/\mathcal{C}$, one has

$$m_i \cdot w = \sum_j (\mu w)_{ij} m_j.$$

Let $m_0 = \sum_i \lambda_i m_i$ and $\gamma_j = \phi(m_j)$. Then classically

$$\begin{aligned}\phi(m_0 \cdot w) &= \phi\Big(\sum_i \lambda_i m_i \cdot w\Big) = \phi\Big(\sum_i \lambda_i \sum_j (\mu w)_{ij} m_j\Big)\\ &= \sum_{i,j} \lambda_i (\mu w)_{ij} \gamma_j = \lambda \mu w \gamma.\end{aligned}$$

Hence S is recognizable. □

Observe that the hypothesis of freeness is essential in order to obtain the commutations of the recognizing matrices.

For S in $K\langle\langle A/\mathcal{C}\rangle\rangle$ and $u \in A^*/\mathcal{C}$, define $S \circ u$ by

$$S \circ u = \sum_{w \in A^*/\mathcal{C}} (S, uw)w.$$

For $u = a \in A$, $S \circ a$ is the operation D_a seen in the Introduction. This defines by Proposition 7 a right action of $A^*/\mathcal{C}$ on $K\langle\langle A/\mathcal{C}\rangle\rangle$.

Lemma 16. *For E in $\mathcal{E}$, one has*

$$\mathrm{eval}_{\mathcal{C}}(E) \circ a = \mathrm{eval}_{\mathcal{C}}(D_a E).$$

Proof. If $E \in \mathcal{E}_0$, this formula reduces to $\pi(E) \circ a = \pi(D_a E)$. It is enough to verify it when E is a word and in this case, it is simply a consequence of the definitions.

Suppose that the formula in the lemma holds in $\mathcal{E}_{n-1}$, $n \geq 1$. Define a mapping $\nu : K\langle\langle A/\mathcal{C}\rangle\rangle \to K\langle\langle A/\mathcal{C}\rangle\rangle^{2\times 2}$ by

$$\nu(S) = \begin{pmatrix} S & 0 \\ S \circ a & \phi_a S \end{pmatrix},$$

where we still denote by ϕ_a the morphism that maps the letters $b \in \mathcal{C}(a)$ onto themselves, and the other letters onto 0. Note that $\phi_a \,\mathrm{eval}_{\mathcal{C}} = \mathrm{eval}_{\mathcal{C}}\,\phi_a$. This is a semiring morphism since, as seen in the Introduction, $ST \circ a = (S \circ a)T + (\phi_a S)(T \circ a)$. One has

$$(\nu \circ \mathrm{eval}_{\mathcal{C}})(E) = \begin{pmatrix} \mathrm{eval}_{\mathcal{C}}(E) & 0 \\ \mathrm{eval}_{\mathcal{C}}(E) \circ a & \phi_a(\mathrm{eval}_{\mathcal{C}}(E)) \end{pmatrix}$$

and moreover, if we put

$$\mu(E) = \begin{pmatrix} E & 0 \\ D_a E & \phi_a E \end{pmatrix}$$

then

$$(\mathrm{eval}_{\mathcal{C}} \circ \mu)(E) = \begin{pmatrix} \mathrm{eval}_{\mathcal{C}}(E) & 0 \\ \mathrm{eval}_{\mathcal{C}}(D_a E) & \mathrm{eval}_{\mathcal{C}}(\phi_a E) \end{pmatrix}.$$

Thus, it suffices to show that $\nu \circ \mathrm{eval}_{\mathcal{C}} = \mathrm{eval}_{\mathcal{C}} \circ \mu$, and since $\mathcal{E}_n = K\langle A_n\rangle$, it is enough to verify it on A_n and, arguing by induction, for $E = H^*$ with $H \in \mathcal{H}_{n-1}$. We check that in this case, both sides coincide.

Indeed, let $S = \mathrm{eval}_{\mathcal{C}}(H)$. Then

$$\mathrm{eval}_{\mathcal{C}}(E) \circ a = \mathrm{eval}_{\mathcal{C}}(H^*) \circ a = \mathrm{eval}_{\mathcal{C}}(H)^* \circ a = S^* \circ a = \phi_a(S^*)\,(S \circ a)\,S^*,$$

where the last equality has been proved in the Introduction. We have $\phi_a(S^*) = \phi_a(S)^* = (\phi_a \,\mathrm{eval}_{\mathcal{C}}(H))^* = (\mathrm{eval}_{\mathcal{C}}\,\phi_a(H))^*$, and by induction

$$\begin{aligned} \phi_a(S^*)\,(S \circ a)\,S^* &= \mathrm{eval}_{\mathcal{C}}\,\phi_a(H)^*\,\mathrm{eval}_{\mathcal{C}}(D_a H)\,\mathrm{eval}_{\mathcal{C}}(H^*) \\ &= \mathrm{eval}_{\mathcal{C}}(\phi_a(H)^*\,D_a H\,H^*) = \mathrm{eval}_{\mathcal{C}}(D_a E). \quad \square \end{aligned}$$

Proof of Proposition 14. Let E be a rigid rational expression. By the theorem, there is a finitely generated stable and verbal submodule M of $\mathcal{E}$ which contains E. For $F \in M$ and $a \in A$, we define $F \cdot a = D_a(F)$. This defines by Proposition 7 a right action of $A^*/\mathcal{C}$ on M. Let $\phi(F) = (F, 1)$. Then, by Lemma 15, the series $S = \sum_{w \in A^*/\mathcal{C}} \phi(E \cdot w)w$ is recognizable.

We have only to verify that $S = \mathrm{eval}_{\mathcal{C}}(E)$. Of course, the whole construction has been devised in order to have this equality. By Lemma 16, we have $\mathrm{eval}_{\mathcal{C}}(E) \circ w = \mathrm{eval}_{\mathcal{C}}(E \cdot w)$ for any $w \in A^*/\mathcal{C}$. Thus

$$\begin{aligned} (S, w) &= \phi(E \cdot w) = (E \cdot w, 1) \\ &= (\mathrm{eval}_{\mathcal{C}}(E \cdot w), 1) = (\mathrm{eval}_{\mathcal{C}}(E) \circ w, 1) = (\mathrm{eval}_{\mathcal{C}}(E), w). \end{aligned}$$

Hence $S = \mathrm{eval}_{\mathcal{C}}(E)$.

The converse, that is the surjectivity of $\mathrm{eval}_{\mathcal{C}}$, is a direct consequence of the work of Droste–Gastin. They prove indeed that the semiring of recognizable series in $K\langle\langle A/\mathcal{C}\rangle\rangle$ is the smallest subsemiring containing $K\langle A/\mathcal{C}\rangle$ and closed under the star operation $S \mapsto S^*$ restricted to proper series such that each word in the support of S has the same, connected alphabet. From their constructions in [7], Section 4, using the LNF morphisms (especially Proposition 34), it is easy to construct for each recognizable series a rigid rational expression which is mapped on this series by $\mathrm{eval}_{\mathcal{C}}$. □

6. Concluding remarks

Remark. The theorem of Droste–Gastin characterizes recognizable series in $K\langle\langle A/\mathcal{C}\rangle\rangle$, generalizing the Kleene-Schützenberger theorem. The characterization involves the star operation restricted to *mono-alphabetic* and *connected* series (see the previous proof). Hence, the rational expression $(ab+c)^*$ of our running example is not covered by this result. However, it is recognizable and has therefore a mono-alphabetic and connected rational expression.

Indeed, by using the identities

$$(x+y)^* = x^*(yx^*)^*,\ (x+y)^* = (x^*y)^*x^* \text{ and } z^* = 1+zz^*,$$

we have

$$\begin{aligned}(ab+c)^* &= ((ab)^*c)^*(ab)^* = (c+(ab)^+c)^*(ab)^*\\ &= c^*((ab)^+c^+)^*(ab)^*\end{aligned}$$

and the latter expression is mono-alphabetic and connected (as usual x^+ stands for xx^*).

In the proof of Proposition 14, we have used the Droste–Gastin theorem for one direction. For the proof of the other direction, one could use another result of the same article, namely Theorem 23 in [7]. Our proof is however quite different and uses our main result.

Idempotent semirings. The semiring K is said to be idempotent if $1+1=1$. In this case, the main result may be modified, by taking connected rational expressions (these are defined by requiring that for each pure star E^*, the set $\mathrm{Alph}(E)$ contains only connected subalphabets), and by introducing the rational identities $\phi_B(H^*)\cdot H^* \equiv H^*$ for any subalphabet B. The proof of the theorem is modified accordingly. As mentioned in [7], one cannot consider connected rational expressions in general semirings.

Acknowledgements

We thank the referees for their numerous remarks that helped improving the presentation and the accuracy of the paper.

Appendix. An example illustrating the main theorem

We take the commutation graph of the running example and $E = (c+ab+b(abc)^*)^*$ which is a rigid rational expression. Then we get

$$\begin{aligned}&D_aE = c^*bE := F,\quad D_bE = (abc)^*E := G,\quad D_cE = E,\\ &D_aF = 0,\quad D_bF = E,\quad D_cF = F\\ &D_aG = bc(abc)^*E + D_aE := H + F,\\ &D_bG = D_bE = G,\quad D_cG = D_cE = E,\\ &D_aH = 0,\quad D_bH = c(abc)^*E := I,\quad D_cH = 0,\\ &D_aI = \phi_a(c)D_a((abc)^*E) = cbc(abc)^*E + cc^*bE := J + K,\\ &D_bI = 0,\quad D_cI = G,\\ &D_aJ = 0,\quad D_bJ = 0,\quad D_cJ = H,\\ &D_aK = 0,\quad D_bK = 0,\quad D_cK = F.\end{aligned}$$

The seven Words E, F, G, H, I, J, K therefore span a stable submodule. If we follow the proof of Proposition 14 and write the matrices μa and μc of the actions of D_a and D_c, we find

$$\mu a = EF + GH + GF + IJ + IK$$
$$\mu c = EE + FF + GE + IG + JH + KF$$

where we write EF for the corresponding elementary matrix. Thus, as predicted by the proof of the proposition, we observe the remarkable commutation

$$\mu a\, \mu c = \mu c\, \mu a = EF + GF + IH + IF.$$

References

[1] V. Antimirov, Partial derivatives of regular expressions, Theoret. Comput. Sci. 155 (1996) 291–319.
[2] J. Berstel, L. Boasson, Towards an algebraic theory of context-free languages, Fund. Inform. 25 (1996) 217–239.
[3] J. Berstel, C. Reutenauer, Rational Series and their Languages, Springer-Verlag, 1988.
[4] J.A. Brzozowski, Derivatives of regular expressions, J. Assoc. Comput. Mach. 11 (1964) 481–494.
[5] P. Cartier, D. Foata, Problèmes combinatoires de commutation et réarrangements, in: Lecture Notes in Mathematics, vol. 85, Springer-Verlag, 1969.
[6] J.W. Carlyle, A. Paz, Realizations by stochastic finite automata, J. Comput. System Sci. 5 (1971) 26–40.
[7] M. Droste, P. Gastin, The Kleene-Schützenberger theorem for formal power series in partially commuting variables, Inform. Comput. 153 (1999) 47–80.
[8] G. Duchamp, D. Krob, On the partially commutative shuffle product, Theoret. Comput. Sci. 96 (1992) 405–410.
[9] S. Dulucq, Equations avec opérateurs: Un outil combinatoire. Thèse de doctorat, Université de Bordeaux I, 1981.
[10] S. Dulucq, Séries algébriques solutions d'équations avec opérateurs, RAIRO Inform. Théor. 2 (1982) 139–163.
[11] M. Fliess, Matrices de Hankel, J. Math. Pures Appl. 53 (1974) 197–222.
[12] Y. Inagaki, T. Fukumura, H. Matuura, Some aspects of linear space automata, Inform. Control 20 (1972) 439–479.
[13] G. Jacob, Représentations et substitutions matricielles dans la théorie algébrique des transductions, Thesis, University of Paris, 1975.
[14] D. Krob, Expressions rationnelles sur un anneau, in: Topics in Invariant Theory, in: Lecture Notes in Mathematics, vol. 1478, Springer-Verlag, 1998, pp. 215–243.
[15] J.S. Lombardy, J. Sakarovitch, Derivatives of rational expressions with multiplicity, Theoret. Comput. Sci. 332 (2005) 141–177.
[16] K. Masashi, Y. Kobayashi, The shuffle algebra and its derivations, Theoret. Comput. Sci. 115 (1993) 359–369.
[17] W. Wechler, Characterization of rational and algebraic power series, RAIRO Inform. Théor. 17 (1983) 3–11.