Available at
www.ElsevierComputerScience.com
POWERED BY SCIENCE @ DIRECT®
Theoretical Computer Science 313 (2004) 31–44

Theoretical Computer Science

www.elsevier.com/locate/tcs

Derivatives of rational expressions and related theorems[☆]

Jean-Marc Champarnaud[*], Gérard Duchamp

LIFAR, Faculté des Sciences et des Techniques, University of Rouen, Place E Blondel, 76821 Mont-Saint-Aignan, Cedex, France

Abstract

Our aim is to study the set of K-rational expressions describing rational series. More precisely we are concerned with the definition of quotients of this set by coarser and coarser congruences which lead to an extension—in the case of multiplicities—of some classical results stated in the Boolean case. In particular, multiplicity analogues of the well known theorems of Brzozowski and Antimirov are provided.

Keywords: Series; Rational expressions; Automata; Congruences

1. Introduction

Language theory is a rich and everlasting domain of study since computers have always been operated by identifiers and sequences of words. In the case when weights are associated to words, the theory of series, which is an extension of language theory, is invoked. Some results of the two theories are strikingly similar, the preeminent example being the theorem of Kleene–Schützenberger which states that a series is rational if and only if it is recognizable (by a K-automaton) [27]. Therefore, we feel that it should be of interest to contribute to build firm foundations to the study of abstract formulae (i.e. K-rational expressions) describing rational series. These formulae have been used as a powerful tool to describe the inverse of a noncommutative matrix [13].

Rational expressions are realizable into the algebra of series. They are the counterpart of regular expressions of language theory and our work on rational expressions is close

[☆] Partially supported by the MENRT Scientific Research Program ACI Cryptology.

[*] Corresponding author. Tel.: +33-0235147026; fax: +33-0235146763.
E-mail address: jmc@dir.univ-rouen.fr (J.-M. Champarnaud).

doi:10.1016/j.tcs.2003.10.005

to the contributions of Antimirov [1], Brzozowski [4] and more recently Champarnaud and Ziadi [5–7] who studied the properties of regular expressions and their derivatives.

The kernel of the projection: *rational expressions* → *rational series* will be called $\sim_{rat}$. We are concerned here with the study of congruences which are finer than $\sim_{rat}$ and which give rise to normal forms (for references on the subject of rational identities see [3,8,17,25]). Antimirov in [1] gives a list of axioms suited to the Boolean case. We give here a list of K-axioms which will be treated as congruences, extending the preceding ones in the case of multiplicities. A set of coarser and coarser congruences is considered and analogues of the well known theorems of Antimirov [1] and Brzozowski [4] are provided in this frame.

The structure of the paper is the following. The main theorems concerning congruences on the set of regular expressions are gathered in the next section. Section 3 gives a brief description of formal series and rational expressions. Section 4 introduces the notion of a K-module congruence, provides a list of admissible congruences to compute with rational expressions and states an analogue of Antimirov's theorem in the setting of multiplicities. Section 5 deals with the existence of deterministic recognizers and gives a generalization of Brzozowski's theorem.

2. Regular expressions

We briefly recall results issued from the works of Brzozowski [4] and Antimirov [1] in the Boolean domain. The reader is referred to [29] for a recent survey of automaton theory.

Brzozowski has defined the notion of *word derivative* of a regular expression. Let $\mathscr{R}(\Sigma)$ be the set of regular expressions over a given alphabet Σ. Let 0 denote the null expression and ε the empty word. Let E, F and G be regular expressions. We consider the following congruences on $\mathscr{R}(\Sigma)$:

- $E+(F+G)\sim(E+F)+G$ (Associativity of $+$) [A].
- $E+F\sim F+E$ (Commutativity of $+$) [C].
- $E+E\sim E$ (Idempotency of $+$) [I].

The $\sim_{aci}$ congruence is defined by [A,C,I].

Theorem 1 (Brzozowski [4]). *The set of derivatives of every regular expression in* $\mathscr{R}(\Sigma)/\!\sim_{aci}$ *is finite.*

Antimirov has introduced the notion of *partial derivative* of a regular expression. A *monomial* is a pair $\langle x,E\rangle$ where x is a symbol of Σ and E a nonnull regular expression. A linear form is a set of monomials. The word concatenation is extended to linear forms by the following equations, where l and l' are arbitrary linear forms, and F and E are regular expressions different of 0 and of ε:

$$l\odot 0=\emptyset,$$

$$\emptyset\odot E=\emptyset,$$

$$\begin{aligned}
l \odot \varepsilon &= l,\\
\{\langle x, \varepsilon\rangle\} \odot E &= \{\langle x, E\rangle\},\\
\{\langle x, F\rangle\} \odot E &= \{\langle x, F \cdot E\rangle\},\\
(l \cup l') \odot E &= (l \odot E) \cup (l' \odot E).
\end{aligned}$$

The linear form $lf(E)$ of a regular expression E is the set of monomials inductively defined as follows:

$$\begin{aligned}
lf(0) &= \emptyset,\\
lf(\varepsilon) &= \emptyset,\\
lf(x) &= \{\langle x, \varepsilon\rangle\}, \quad \forall x \in \Sigma,\\
lf(F + G) &= lf(F) \cup lf(G,),\\
lf(F \cdot G) &= \begin{cases} lf(F) \odot G & \text{if } Null(F) = 0,\\ lf(F) \odot G \cup lf(G) & \text{otherwise,} \end{cases}\\
lf(F^*) &= lf(F) \odot F^*.
\end{aligned}$$

Given a linear form $l = \{\langle x_1, F_1\rangle, \ldots, \langle x_k, F_k\rangle\}$ we write $\sum lf(E)$ to denote the regular expression $x_1 \cdot F_1 + \cdots + x_k \cdot F_k$ (up to an arbitrary permutation of the summands). Notice that $\sum \emptyset$ is 0.

Theorem 2 (Antimirov [1]). *For any regular expression E in $\mathscr{R}(\Sigma)$, the following linear factorization holds*:

$$E = \begin{cases} \sum lf(E) & \textit{if } Null(E) = 0,\\ \varepsilon + \sum lf(E) & \textit{otherwise.} \end{cases}$$

Finally, F is a partial derivative of E w.r.t. x if and only if there exists a monomial $\langle x, F\rangle$ in $lf(E)$. The following result holds:

Theorem 3 (Antimirov [1]). *The set of partial derivatives of every regular expression in $\mathscr{R}(\Sigma)$ is finite.*

3. Series and rational expressions

3.1. *Noncommutative formal series (NFS)*

3.1.1. *The algebra of NFS*

We give here a brief description of the, by now classical, theory of series. The reader is also invited to consult [3,14,19,20,28].

A semiring $K(+,\times)$ is the data of two structures of monoid $(K,+)$ (commutative) and $(K,\times)$ (not necessarily commutative), $\times$ being distributive over $+$ and 0_K being an annihilator (roughly speaking, a semiring is a ring where the "minus" operation may not exist). For a set of symbols Σ, a NFS is a mapping $f:\Sigma^*\to K$. The set of NFS (i.e. K^{Σ^*}) is often denoted $K\langle\langle\Sigma\rangle\rangle$. One denotes alternatively f in the "sum-like" form $S=\sum_{w\in\Sigma^*} f(w)w$ which appeals, in a natural way, the scalar product denotation $f(w)=\langle S|w\rangle$.

For every family of series $(S_i)_{i\in I}$, if for each word $w\in\Sigma^*$ the mapping $i\to\langle S_i|w\rangle$ has a finite support (i.e. the set of indices for which $\langle S_i|w\rangle\neq 0$ is finite), then the series

$$\sum_{w\in\Sigma^*}\left(\sum_{i\in I}\langle S_i|w\rangle\right)w$$

is well-defined and will be denoted by $\sum_{i\in I} S_i$. Such a family $(S_i)_{i\in I}$ will be called summable.

The following operations are natural in $K\langle\langle\Sigma\rangle\rangle$. Let us recall them:

(1) Sum and scalings are defined componentwise:

$$\sum_{w\in\Sigma^*} f(w)w+\sum_{w\in\Sigma^*} g(w)w := \sum_{w\in\Sigma^*}(f(w)+g(w))w,$$

$$\lambda\sum_{w\in\Sigma^*} f(w)w := \sum_{w\in\Sigma^*}(\lambda f(w))w; \quad \left(\sum_{w\in\Sigma^*} f(w)w\right)\lambda := \sum_{w\in\Sigma^*}(f(w)\lambda)w.$$

(2) Concatenation, Cauchy product, or convolution:

$$\left(\sum_{w\in\Sigma^*} f(w)w\right).\left(\sum_{w\in\Sigma^*} g(w)w\right) := \sum_{w\in\Sigma^*}\left(\sum_{uv=w} f(u)g(v)\right)w.$$

(3) If S is without constant term (i.e. $\langle S|\varepsilon\rangle=0_K$), the family $(S^n)_{n\in\mathbb{N}}$ is summable, and the sum $\sum_{n\geqslant 0} S^n$ will be denoted S^*.

Now, we get an algebra with four binary laws, two external ones (scalings) and two internal ones (sum and concatenation) and a unary internal law partially defined (the star). Notice that, when K is commutative, with f and λ as above, one has $\lambda.f = f.\lambda$ and only the left action of K is required.

The adjoint operation of left and right multiplications can be called shifts (known sometimes as "quotients" see [14]) and is of the first importance for the study of rationality. One can use a covariant denotation (such as $u\triangleleft f$; $f\triangleright u$ [15]) or a contravariant one (such as $u^{-1}f$; fu^{-1}).

Definition 4. (A) Right shifts (left quotients) of $S:=\sum_{w\in\Sigma^*}\langle S|w\rangle w$ are defined by

$$\langle S\triangleright u|w\rangle = \langle S|uw\rangle = \langle u^{-1}S|w\rangle.$$

(B) Left shifts (right quotients) of $S:=\sum_{w\in\Sigma^*}\langle S|w\rangle w$ are defined by

$$\langle u\triangleleft S|w\rangle = \langle S|wu\rangle = \langle Su^{-1}|w\rangle.$$

Note 1. (i) It is easy to see that "triangle" is covariant: $(S \triangleright u) \triangleright v = S \triangleright uv$; $u \triangleleft (v \triangleleft S) = uv \triangleleft S$, and "quotient" is contravariant: $u^{-1}(v^{-1}S) = (vu)^{-1}S$; $(Su^{-1})v^{-1} = S(vu)^{-1}$.

(ii) Shifts are (two-sided) linear, they satisfy very simple identities. Let $a \in \Sigma$; S, $S_i \in K\langle\langle\Sigma\rangle\rangle$ $(i = 1, 2)$. The following identities hold:

$$\begin{aligned}
a^{-1}x &= \varepsilon \text{ if } x = a,\\
&= 0 \text{ if } x \in (\Sigma - \{a\}) \cup \{0\},\\
a^{-1}(S_1 + S_2) &= a^{-1}S_1 + a^{-1}S_2,\\
a^{-1}(\lambda S) &= \lambda a^{-1}S;\ a^{-1}(S\lambda) = (a^{-1}S)\lambda,\\
a^{-1}(S_1.S_2) &= (a^{-1}S_1).S_2 + const(S_1)a^{-1}(S_2),\\
a^{-1}(S^*) &= (a^{-1}S).S^* \text{ (if } S \text{ has a null constant term).}
\end{aligned}$$

Notice that similar but more complicated identities hold for the trace monoid [12].

(iii) Right shifts commute with left shifts (straightforwardly due to associativity) and satisfy similar identities.

Example 5. For example, with $a \in \Sigma$; $\alpha, \beta \in K$ and $S = (a\alpha)^*(\beta a)^*$ one has $(a^{-1})^2 S = \alpha^2 S + (\alpha\beta + \beta^2)(\beta a)^*$. Finally, we get: $a^{-n}S = \alpha^n S + \sum_{1 \leqslant j \leqslant n} (\alpha^{n-j}\beta^j)(\beta a)^*$.

3.2. Rational expressions

3.2.1. Construction, constant terms and shifts

The completely free formulas for these laws is the universal algebra generated by $\Sigma \cup \{0_{\mathscr{E}}\}$ as constants and the five preceding laws ($1_{\mathscr{E}}$ will be constructed as $0_{\mathscr{E}}^*$ and still be denoted ε). These expressions, by a standard argument, form a set which will be denoted $\mathscr{E}^{cf}(\Sigma, K)$.

Example 6. For example $(a^*)^* \in \mathscr{E}^{cf}(\Sigma, K)$. However, we will see later that this expression is not to be considered as valid in our setting.

Now, we construct a pull-back of the "constant term" mapping of the series.

Definition 7. (i) The function $const : \mathscr{E}^{cf}(\Sigma, K) \to K$ is (partially) recursively defined by the rules

(1) If $x \in \Sigma \cup \{0_{\mathscr{E}}\}$ then $const(x) = 0_K$.

(2) If $E, E_i \in \mathscr{E}^{cf}(\Sigma, K)$, $i = 1, 2$ then

$$\begin{aligned}
&const(E_1 + E_2) = const(E_1) + const(E_2),\\
&const(E_1 \cdot E_2) = const(E_1) \times const(E_2),\\
&const(\lambda E) = \lambda\, const(E),\ const(E\lambda) = const(E)\lambda.
\end{aligned}$$

(3) If $const(E) = 0_K$ then $const(E^*) = 1_K$.

(ii) The domain of *const* (i.e. the set of expressions for which *const* is defined) will be denoted $\mathscr{E}(\Sigma,K)$ (or $\mathscr{E}$, for short) in the sequel (we then have $(0_K)^*=\varepsilon\in\mathscr{E}$).

Remark 8. (i) We define left and right shifts by formulas of Note 1 and their right analogues.

In this way, it is easy to see that we get well (everywhere) defined operators on $\mathscr{E}(\Sigma,K)$ which will be still denoted $a^{-1}(?)$ and $(?)a^{-1}$ in the sequel.

(ii) The set $\mathscr{E}(\Sigma,\mathbb{B})$ is a strict subset of the set of free regular expressions but, due to the (Boolean) identity $(X+\varepsilon)^*=X^*$, the two sets have the same expressive power.

(iii) The class of rational expressions is a small set (in the sense of Mc Lane [22]), its cardinal is countable if Σ and K are finite or countable.

(iv) Sticking to our philosophy of "following the Boolean track", we must be able to evaluate rational expressions within the algebra of series. It is a straightforward verification to see that, given a mapping $\phi:\Sigma\to\Sigma^+$, there exists a unique (poly)morphism $\bar{\phi}:\mathscr{E}\to K\langle\langle\Sigma\rangle\rangle$ which extends ϕ. In particular, let $\phi:\Sigma\hookrightarrow\Sigma^+$ be the inclusion mapping, then the kernel of $\bar{\phi}$ will be denoted $\sim_{rat}$. Notice here that $\bar{\phi}(1_{\mathscr{E}})=\varepsilon$.

Now, we can state a celebrated theorem discovered by Schützenberger and coined as Kleene–Schützenberger's theorem.

Theorem 9. *For a series $S\in K\langle\langle\Sigma\rangle\rangle$, the following conditions are equivalent*:

(i) *The series S is in the image of $\bar{\phi}$.*

(ii) *There exists a finite family $(S_i)_{i\in I}$, stable under derivation (i.e. $(\forall i\in I)(\forall a\in\Sigma)$ $a^{-1}S_i=\sum_{j\in I}\mu_{ij}(a)S_j$) such that S is a linear combination of the S_i (i.e. $S=\sum_{i\in I}\lambda_iS_i$).*

Definition 10. A series which fulfills the preceding equivalent conditions will be called rational. The set of rational series is denoted $K^{rat}\langle\langle\Sigma\rangle\rangle$.

3.2.2. Congruences

We are now interested to describe series by quotient structures of $\mathscr{E}(\Sigma,K)$ (going from $\mathscr{E}(\Sigma,K)\cong\mathscr{E}(\Sigma,K)/=$ to $K^{rat}\langle\langle\Sigma\rangle\rangle\cong\mathscr{E}(\Sigma,K)/\sim_{rat}$). If the equivalence is $\sim_{rat}$, we get the series with the advantage of algebraic facilities (K-module structures, many identities, etc...) but syntactic difficulties. In fact, the equivalence $\sim_{rat}$ is not well understood (the question of systems of identities—on expressions—for the K-algebra of series has been discussed in [8,17]). On the other end, equality does not provide even the identity: $\lambda(E+F)\sim\lambda E+\lambda F$ or, at least, associativity. This is the reason why Brzozowski [4] and Antimirov [1] studied intermediate congruences. What follows is a step in this direction.

Definition 11. A congruence on the algebra $\mathscr{E}(K,\Sigma)$ is an equivalence $\sim$ which is compatible with subtree substitutions.

The following proposition is rather straightforward, but of crucial importance.

Proposition 12. *The set of congruences on $\mathscr{E}(\Sigma,K)$ is a complete sublattice of the lattice of all equivalence relations.*

At this level, three things are lacking. First, rational expressions do not yet form a K-module in spite of the fact that the operators a^{-1} are wanted to be linear; second, an expression can have infinitely many independent derivatives (for example $E=(a^*).(a^*)$ with $K=\mathbb{N}$) and to end with we do not recover Brzozowski's theorem. There is a simple way to solve this at once. It consists in associating the expressions which are identical "up to a K-module axiom"; these congruences will be called K-module congruences.

4. *K*-module congruences

From now on and for a lighter exposition, we will consider K as a commutative semiring. For K noncommutative the theory holds but needs the structure of K–K-bimodule with is rather cumbersome to expound (and therefore confusing at first sight).

We shall see that there is a finest congruence $\sim_{acm1}$ such that the quotients of the laws $+:\mathscr{E}\times\mathscr{E}\to\mathscr{E}$ and $.ext:K\times\mathscr{E}\to\mathscr{E}$ endow $\mathscr{E}/\sim$ with a K-module structure. But, to get the classical "step by step" construction which guarantees that every rational expression can be embedded into a finite type module, one needs a little more (i.e. $\sim_{acm2}$).

4.1. General definitions and properties

Definition 13. Let $(M,+)$ be a commutative monoid with neutral 0_M. A K-module structure on M, is the data of an external law $K\times M\to M$ satisfying identically:
(1) $\lambda(u+v)=\lambda u+\lambda v$; $\lambda 0_M=0_M$.
(2) $(\lambda+\mu)u=\lambda u+\mu u$; $0_K u=0_M$.
(3) $\lambda(\mu u)=(\lambda\mu)u$; $1_K u=u$.

The notions of morphisms and submodules are straigthforward.

Remark 14. (i) The definition above stands for left modules and we a have a similar definition for right modules.

(ii) This structure amounts to the data of a morphism of semirings

$$K(+,\times)\to(End(M,+),+,\circ).$$

We give now some (standard) definitions on the set of functions $X\to K$ which will be of use below.

Definition 15. (i) For any set X, the set of functions $X\to K$ is a module and will be denoted K^X. In particular, the set $K\langle\langle\Sigma\rangle\rangle:=K^{\Sigma^*}$ of NFS forms a K-module.

(ii) The support of $f\in K^X$ is defined as $supp(f)=\{x\in X\,|\,f(x)\neq 0_K\}$.

(iii) The subset $K^{(X)}\subset K^X$ of functions with finite support is a submodule of K^X, sometimes called the free module with basis X.

Example 16. A commutative and idempotent monoid $(M,+)$ is naturally endowed with a (unique) $\mathbb{B}$-module structure given by $1_{\mathbb{B}}x=x$; $0_{\mathbb{B}}x=0_M$. This setting will be used in Section 5.

Note 2. (i) For implementation (as needed, for instance, after Theorem 23) an object $f\in K^{(X)}$ is better realized as a dynamic two rows array

$$\begin{array}{c|c|c} x_1 & \cdots & x_n \\ \hline \alpha_1 & \cdots & \alpha_n \end{array}$$

$x_1<\cdots<x_n$ being the support of f and $f(x_i)=\alpha_i$.

(ii) Every module considered below will be endowed with a richer structure, that is a linear action of the free monoid on it, denoted $(?).u$ and such that $(?).(uv)=((?).u).v$. Such a structure will be called a K–Σ^*-module structure. In fact, these actions will always come from the projections of (iterated) derivatives.

Now, we have to extend in this general framework the notion of stability mentioned in Theorem 9.

Definition 17. (i) Let $(m_i)_{i\in I}$ be a finite family in a K–Σ^*-module M. We say that it is stable under transitions (FST in the following) iff for every letter $a\in\Sigma$ and $i\in I$, we have coefficients $\mu_{ij}(a)$ such that

$$m_i.a=\sum_{j\in I}\mu_{ij}(a)m_j.$$

Equivalently, this amounts to say that the submodule generated by the family is stable under the action of Σ^*.

(ii) (λ-determinism) A FST will be called λ-deterministic if the rows of the transition matrices can be choosen with at most one nonzero element. That is for every letter $a\in\Sigma$ and $i\in I$, either $m_i.a=0_M$ or there exists $j\in I$ and $\mu_{ij}(a)$ such that

$$m_i.a=\mu_{ij}(a)m_j.$$

(iii) (Determinism for a FST) A FST will be called deterministic if the rows of the transition matrices can be choosen with at most one nonzero element which must be 1_K. That is for every letter $a\in\Sigma$ and $i\in I$, either $m_i.a=0_M$ or there exists $j\in I$ such that

$$m_i.a=m_j.$$

(iv) Let $\mathscr{F}=(m_i)_{i\in I}$ be a FST then, for every m linear combination of the FST (i.e. $m=\sum_{i\in I}\lambda_i m_i$) we will say that m admits the FST $\mathscr{F}$.

There is a simple criterion to test whether an element admits a deterministic FST.

Proposition 18 (Deterministic criterion). *Let M be a K–Σ^*-module. Then we have*

(i) *An element $m \in M$ admits a deterministic FST iff the set $\{m.u\}_{u\in\Sigma^*}$ is finite.*

(ii) *More precisely, if the (deterministic) FST is of cardinality n, the cardinality of the orbit of m by Σ^* (i.e. $m.\Sigma^* = \{m.u\}_{u\in\Sigma^*}$) has a cardinality which does not exceed $(n+1)^n$.*

Proof. Statements (i) and (ii) can be proven simultaneously, considering that the cardinality of the monoid of (row) deterministic $n \times n$ matrices (i.e. the set of matrices with at most one "one" on each row) has cardinality $(n+1)^n$. □

Note 3. (i) From the preceding proof one sees that, if an element admits a deterministic FST, there is a deterministic FST to which this element belongs.

(ii) If m admits a FST and if K is finite, then its orbit is finite and hence, m admits a deterministic FST.

(iii) The bound is reached for $\sharp\Sigma \geqslant 3$ and $\sharp K \geqslant n$. In fact, the monoid of (row) deterministic $n \times n$ matrices (seen as mappings $f : [0..n] \to [0..n]$ such that $f(0) = 0$) is generated by

- the transposition $(1,2)$,
- the long cycle $(1,2,3,\ldots,n)$,
- the projection $k \to k$; $k < n$ and $n \to 0$.

To each letter corresponds one of the preceding transitions (all of them must be choosen). Since $\sharp K \geqslant n$ we can take a family of n different coefficients $(\lambda_1,\lambda_2,\ldots,\lambda_n)$. Using the standard process to compute a FST with given transition matrices, we see that the expression with coordinate vector $(\lambda_1,\lambda_2,\ldots,\lambda_n)$ has an orbit with exactly $(n+1)^n$ elements.

The characterization for the λ-determinism seems to be not so simple. It is possible, however, to complete it in the case of one variable ($\Sigma = \{a\}$) and K a (commutative) field.

Proposition 19 (λ-deterministic criterion). *Let $\Sigma = \{a\}$ be a one letter alphabet and K be a field. Let M be a K–Σ^*-module. Then, an element $m \in M$ admits a λ-deterministic FST iff there exists an $N \in \mathbb{N} - \{0\}$ such that the module generated by $(m.a^n)_{n\geqslant N}$ is finite dimensional and if a^N acts diagonally on it.*

Proof. The "if" part follows from the fact that the monoid of λ-deterministic row matrices is of rank less than $(n+1)^n$. The "only if" part is shown by the explicit construction of a FST. □

4.2. Admissible congruences: a basic list

Now, we want to compute with rational expressions, so we need to give us additional rules. These rules must preserve the actions of $(a^{-1}(?))_{a\in\Sigma}$ and, since they must describe rational series, they must be finer than $\sim_{rat}$.

Definition 20. (i) A congruence $\sim$ on the set $\mathscr{E}(K,\Sigma)$ will be called admissible iff it is finer than $\sim_{rat}$ and compatible with the operators a^{-1} and the *const* mapping.

(ii) We give the following list of congruences on $\mathscr{E}(K,\Sigma)$:

- $E_1+(E_2+E_3)\sim(E_1+E_2)+E_3$ $(A+)$
- $E_1+E_2\sim E_2+E_1$ (C)
- $E+0_{\mathscr{E}}\sim 0_{\mathscr{E}}+E\sim E$ (N)
- $\lambda(E+F)\sim\lambda E+\lambda F$; $\lambda 0_{\mathscr{E}}\sim 0_{\mathscr{E}}$ $(ExtDl)$
- $(\lambda+\mu)E\sim\lambda E+\mu E$; $0_K E\sim 0_{\mathscr{E}}$ $(ExtDr)$
- $\lambda(\mu E)\sim(\lambda\mu)E$; $1_K E\sim E$ $(ExtA)$
- $(E+F)\cdot G\sim E\cdot G+F\cdot G$; $0_{\mathscr{E}}\cdot F\sim 0_{\mathscr{E}}$ (Dr)
- $E\cdot(F+G)\sim E\cdot F+E\cdot G$; $E\cdot 0_{\mathscr{E}}\sim 0_{\mathscr{E}}$ (Dl)
- $\varepsilon\cdot E\sim E$ (Ul) $(Unit\ left)$
- $E\cdot\varepsilon\sim E$ (Ur) $(Unit\ right)$
- $(\lambda E)\cdot F\sim\lambda(E\cdot F)$ (Mix$A\cdot$)
- $E\cdot(F\cdot G)\sim(E\cdot F)\cdot G$ $(A\cdot)$
- $E^*\sim\varepsilon+E\cdot E^*$ $(Star)$

(iii) The $\sim_{acm1}$ congruence is defined by $[A+,C,N,Ext(Dl,Dr,A)]$. $\sim_{acm2}$ is defined by $\sim_{acm1}\wedge MixA\cdot\wedge Dr$ that is $[A+,C,N,MixA\cdot,Ext(Dl,Dr,A)]$. $\sim_{acm3}$ is defined by $\sim_{acm1}\wedge MixA\cdot,\wedge A\cdot,\wedge Dr,l\wedge Ur,l$ that is $[A+,C,N,MixA\cdot,A\cdot,Dr,Dl,Ur,Ul,Ext(Dl,Dr,A)]$.

(iv) In the following $\mathscr{E}/\!\sim_{acmi}$ will be denoted $\mathscr{E}_i$.

Proposition 21. (i) *The set of admissible congruences is a complete sublattice of the lattice of all congruences on* $\mathscr{E}(K,\Sigma)$.

(ii) *All the* $\sim_{acmi}$ *are admissible congruences.*

Remark 22. (i) It is obvious that $\sim_{acm1}\subset\sim_{acm2}\subset\sim_{acm3}$.

(ii) The congruence $\sim_{acm1}$ is the finest one such that the quotients of the laws (sum and external product of $\mathscr{E}(K,\Sigma)$) endow the quotient $\mathscr{E}/\!\sim$ with a K-module structure.

(iii) For every admissible congruence $\sim$ coarser than $\sim_{acm1}$, the quotient $\mathscr{E}/\!\sim$ is canonically endowed with a (left) K-module structure (and hence a K–Σ^*-module structure since the congruence is a^{-1}-compatible).

The following proposition states that there is a tractable normal form in every quotient $\mathscr{E}_i=\mathscr{E}/\!\sim_{acmi}$, for $i=1,2,3$.

Theorem 23. *The modules* $\mathscr{E}_i$; $i=1,2,3$ *are free.*

4.3. An analogue for a theorem of Antimirov

Now we state an analogue of a theorem of Antimirov in our setting.

Theorem 24. (i) *To every* (*class of*) *rational expression*(*s*) $E\in\mathscr{E}/\!\sim_{acm2}$, *one can associate algorithmically a FST* $\mathscr{F}_E=(E_i)_{i\in I}$ *such that* E *is a linear combination of* $\mathscr{F}_E$.

(ii) (*Deterministic property*). *If the semiring is finite, then the set of derivatives in* $\mathscr{E}/\!\sim_{acm1}$ *of every rational expression is finite and hence admits a deterministic FST.*

Remark 25. The algorithms provided by a step by step construction are not always the best possible (see [11] for a probabilistic discussion on this point). One could, when it happens, avoid redundancy; see below an example where this can be done.

Example 26. Let $E = x^*(xx + y)^*$. The following FSTs are inductively computed:

$$
\begin{aligned}
fst(x) &= \{x, \varepsilon\},\\
fst(x^*) &= \{xx^*, \varepsilon\},\\
fst(xx) &= \{xx, x, \varepsilon\},\\
fst(xx + y) &= \{xx, x, y, \varepsilon\},\\
fst((xx + y)^*) &= \{xx(xx + y)^*, x(xx + y)^*, y(xx + y)^*, \varepsilon\},\\
fst(E = x^*(xx + y)^*) &= \{E_1 = xx^*(xx + y)^*, E_2 = xx(xx + y)^*;\\
&\qquad E_3 = x(xx + y)^*, E_4 = y(xx + y)^*, E_5 = \varepsilon\},\\
E &= E_1 + E_2 + E_4 + E_5.
\end{aligned}
$$

The previous theorem predicts the existence of a (algorithmically constructible) FST in the generated submodule of which every term is embedded. If K is a field or a finite semiring one can take a finite set of derivatives. This is not possible in general as shown by the following critical counterexample.

Example 27. Let $K = \mathbb{N}$ and $E = a^* \cdot a^*$. Then, applying the rules, one can show that, in $\mathscr{E}/\sim_{acm3}$, we have $a^{-n}E = E + na^*$ and so, the set of derivatives of E is infinite and cannot be generated by any finite subset of it. Moreover, the associated series admits no deterministic recognizer and hence it is so for E itself.

In fact, looking closer at the proof of Theorem 24(ii), one sees that the conclusion holds if the semiring satisfies the following weaker property:

Property B. [1] *The submonoid generated by a finite number of matrices in $K^{n\times n}$ is finite.*

Note 4. It is clear that finiteness implies Property B but the converse is false as shown by the semiring $\mathbb{B}^{(\mathbb{N})} \oplus \mathbb{B}.1_{\mathbb{N}}$, the subsemiring of functions $\mathbb{N} \to \mathbb{B}$ being either almost everywhere 0 or almost everywhere 1 (i.e. the subsets which are either finite or cofinite).

[1] In honour of Burnside, Brzozowski and Boole. Note that condition B is stronger that Burnside condition [10] for semirings.

5. Determinism and the converse of a theorem of Brzozowski

Our concern here is to study the existence of deterministic recognizers. We give a generalization of Brzozowski's theorem and its converse in the sense that we provide a necessary and sufficient condition over the semiring K so that every automaton could have a deterministic counterpart. Now, we weaken the $\sim_{acm1}$ equivalence so that, by specialization to $K=\mathbb{B}$ one should recover $\sim_{aci}$.

Definition 28. For a semiring K, the $\sim_{acs}$ equivalence is defined, on the set $\mathscr{E}_0=\mathscr{E}(K,\Sigma)\cup\{\omega\}$ $(\omega\notin\mathscr{E})$, by the pairs
- $E_1+(E_2+E_3)\sim(E_1+E_2)+E_3$ $(A+)$,
- $E_1+E_2\sim E_2+E_1$ (C),
- $E+\omega\sim\omega+E\sim E$ (N)

and the (S) relations
- $\lambda(E+F)\sim\lambda E+\lambda F$; $\lambda\omega\sim\omega$ $(ExtDl)$
- $(\lambda+\mu)E\sim\lambda E+\mu E$; $0_K E\sim\omega$ $(ExtDr)$
- $\lambda(\mu E)\sim(\lambda\mu)E$; $1_K E\sim E$ $(ExtA)$

One extends the operators a^{-1} to $\mathscr{E}_0$ by $a^{-1}(\omega)=\omega$. Then it is easy to check that $E\sim_{acs}F\Longrightarrow a^{-1}(E)\sim_{acs}a^{-1}(F)$.

Remark 29. One can check, in view of Example 16, that the trace on $\mathscr{E}$ of the congruence $\sim_{acs}$, in case $K=\mathbb{B}$, is the $\sim_{aci}$ congruence of Brzozowski.

Theorem 30. *For any semiring, the following conditions are equivalent:*
(i) *For every $E\in\mathscr{E}_0/\sim_{acs}$, the set $\{u^{-1}E\}u\in\Sigma^*$ is finite.*
(ii) *K satisfies property* B.

5.1. Reconstruction lemma, congruence $\sim_{acm3}$ and the linear forms of Antimirov

A well known lemma in language theory (and a little less in the theory of series) states that, for a series $S\in K\langle\langle\Sigma\rangle\rangle$ and with $const(S)=\langle S|\varepsilon\rangle$, one has

$$S=const(S)\varepsilon+\sum_{a\in\Sigma}a(a^{-1}S).$$

This equality can be stated (but, of course not necessarily satisfied) in $\mathscr{E}(K,\Sigma)/\sim$ for all admissible congruences which satisfy $(A+)$ and (C). We will call it the *reconstruction lemma* (RL) [15]. We establish the equivalence of (RL) and (Star) $(E^*\sim\varepsilon+E\cdot E^*)$. Otherwise stated, if one of these two statement holds, the other does.

Theorem 31. *Let $\sim$ be an admissible congruence coarser than $\sim_{acm3}$. Then $(Star)$ and (RL) are equivalent within $\mathscr{E}/\sim$.*

6. Conclusion

We have studied several congruences; our results can be summarized as follows:

	$\sim_{acm1}$	$\sim_{acm2}$	$\sim_{acm3}$
Feature	K–Σ^*-module structure Determinism (K of type B)	FST (existence)	Reconstruction lemma $\Leftrightarrow$ Star

References

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

[2] J. Berstel, D. Perrin, Theory of Codes, Academic Press, New York, 1985.

[3] J. Berstel, C. Reutenauer, Rational series and their languages, EATCS Monographs on Theoretical Computer Science, Springer, Berlin, 1988.

[4] J.A. Brzozowski, Derivatives of regular expressions, J. Assoc. Comput. Mach. 11 (4) (1964) 481–494.

[5] J.-M. Champarnaud, D. Ziadi, New finite automaton constructions based on canonical derivatives, in: S. Yu (Ed.), CIAA'2000, Lecture Notes in Computer Science, Vol. 2088, Springer, Berlin, 2001, pp. 94–104.

[6] J.-M. Champarnaud, D. Ziadi, From Mirkin's Prebases to Antimirov's word partial derivatives, Fund. Inform. 45 (3) (2001) 195–205.

[7] J.-M. Champarnaud, D. Ziadi, Canonical derivatives, partial derivatives, and finite automaton constructions, Theoret. Comput. Sci. 289 (2002) 137–163.

[8] J.H. Conway, Regular Algebras and Finite Machines, Chapman & Hall, London, 1974.

[9] K. Culik II, J. Kari, Finite state transformations of images, Proc. ICALP 95, Lecture Notes in Computer Science, Vol. 944, Springer, Berlin, 1995, pp. 51–62.

[10] M. Droste, P. Gastin, On aperiodic and star-free formal power series in partially commuting variables, in: D. Krob, A.A. Mikhalev, A.V. Mikhalev (Eds.), Proc. FPSAC'00, Springer, Berlin, June 2000.

[11] G. Duchamp, M. Flouret, É. Laugerotte, J.-G. Luque, Direct and dual laws for automata with multiplicities, Theoret. Comput. Sci. 267 (2001) 105–120.

[12] G. Duchamp, D. Krob, Combinatorics on traces, in: G. Rozenberg, V. Dieckert (Eds.), Book of traces EATCS monograph, World Scientific, Singapore, 1995.

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

[14] S. Eilenberg, Automata, Languages and Machines, Vol. A, Academic Press, New York, 1974.

[15] G. Jacob, Représentations et substitutions matricielles dans la théorie algébrique des transductions, Thèse d'état, Université Paris, Vol. VII, 1975.

[16] S.C. Kleene, Representation of events in nerve nets and finite automata, Automata Studies, Princeton University Press, Princeton, NJ, 1956, pp. 3–42.

[17] D. Krob, Models of a K-rational identity system, J. Comput. System Sci. 45 (3) (1992) 396–434.

[18] D. Krob, Differentiation of K-rational expressions identity system, Internat. J. Algebra Comput. 3 (1) (1993) 15–41.

[19] W. Kuich, Semirings and Formal Power Series, Handbook of Formal Languages, Vol. I, Springer, Berlin, 1997, pp. 609–677.

[20] W. Kuich, A. Salomaa, Semirings, automata, languages, in: EATCS Monographs on Theoretical Computer Science, Vol. 5, Springer, Berlin, 1986.

[21] M. Lothaire, Combinatorics on Words, Addison-Wesley, Reading, MA, 1983.

[22] S. Mac Lane, Categories for the Working Mathematician, 4th Ed., Springer, Berlin, 1988.

[23] B.G. Mirkin, An algorithm for constructing a base in a language of regular expressions, Engng. Cybernet. 5 (1966) 110–116.

[24] M. Mohri, F. Pereira, M. Riley, A rational design for a weighted finite-state transducer library, Lecture Notes in Computer Science, Vol. 1436, Springer, Berlin, 1998, pp. 43–53.

[25] C. Reutenauer, A survey on noncommutative rational series, Proc. FPSAC'94.

[26] A. Salomaa, M. Soittola, Automata-Theoretic Aspects of Formal Power Series, Springer, Berlin, 1978.

[27] M.P. Schützenberger, On the definition of a family of automata, Inform. Control 4 (1961) 245–270.

[28] R.P. Stanley, Enumerative Combinatorics, Vol. 2, Cambridge University Press, Cambridge, 1999.

[29] S. Yu, Regular languages, in: G. Rozenberg, A. Salomaa (Eds.), Handbook of Formal Languages, Words, Languages, Grammars, Vol. I, Springer, Berlin, 1997, pp. 41–110.