T(A) = T(B)?

Géraud Sénizergues

technical report nr 1209-99
LaBRI et Université de Bordeaux I, 351, Cours de la Libération 33405 Talence, France **

Abstract. The equivalence problem for deterministic pushdown transducers with inputs in a free monoid X^* and outputs in a linear group $H = \mathrm{GL}_n(\mathbb{Q})$, is shown to be *decidable*.
We first reduce the problem to the equivalence problem for deterministic rational series on the alphabet associated with a dpdt $\mathcal{M}$ and with coefficients in the group H. We then exhibit a *formal system* which generates only equivalent pairs of such series. Conversely, every pair of equivalent series admits a *regular proof*. Using previous works on test-sets, we show that the set of "regular" proofs is recursively enumerable.
As a corollary, the equivalence problem for dpdt's from a free monoid X^* into a free group $\mathrm{F}(Y)$ (or, a fortiori, a free monoid Y^*), is decidable.

Keywords: deterministic pushdown transducers; rational series; finite dimensional vector spaces; matrix semi-groups; test-sets; complete formal systems.

** email:ges@labri.u-bordeaux.fr
fax: 05-56-84-66-69
URL: http://www.labri.u-bordeaux.fr/~ges

1 Introduction

1.1 Transductions

A *transducer* is a device $\mathcal{M}$ which recognizes a function or, more generally, a binary relation from a free monoid X^* to another monoid H (which might be itself a free monoid Y^*). Such a binary relation is often called the *transduction* recognized by $\mathcal{M}$ and denoted by $\mathrm{T}(\mathcal{M})$. Given a family $\mathcal{F}$ of transducers , the equivalence problem for $\mathcal{F}$ is the following decision problem:

INSTANCE: $A, B,$ two transducers in $\mathcal{F}$

QUESTION: $\mathrm{T}(A) = \mathrm{T}(B)$?

This problem has been solved, positively or negatively, for many families of *finite* transducers (i.e. finite automata over $X^* \times H$), see the surveys [Cul90], [Lis96]. The case where $\mathcal{F}$ is the family of *deterministic pushdown* transducers, (dpdt's for short), has been also adressed in several works ([IR81, CK86b, TS89, Sén98a]):

- the case where $H = Y^*$ is adressed in [IR81, CK86b, TS89] and the equivalence problem is known to be decidable when A is a *strict-real-time* dpdt while B is a general dpdt [TS89].

- the case where H is an *abelian* group is known to be decidable ([Sén98b, section 11], [Sén98a]).

1.2 Main result

We show here that, given two deterministic pushdown *transducers* A, B from a free monoid X^* into a *linear group* $H = \mathrm{GL}_n(\mathsf{Q})$, one can decide whether $\mathrm{T}(A) = \mathrm{T}(B)$ or not (theorem 10.4).

This main new result immediately implies that the same problem is decidable for any group (or monoid) H, as soon as H is embeddable in a linear group $\mathrm{GL}_n(\mathsf{Q})$. Hence we obtain as a corollary the decidability of the equivalence problem for dpdt's A, B from a free monoid X^* into a *free group* $H = \mathrm{F}(Y)$, or a *free monoid* $H = Y^*$. Hence our main result generalizes the two above mentionned results from ([TS89],[Sén98a]).

1.3 Formalism, techniques and organization

We choosed here to see a transduction $T \subseteq X^* \times H$ as a *formal series* in $\mathsf{B}\langle\langle\, H \times X^* \,\rangle\rangle$, i.e. a series over the monoid of undeterminates $H \times X^*$ and with boolean coefficients. The nature of the problem leads then us to translate this equivalence problem as the problem of deciding whether

$$S \equiv T?$$

for two series $S, T \in \mathsf{B}\langle\langle\ K * V^*\ \rangle\rangle$, where K is an extension of the group H, V is an alphabet of variables associated with (A, B), $K * V^*$ is the free product of K by the free monoid V^* and $\equiv$ is a congruence over the semi-ring $\mathsf{B}\langle\langle\ K * V^*\ \rangle\rangle$. This congruence is defined, roughly speaking, by: $S \equiv T$ if and only if, S and T "generate the same series in $\mathsf{B}\langle\langle\ H \times X^*\ \rangle\rangle$". Our method for deciding such an equivalence leans on a combination of the methods developped in ([Sén97], [Sén98b]) for the equivalence problem for dpda's, with the methods developped in ([Gub85], [CK86a]) for Ehrenfeucht's conjecture (about the existence and computability of test-sets).
We exhibit a formal system $\mathcal{H}_0$ which generates pairs (S, T) of equivalent series in $\mathsf{B}\langle\langle\ K * V^*\ \rangle\rangle$ (mod $\equiv$). We define a notion of *regular* proof for this formal system: such proofs may be infinite but have regularities which resemble on one hand regular trees and, on the other hand, DT0L-languages. Each regular proof is described by some finite structure that we call a *germ* of proof. The two crucial steps of our solution are:

- the statement that the set of germs of proof is recursively enumerable (lemma 5.13); this step leans heavily on the ideas of [Gub85], [CK86a].
- the statement that $\mathcal{H}_0$ is "regularly complete"(theorem 10.3): every pair (S, T) of equivalent series has some regular proof in the system $\mathcal{H}_0$; this step is an adaptation to the case of series in $\mathsf{B}\langle\langle\ K * V^*\ \rangle\rangle$ of the techniques developped in ([Sén97], [Sén98b]) for series in $\mathsf{B}\langle\langle\ H \times V^*\ \rangle\rangle$, in the particular case where H was abelian.

The organization of the paper should be clear from the table of contents below. Though this organization is similar to that of ([Sén97], [Sén98b]), several parts of this work are completely new or at least significantly different from their corresponding part for ordinary automata; we have marked with a (†) symbol such *really new* paragraphs.

Table of Contents

2 Preliminaries

2.1 Finite K-automata †

K-automata Let $(K, \cdot)$ be some group. We call a finite K-automaton over the finite alphabet W any 7-tuple

$$\mathcal{M} =< K, W, Q, \delta, k_0, q_0, Q' >$$

such that Q is the finite set of states, δ, the set of transitions, is a finite subset of $Q \times W \times K \times Q$, $k_0 \in K$, $q_0 \in Q$ and $Q' \subseteq Q$. The series recognized by $\mathcal{M}$, $\mathrm{S}(\mathcal{M})$, is the element of $\mathsf{B}\langle\langle\ K * W^*\ \rangle\rangle$defined by

$$\mathrm{S}(\mathcal{M}) = k_0 \cdot A \cdot B^* \cdot C$$

where $A \in \mathsf{B}_{1,Q}\langle\langle\ K * W^*\ \rangle\rangle, B \in \mathsf{B}_{Q,Q}\langle\langle\ K * W^*\ \rangle\rangle$, and $C \in \mathsf{B}_{Q,1}\langle\langle\ K * W^*\ \rangle\rangle$ are given by:

$$A_{1,q} = \emptyset(\text{ if } q \neq q_0), \quad A_{1,q_0} = \epsilon,$$

$$B_{q,q'} = \sum_{(q,v,h,q') \in \delta} v \cdot h,$$

$$C_{q,1} = \emptyset \ \ (\ \text{ if } q \notin Q'), C_{q,1} = \epsilon \ \ (\ \text{ if } q \in Q').$$

(One can also deduce these definitions from the general one for an automaton over a monoid and the corresponding notion of subset recognized by such an automaton. In this article we chosed to speak of "boolean series" rather than "subsets", see §2.4). $\mathcal{M}$ is said W-*deterministic* iff,

$$\forall q \in Q, \forall v \in W, \mathrm{Card}(\{(k, r') \in K \times Q \mid (r, v, k, r') \in \delta\}) \leq 1. \tag{1}$$

$m-K$-automata Let $n, m \in \mathbb{N}-\{0\}$ be positive integers. By $\mathsf{B}_{n,m}\langle\langle\ K*W^*\ \rangle\rangle$ we denote the set of matrices of dimension (n, m) with entries in the semi-ring $\mathsf{B}\langle\langle\ K*W^*\ \rangle\rangle$. We call a finite m-K-automaton over the alphabet W any 7-tuple

$$\mathcal{M} =< K, W, Q, \delta, k_0, q_0, (Q'_j)_{1 \leq j \leq m} >$$

such that $< K, W, Q, \delta, k_0, q_0, Q >$ is a finite K-automaton and for every $j \in [1, m]$, $Q'_j \subseteq Q$. For every $j \in [1, m]$ we denote by $\mathcal{M}_j$ the finite K-automaton

$$\mathcal{M}_j =< K, W, Q, \delta, k_0, q_0, Q'_j > .$$

The vector recognized by $\mathcal{M}$, $\mathrm{S}(\mathcal{M}) \in \mathsf{B}_{1,m}\langle\langle\ K * W^*\ \rangle\rangle$, is defined by:

$$\mathrm{S}(\mathcal{M}) = (\mathrm{S}(\mathcal{M}_1), \ldots, \mathrm{S}(\mathcal{M}_j), \ldots, \mathrm{S}(\mathcal{M}_m)).$$

$\mathcal{M}$ is said W-*deterministic* iff it fulfills the condition (1) above and the condition (2) below:

$$\forall j, \ell \in [1, m], j \neq \ell \Rightarrow Q'_j \cap Q'_\ell = \emptyset. \tag{2}$$

2.2 Pushdown H-automata

Let us consider some group H. We call a *pushdown H-automaton* over the finite alphabet X any 7-tuple

$$\mathcal{M} =< H, X, Z, Q, \delta, q_0, z_0 >$$

where Z is the finite stack-alphabet, Q is the finite set of states, $q_0 \in Q$ is the initial state, z_0 is the initial stack-symbol and $\delta : QZ \times (X \cup \{\epsilon\}) \rightarrow \mathcal{P}_f(H \times QZ^*)$, is the transition mapping. Let $q, q' \in Q, \omega, \omega' \in Z^*, z \in Z, h \in H, w \in X^*$ and $a \in X \cup \{\epsilon\}$; we note $(qz\omega, h, aw) \longmapsto_{\mathcal{M}} (q'\omega'\omega, h \cdot h', w)$ if $(h', q'\omega') \in \delta(qz, a)$. $\stackrel{*}{\longmapsto}_{\mathcal{M}}$ is the reflexive and transitive closure of $\longmapsto_{\mathcal{M}}$. For every $q\omega, q'\omega' \in QZ^*$ and $h \in H, w \in X^*$, we note $q\omega \xrightarrow{(h,w)}_{\mathcal{M}} q'\omega'$ iff

$$(q\omega, 1_H, w) \stackrel{*}{\longmapsto}_{\mathcal{M}} (q'\omega', h, \epsilon).$$

$\mathcal{M}$ is said *deterministic* iff it fulfills the following disjunction:

$$\text{either } \mathrm{Card}(\delta(qz, \epsilon)) = 1 \text{ and for every } x \in X, \mathrm{Card}(\delta(qz, x)) = 0, \qquad (3)$$

$$\text{or } \mathrm{Card}(\delta(qz, \epsilon)) = 0 \text{ and for every } x \in X, \mathrm{Card}(\delta(qz, x)) \leq 1. \qquad (4)$$

A H-dpda $\mathcal{M}$ is said *normalized* iff, for every $qz \in QZ, x \in X$:

$$q'\omega' \in \delta_2(qz, x) \Rightarrow \mid \omega' \mid \leq 2, \text{ and } q'\omega' \in \delta_2(qz, \epsilon) \Rightarrow \mid \omega' \mid = 0, \qquad (5)$$

where $\delta_2 : QZ \times (X \cup \{\epsilon\}) \rightarrow \mathcal{P}_f(QZ^*)$, is the second component of the map δ. Given some deterministic pushdown H-automaton $\mathcal{M}$ and a finite set $F \subseteq QZ^*$ of configurations, the *series* (in $\mathsf{B}\langle\langle H \times X^* \rangle\rangle$) *recognized by $\mathcal{M}$ with final configurations F* is defined by

$$\mathrm{S}(\mathcal{M}, F) = \sum_{c \in F} \sum_{q_0 z_0 \xrightarrow{(h,w)}_{\mathcal{M}} c} (h, w).$$

Intuitively, for every pair (h, w) having a coefficient 1 in the series $\mathrm{S}(\mathcal{M}, F)$, h can be seen as the "output" of the automaton $\mathcal{M}$ on the "input" w. $\mathcal{M}$ can then be named a deterministic pushdown *transducer* from X^* to H.
As $\mathsf{B}\langle\langle H \times X^* \rangle\rangle$ is isomorphic with $\mathsf{B}\langle\langle H \rangle\rangle\langle\langle X^* \rangle\rangle$, we often denote by $h \cdot w$ the pair $(h, w) \in H \times X^*$. For the same technical reasons as in the boolean case ([Sén97]), we suppose that Z contains a special symbol e subject to the property:

$$\forall q \in Q, \delta(qe, \epsilon) = \{(1_H, q)\} \text{ and } \mathrm{im}(\delta_2) \subseteq \mathcal{P}_f(Q(Z - \{e\})^*). \qquad (6)$$

2.3 Deterministic context-free H-grammars

Let us fix some H-dpda $\mathcal{M}$. The *variable* alphabet $V_{\mathcal{M}}$ associated with $\mathcal{M}$ is defined as: $V_{\mathcal{M}} = \{[p, z, q] \mid p, q \in Q, z \in Z\}$. The context-free H-grammar associated with $\mathcal{M}$ is then $G_{\mathcal{M}} =< H, X, V_{\mathcal{M}}, P_{\mathcal{M}} >$ where $P_{\mathcal{M}}$ is the set of all the pairs of one of the following forms:

$$([p, z, q], x \cdot h \cdot [p', z_1, p''][p'', z_2, q]) \tag{7}$$

where $p, q, p', p'' \in Q, x \in X, (h, p'z_1z_2) \in \delta(pz, x)$

$$([p, z, q], x \cdot h \cdot [p', z', q]) \tag{8}$$

where $p, q, p' \in Q, x \in X, (h, p'z') \in \delta(pz, x)$

$$([p, z, q], a \cdot h) \tag{9}$$

where $p, q, \in Q, a \in X \cup \{\epsilon\}, (h, q) \in \delta(pz, a)$.

We call *mode* every element of $QZ \cup \{\epsilon\}$. For every $q \in Q, z \in Z$, qz is said ϵ-*bound* (respectively ϵ-free) iff condition (3) (resp. condition (4)) in the above definition of deterministic H-automata is realized. The mode ϵ is said ϵ-free.
Let K be a group containing H. We define a mapping $\mu : K * V^* \to QZ \cup \{\epsilon\}$ by

$$\mu(\epsilon) = \epsilon \text{ and } \mu(k \cdot [p, z, q] \cdot \beta) = pz,$$

for every $k \in K, p, q \in Q, z \in Z, \beta \in V^*$. For every $w \in V^*$ we call $\mu(w)$ the *mode* of the word w.

2.4 Monoids acting on semi-rings

Semi-ring $\mathsf{B}\langle\langle M \rangle\rangle$ The reader is referred to [BR88] for formal power series. Let us just review some terminology. Let $(\mathsf{B}, +, \cdot, 0, 1)$ where $\mathsf{B} = \{0, 1\}$ denote the semi-ring of "booleans". Let M be some monoid. By $(\mathsf{B}\langle\langle M \rangle\rangle, +, \cdot, \emptyset, 1_M)$ we denote the semi-ring of *boolean series* over M: the set $\mathsf{B}\langle\langle M \rangle\rangle$ is defined as B^M; the sum and product are defined as usual; each element $m \in M$ can be identified with the element of B^M mapping m on 1 and every other element $w' \in M - \{m\}$ on 0; every boolean series $S \in \mathsf{B}\langle\langle M \rangle\rangle$ can be written in a unique way as: $S = \Sigma_{w \in M} S_w \cdot w$, where, for every $w \in M$, $S_w \in \mathsf{B}$.
The map $\chi : \mathcal{P}(M) \to \mathsf{B}\langle\langle M \rangle\rangle$ associating to every subset P of M its characteristic series $\chi_P \in \mathsf{B}\langle\langle M \rangle\rangle$ is a semi-ring isomorphism from $(\mathcal{P}(M), \cup, \cdot, \emptyset, \{1_M\})$ to $(\mathsf{B}\langle\langle M \rangle\rangle, +, \cdot, \emptyset, 1_M)$. Therefore we can sometimes identify a series S with the subset $P = \{m \in M, S_m = 1\}$.
The usual ordering $\leq$ on B extends to $\mathsf{B}\langle\langle M \rangle\rangle$ by:

$$S \leq S' \text{ iff } \forall w \in W^*, S_w \leq S'_w.$$

We recall that for every $S \in \mathsf{B}\langle\langle\ M\ \rangle\rangle$, S^* is the series defined by: $S^* = \sum_{0\leq n} S^n$. Given two monoids M, M', a map $\psi : \mathsf{B}\langle\langle\ M\ \rangle\rangle \ \rightarrow \mathsf{B}\langle\langle\ M'\ \rangle\rangle$ is said *σ-additive* iff it fulfills: for every denumerable family $(S_i)_{i\in\mathbb{N}}$ of elements of $\mathsf{B}\langle\langle\ M\ \rangle\rangle$,

$$\psi(\sum_{i\in\mathbb{N}} S_i) = \sum_{i\in\mathbb{N}} \psi(S_i).$$

(In fact $\mathsf{B}\langle\langle\ M\ \rangle\rangle$ is always a *complete* semi-ring in the algebraic sense defined in [Kro87]; the map $\sum_I : M^I \rightarrow M$ sending $(S_i)_{i\in I}$ on $\sum_{i\in I} S_i$, is defined everywhere on M^I, is strongly associative and multiplication does distribute over this generalized sum.)

Actions of monoids Given a semi-ring $(\mathsf{S}, +, \cdot, 0, 1)$ and a monoid $(\mathsf{M}, \cdot, 1_M)$, a map $\circ : \mathsf{S} \times \mathsf{M} \rightarrow \mathsf{S}$ is called a *right-action* of the monoid M over the semi-ring S iff, for every $S, T \in \mathsf{S}, m, m' \in \mathsf{M}$:

$$0 \circ m = 0,\ \ S \circ 1_M = S,\ \ (S + T) \circ m = (S \circ m) + (T \circ m) \quad \text{and} \tag{10}$$

$$S \circ (m \cdot m') = (S \circ m) \circ m' \tag{11}$$

In the particular case where $\mathsf{S} = \mathsf{B}\langle\langle\ N\ \rangle\rangle$, for some monoid N, $\circ$ is said to be a σ-right-action if it fulfills the additional property that, for every denumerable family $(S_i)_{i\in\mathbb{N}}$ of elements of S and $m \in \mathsf{M}$:

$$(\sum_{i\in\mathbb{N}} S_i) \circ m = \sum_{i\in\mathbb{N}} (S_i \circ m). \tag{12}$$

***M* acting on $\mathsf{B}\langle\langle\ M\ \rangle\rangle$ (residuals action)** We recall the following classical σ-right-action $\bullet$ of the monoid M over the semi-ring $\mathsf{B}\langle\langle\ M\ \rangle\rangle$: for all $S, S' \in \mathsf{B}\langle\langle\ M\ \rangle\rangle, u \in M$

$$S \bullet u = S' \Leftrightarrow \forall w \in M,\ \ S'_w = S_{u\cdot w}. \tag{13}$$

(i.e. $S \bullet u$ is the *left-quotient* of S by u , or the *residual* of S by u). For every $S \in \mathsf{B}\langle\langle\ M\ \rangle\rangle$ we denote by $\mathsf{Q}(S)$ the set of residuals of S:

$$\mathsf{Q}(S) = \{S \bullet u \mid u \in M\}.$$

Let us denote by $\mathsf{B}_{n,m}\langle\langle\ M\ \rangle\rangle$ the set of matrices of dimension n, m with entries in $\mathsf{B}\langle\langle\ M\ \rangle\rangle$. The right-action $\bullet$ on $\mathsf{B}\langle\langle\ M\ \rangle\rangle$ is extended componentwise to $\mathsf{B}_{n,m}\ \langle\langle\ M\ \rangle\rangle$: for every $S = (s_{i,j})$, $u \in M$, the matrix $T = S \bullet u$ is defined by $t_{i,j} = s_{i,j} \bullet u$. The notation $\mathsf{Q}(S) = \{S \bullet u \mid u \in M\}$, is extended to matrices as well. Given $n \geq 1, m \geq 1$, and $S \in \mathsf{B}_{n,m}\langle\langle\ M\ \rangle\rangle$ we denote by $\mathsf{Q}_r(S)$ the set of *row-residuals* of S:

$$\mathsf{Q}_r(S) = \bigcup_{1\leq i\leq n} \mathsf{Q}(S_{i,*}).$$

The ordering $\leq$ on B is extended componentwise to $\mathsf{B}_{n,m}\langle\langle\ M\ \rangle\rangle$.

$M = K * W^*$ †

We refer the reader to [LS77] for a definition of the free product of two monoids (or groups). We focus here on the monoid $M = K * W^*$ defined as the free product of a group K with a free monoid W^*.

Definition 2.1 *We denote by $\preceq$ the binary relation over $K * W^*$ defined by: for every $u, w \in K * W^*$, $u \preceq w \Leftrightarrow \exists v \in K * W^*, u \cdot v = w$.*

One can easily check that $\preceq$ is a quasi-order i.e. a reflexive and transitive relation.

Definition 2.2 *Let $u \in K * W^*$. The monomial u is said* left-unitary *(resp.* right-unitary*) iff $u = \epsilon$ or $\exists v \in W, \beta \in K * W^*$ such that $u = v \cdot \beta$ (resp. $\exists v \in W, \alpha \in K * W^*$ such that $u = \alpha \cdot v$).*
A series $S \in \mathsf{B}\langle\langle\ K * W^*\ \rangle\rangle$ is said left-unitary (resp. right-unitary) iff all its monomials are left-unitary (resp. right-unitary).
A row-vector $S \in \mathsf{B}_{1,m}\langle\langle\ K * W^*\ \rangle\rangle$ is said left-unitary (resp. right-unitary) iff the series $\bar{S} = \sum_{j=1}^{n} S_j$ is left-unitary (resp. right-unitary).

Let M' be a monoid containing K as a submonoid. A map $\psi : \mathsf{B}\langle\langle\ K * W^*\ \rangle\rangle \to \mathsf{B}\langle\langle\ M'\ \rangle\rangle$ is called a *substitution* iff it is a semi-ring homomorphism which is σ-additive and leaves K pointwise invariant (i.e. $\forall k \in K, \psi(k) = k$). Such a map is completely defined by its restriction on the alphabet W.
Let us consider the unique σ-additive semi-ring homomorphism $\theta : \mathsf{B}\langle\langle\ K * W^*\ \rangle\rangle \to \mathsf{B}\langle\langle\ W^*\ \rangle\rangle$ such that:

$$\forall k \in K, \theta(k) = \epsilon, \ \ \forall w \in W, \theta(w) = w.$$

The *support* of a series $S \in \mathsf{B}\langle\langle\ K * W^*\ \rangle\rangle$ is defined by:

$$\mathrm{supp}(S) = \theta(S).$$

$K \times X^*$ acting on $\mathsf{B}\langle\langle\ K * V^*\ \rangle\rangle$ (automaton action)† Let us fix now a deterministic (normalized) H-dpda $\mathcal{M}$. We consider the associated H-grammar $G_{\mathcal{M}}$ and a group K containing the group H.

Action $\otimes$ We define a σ-right-action $\otimes$ of the monoid $K \times (X \cup \{e\})^*$ over the semi-ring $\mathsf{B}\langle\langle\ K * V^*\ \rangle\rangle$by: for every $p, q \in Q, z \in Z, x \in X, h \in H, k \in K$:

$$[p, z, q] \otimes x = \sum_{([p,z,q],m) \in P_{\mathcal{M}}} m \bullet (1_H, x), \tag{14}$$

$$[p, z, q] \otimes e = h \text{ iff } ([p, z, q], h) \in P_{\mathcal{M}}, \tag{15}$$

$$[p, z, q] \otimes e = \emptyset \text{ iff } (\{[p, z, q]\} \times H \cdot V^*) \cap P_{\mathcal{M}} = \emptyset, \tag{16}$$

$$k \otimes x = \emptyset, \ \ k \otimes e = \emptyset. \tag{17}$$

The action is extended to all monomials by: for every $k \in K, \beta \in K * V^*, y \in X \cup \{e\}$,

$$(k \cdot [p, z, q] \cdot \beta) \otimes y = k \cdot ([p, z, q] \otimes y) \cdot \beta, \tag{18}$$

and for every $S \in \mathsf{B}\langle\langle\ K * V^*\ \rangle\rangle, k \in K$,

$$S \otimes k = k^{-1} \cdot S. \tag{19}$$

Action $\odot$ A series $S \in \mathsf{B}\langle\langle\, K * V^* \,\rangle\rangle$ is said *ϵ-free* iff

$$\forall w \in K * V^*, S_w = 1 \Rightarrow \mu(w) \text{ is } \epsilon - \text{free}.$$

We define the map $\rho_\epsilon : \mathsf{B}\langle\langle\, K * V^* \,\rangle\rangle \to \mathsf{B}\langle\langle\, K * V^* \,\rangle\rangle$ as the unique σ-additive map such that,

$$\rho_\epsilon(\emptyset) = \emptyset, \;\; \rho_\epsilon(\epsilon) = \epsilon,$$

for every $k \in K, S \in \mathsf{B}\langle\langle\, K * V^* \,\rangle\rangle$,

$$\rho_\epsilon(k \cdot S) = k \cdot \rho_\epsilon(S),$$

and for every $p \in Q, z \in Z, q \in Q, \beta \in K * V^*$,

$$\rho_\epsilon([p,z,q] \cdot \beta) = \rho_\epsilon(([p,z,q] \otimes e) \cdot \beta) \text{ if } pz \text{ is } \epsilon - \text{bound and,}$$

$$\rho_\epsilon([p,z,q] \cdot \beta) = [p,z,q] \cdot \beta \text{ if } pz \text{ is } \epsilon - \text{free}.$$

The above definition is sound because, by hypothesis (5), every $[p,z,q] \otimes e$ is either the unit series ϵ or the empty series $\emptyset$. One can notice that for every $w \in K * V^*$, $\rho_\epsilon(w) \in K * V^* \cup \{\emptyset\}$. We call ρ_ϵ the ϵ-reduction map. We then define $\odot$ as the unique right-action of the monoid $K \times X^*$ over the semi-ring $\mathsf{B}\langle\langle\, K * V^* \,\rangle\rangle$ such that: for every $S \in \mathsf{B}\langle\langle\, K * V^* \,\rangle\rangle, k \in K, x \in X$,

$$S \odot x = \rho_\epsilon(\rho_\epsilon(S) \otimes (k,x)).$$

One can notice that if $u \in K * V^* - K$, then $S \odot u$ is ϵ-free. Let us consider the unique substitution $\varphi : \mathsf{B}\langle\langle\, K * V^* \,\rangle\rangle \to \mathsf{B}\langle\langle\, K \times X^* \,\rangle\rangle$ fulfilling: for every $v \in V$,

$$\varphi(v) = \sum_{\substack{k \in K, u \in X^* \\ v \odot ku = \epsilon}} k \cdot u$$

(in other words, φ maps every subset $L \subseteq K * V^*$ on the set generated by the grammar G from the set of axioms L).

Lemma 2.3 *For every $S \in \mathsf{B}\langle\langle\, K * V^* \,\rangle\rangle, k \in K, u \in X^*$,*

1. $\varphi(\rho_\epsilon(S)) = \varphi(S)$
2. $\varphi(S \odot (k,u)) = \varphi(S) \bullet (k,u)$, *i.e. φ is a morphism of right-actions.*

We denote by $\equiv$ the kernel of φ i.e.: for every $S, T \in \mathsf{B}\langle\langle\, K * V^* \,\rangle\rangle$,

$$S \equiv T \Leftrightarrow \varphi(S) = \varphi(T).$$

3 Effective test-sets for morphic sets †

We introduce here a notion of *morphic* subset of a finitely generated monoid which slightly generalizes the usual notion of DTOL-subset of a free monoid (i.e. DTOL language). The main result of this section is that such subsets always admit *finite test-sets* with respect to morphisms into a given linear monoid $H = \mathrm{M}_{n,n}(\mathbb{Q})$ and that such test-sets can be computed (theorem 3.5). However, this result follows quite easily from the ideas developped in ([Gub85, CK86a]) and some classical results in algorithmic polynomial ideal theory ([Hil90, Her26, Buc85]).

3.1 Morphic sets †

Let $(M, \cdot, 1_M)$ be a monoid.

Definition 3.1 *A subset L of M is said purely morphic iff there exists an element $u \in M$ and a finite sequence $\psi_1, \psi_2, \ldots, \psi_m (m \geq 1)$ of homomorphisms $\psi_i : M \to M$ such that:*

$$L = \{\psi(u) \mid \psi \in \mathcal{N}\}$$

where $\mathcal{N} = \{\psi_1, \psi_2, \ldots, \psi_m\}^*$, i.e. $\mathcal{N}$ is the sub-monoid of $\mathrm{Hom}(M, M)$ *generated by $\{\psi_1, \psi_2, \ldots, \psi_m\}$.*

Remark 3.2 *In the particular case where M is a finitely generated free monoid X^*, the notion of "pure morphic subset" coincides with the classical notion of "DTOL language" ([RS80]).*

Definition 3.3 *A subset $L \subseteq M$ is said morphic iff there exists an element $u \in M$, a finite sequence $\psi_1, \psi_2, \ldots, \psi_m (m \geq 1)$ of homomorphisms $\psi_i : M \to M$ and a rational subset $\mathcal{R}$ of $\{\psi_1, \psi_2, \ldots, \psi_m\}^*$ such that:*

$$L = \{\psi(u) \mid \psi \in \mathcal{R}\}.$$

(We recall the rational subsets of $\{\psi_1, \psi_2, \ldots, \psi_m\}^*$ can be characterised as the images of the rational subsets of a free monoid $\{y_1, y_2, \ldots, y_m\}^*$ of rank m, by the homomorphism $\Psi_0 : \{y_1, y_2, \ldots, y_m\}^* \to \{\psi_1, \psi_2, \ldots, \psi_m\}^*$ which maps y_i on ψ_i for every $i \in [1, m]$).

3.2 Test-sets †

Definition 3.4 *Let $(M, \cdot, 1_M), (N, \cdot, 1_N)$ be two monoids and $L \subseteq M$. A subset $F \subseteq L$ is called a* test-set *for L with respect to N iff, F is finite and, for every pair of homorphisms $\eta, \eta' : M \to N$, if η agrees with η' on F, then it also agrees on L:*

$$[\forall x \in F, \eta(x) = \eta'(x)] \Rightarrow [\forall x \in L, \eta(x) = \eta'(x)].$$

Our aim is to prove the following statement about test-sets in a finitely generated monoid.

Theorem 3.5 *Let $(M, \cdot, 1_M)$ be a finitely generated monoid, L be a morphic subset of M, n a non-negative integer and $H = \mathrm{M}_{n,n}(\mathbb{Q})$ (the monoid of square n by n matrices with entries in $\mathbb{Q}$). Then L admits a test-set F with respect to H and such a test-set can be computed from any $m+2$-tuple $u, \psi_1, \ldots, \psi_m, \mathcal{R}$ defining L.*

We shall first prove theorem 3.5 in the case of pure morphic subsets of a free monoid. Let W_1 be a finite alphabet, $u_1 \in W_1^*$ and $\xi_1, \ldots, \xi_m \in \mathrm{Hom}(W_1^*, W_1^*)$. Let us consider the pure morphic subset

$$L_1 = \{\xi(u_1) \mid \xi \in \mathcal{N}_1\}$$

where $\mathcal{N}_1 = \{\xi_1, \xi_2, \ldots, \xi_m\}^*$. We introduce (as in [CK86a]) the subsets:

$$F_k = \{\xi(u_1) \mid \xi \in \{\xi_1, \ldots, \xi_m\}^{\leq k}\}.$$

Lemma 3.6 *Let $k \in \mathbb{N}$ such that F_k is a test-set for F_{k+1}. Then F_k is a test-set for L_1.*

Proof: We use here the arguments of [CK86a, p.79]. Let us prove, by induction on ℓ, that, under the hypothesis of the lemma,

$$\forall \ell \geq k+1, F_k \text{ is a test-set for } F_\ell. \tag{20}$$

The basis of the induction is clear.
Suppose that F_k is a test-set for F_ℓ where $\ell \geq k+1$.
Let $\eta, \eta' : W_1^* \to H$ be two homomorphisms such that $\eta|L_k = \eta'|L_k$. Let $x \in F_{\ell+1}$.
If $x = u_1$, then $\eta(u_1) = \eta'(u_1)$ (because $u_1 \in F_\ell$).
Otherwise $x = \xi_i(x')$ for some $x' \in F_\ell$. As the morhisms η, η' are equal on F_{k+1} the morhisms $\eta \circ \xi_i, \eta' \circ \xi_i$ are equal on F_k, hence by induction hypothesis:

$$\eta \circ \xi_i | F_\ell = \eta' \circ \xi_i | F_\ell.$$

It follows that $\eta \circ \xi_i(x') = \eta' \circ \xi_i(x')$, i.e.

$$\eta(x) = \eta'(x).$$

We have proved that F_k is a test-set for $F_{\ell+1}$. Hence (20) is established. As $L_1 = \bigcup_{\ell \geq k} F_\ell$, (20) implies that F_k is a test-set for L_1. □

Lemma 3.7 *One can compute, from the $m+1$ tuple $u_1, \xi_1, \ldots, \xi_m$, an integer k such that F_k is a test-set for F_{k+1} with respect to H.*

Proof: We use here Guba's main idea,([Gub85]). Let us associate with every variable $w \in W_1$ a sequence of $2 \cdot n^2$ undeterminates:

$$(w_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n}, (w'_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n}.$$

We define homomorphisms $\zeta, \zeta' : W_1^* \to \mathrm{M}_{n,n}(\mathbb{Q}[w_{1,1}, \ldots, w_{n.n}, w'_{1,1}, \ldots, w'_{n.n}])$ by: for every $w \in W_1$

$$\zeta(w) = (w_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n}, \quad \zeta'(w) = (w'_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n}.$$

For every word $u \in W_1^*$ we consider the $2 \cdot n^2$ polynomials $(P_{u,i,j})_{1 \leq i \leq n, 1 \leq j \leq n} \in \mathbb{Q}[w_{1,1}, \ldots, w_{n.n}], (P'_{u,i,j})_{1 \leq i \leq n, 1 \leq j \leq n} \in \mathbb{Q}[w'_{1,1}, \ldots, w'_{n.n}]$ defined by:

$$P_{u,i,j} = (\zeta(u))_{i,j}, \quad P'_{u,i,j} = (\zeta'(u))_{i,j}.$$

One can check that, for any pair of morphisms $\eta, \eta' : W_1^* \to H$,

$$\eta(u) = \eta'(u) \Leftrightarrow [\forall (i,j) \in [1,n]^2, P_{u,i,j}(\ldots, (\eta(w))_{i',j'}, \ldots) = P'_{u,i,j}(\ldots, (\eta'(w))_{i',j'}, \ldots) \tag{21}$$

i.e. $\eta(u) = \eta'(u)$ iff the n^2 polynomials $P_{u,i,j} - P'_{u,i,j}$ are vanishing when one gives the undeterminates $w_{i',j'}$ the value $(\eta(w))_{i',j'}$ and the undeterminates $w'_{i',j'}$ the value $(\eta'(w))_{i',j'}$. Let us denote by I_k the ideal of $\mathbb{Q}[w_{1,1}, \ldots, w_{n.n}, w'_{1,1}, \ldots, w'_{n.n}]$ generated by $\{P_{u,i,j} - P'_{u,i,j} \mid u \in F_k, (i,j) \in [1,n]^2\}$. As the ring $\mathbb{Q}[w_{1,1}, \ldots, w_{n.n}, w'_{1,1}, \ldots, w'_{n.n}]$ is noetherian (by the the so-called "Hilbert's finite basis theorem", [Hil90]), there exists some $k \geq 0$ such that,

$$I_k = I_{k+1}. \tag{22}$$

Moreover, given a polynomial P and a finite sequence of polynomials $P_1, \ldots, P_\rho$ in $\mathbb{Q}[w_{1,1}, \ldots, w'_{n.n}]$ generating an ideal I, one can decide whether $P \in I$? (an historical reference is [Her26], see [Buc85] for up-to-date computational methods). It follows that one can compute an integer k satisfying (22). By (21) for such an integer k, F_k is a test-set for F_{k+1}. □

Lemma 3.8 *Let W_1 be a finite alphabet, L_1 be a pure morphic subset of the free monoid W_1^*, n a non-negative integer and $H = \mathrm{M}_{n,n}(\mathbb{Q})$. Then L admits a test-set F with respect to H and such a test-set can be computed from any $m+1$-tuple $u, \xi_1, \ldots, \xi_m$ defining L.*

Proof: By lemma 3.7 one can compute an integer $k \geq 0$ such that F_k is a test-set for F_{k+1} with respect to H and by lemma 3.6 F_k is also a test-set for L_1. □

Lemma 3.9 *Let W_1 be a finite alphabet, L be a morphic subset of the free monoid W_1^*, n a non-negative integer and $H = \mathrm{M}_{n,n}(\mathbb{Q})$. Then L admits a test-set F with respect to H and such a test-set can be computed from any $m+2$-tuple $u_1, \xi_1, \ldots, \xi_m, \mathcal{R}$ defining L.*

Proof: Let $Y = \{y_1, y_2, \ldots, y_m\}$ be a new alphabet and $\Psi_0 : Y^* \to \mathrm{Hom}(W_1^*, W_1^*)$ which maps y_i on ξ_i, for every $i \in [1,m]$. Let $\mathcal{B} =< Y, Q, \gamma, q_-, Q_+ >$ be a complete deterministic finite automaton, such that

$$\Psi_0({}^t\mathrm{L}(\mathcal{B})) = \mathcal{R},$$

(i.e. $\mathcal{B}$ recognizes a language whose mirror-image is sent onto $\mathcal{R}$ by Ψ_0). We consider the alphabet

$$W_2 = W_1 \cup Q,$$

the word

$$u_2 = q_- \cdot u_1,$$

with every homorphism $\xi_i \in \mathrm{Hom}(W_1^*, W_1^*)$ we associate the new homorphism $\bar{\xi}_i \in \mathrm{Hom}(W_2^*, W_2^*)$ defined by

$$\forall w \in W_1, \bar{\xi}_i(w) = \xi_i(w), \;\; \forall q \in Q, \bar{\xi}_i(q) = \gamma(q, y_i) \in Q.$$

With every homomorphism $\eta \in \mathrm{Hom}(W_1^*, H)$ we associate the homorphism $\bar{\eta} \in \mathrm{Hom}(W_2^*, H)$ defined by

$$\forall q \in Q_+, \bar{\eta}(q) = 1_H, \;\; \forall q \in Q - Q_+, \bar{\eta}(q) = 0_H, \;\; \forall w \in W_1, \bar{\eta}(w) = \eta(w),$$

where 0_H denotes the $n - n$ matrix with only null entries. Let L_2 be the pure morphic subset of W_2^* defined by:

$$L_2 = \{\bar{\xi}(u_2) \mid \bar{\xi} \in \{\bar{\xi}_1, \ldots, \bar{\xi}_m\}^*\}.$$

By lemma 3.8, L_2 admits a test-set F' with respect to H and this subset F' can be computed.
Let us consider the homorphism $\bar{\Pi} \in \mathrm{Hom}(W_2^*, W_1^*)$ defined by

$$\forall q \in Q, \bar{\Pi}(q) = \epsilon, \;\; \forall w \in W_1, \bar{\Pi}(w) = w,$$

and let us define the subset

$$F = \bar{\Pi}(F' \cap (Q_+ \cdot W_1^*)).$$

One can check that, for every pair of morphisms $\eta, \eta' \in \mathrm{Hom}(W_1^*, H)$,

$$\begin{aligned} \forall x \in L, \eta(x) = \eta'(x) &\Leftrightarrow \\ \forall x \in L_2, \bar{\eta}(x) = \bar{\eta'}(x) &\Leftrightarrow \\ \forall x \in F', \bar{\eta}(x) = \bar{\eta'}(x) &\Leftrightarrow \\ \forall x \in F, \eta(x) = \eta'(x). & \end{aligned}$$

Hence F is a test-set for L with respect to H and F can be constructed. $\Box$

We are ready now to **prove** theorem 3.5.
Let $\Pi : W_1^* \to M$ be a surjective morphism (where W_1 is some finite alphabet). Let L be a morphic subset of M. We suppose it is defined by a $m+2$-tuple $u_0, \psi_1, \ldots, \psi_m, \mathcal{R}$, with $u_0 \in M$, $\psi_i \in \mathrm{Hom}(M, M), \mathcal{R} \in \mathrm{Rat}(\mathrm{Hom}(M, M))$. Let us fix some lifting $u_1, \xi_1, \ldots, \xi_m$ of this $m+1$-tuple, i.e. $u_1 \in W_1^*, \xi_i \in \mathrm{Hom}(W_1^*, W_1^*)$ such that:

$$\Pi(u_1) = u_0,$$

$$\Pi \circ \xi_i = \psi_i \circ \Pi.$$

Let us consider some rational subset $\bar{\mathcal{R}}$ of $\{y_1, \ldots, y_m\}^*$ such that

$$\mathcal{R} = \Psi_0(\bar{\mathcal{R}})$$

where Ψ_0 maps every y_i on ψ_i and let us define

$$\mathcal{R}_1 = \Psi_1(\bar{\mathcal{R}})$$

where Ψ_1 maps every y_i on ξ_i. Let us consider the morphic subset L_1 of W_1^* defined by this lifting:

$$L_1 = \{\xi(u_1) \mid \xi \in \mathcal{R}_1\}.$$

By lemma 3.9, L_1 admits a test-set F_1 with respect to H and such a test-set can be computed. One can check that $F = \Pi(F_1)$ is a test-set for L with respect to H. $\square$

4 Series and matrices

4.1 Deterministic series and matrices

We introduce here a notion of *deterministic* series which, in the case where the alphabet W is associated to a dpda $\mathcal{M}$ and the group K is reduced to $\{1\}$, generalizes the classical notion of *configuration* of $\mathcal{M}$. Let us consider a pair $(W, \smile)$ where W is an alphabet and $\smile$ is an equivalence relation over W. We call $(W, \smile)$ a *structured* alphabet. The two examples we have in mind are:

- the case where $W = V$, the variable alphabet associated to $\mathcal{M}$ and $[p, A, q] \smile [p', A', q']$ iff $p = p'$ and $A = A'$ (see [Har78])
- the case where $W = X$, the terminal alphabet of $\mathcal{M}$ and $x \smile y$ holds for every $x, y \in X$ (see [Har78]).

Let us also consider a group K.

Definitions

Definition 4.1 *Let* $S, T \in \mathsf{B}\langle\langle K * W^* \rangle\rangle$*.* S, T *are said* proportional *and we note* $S \approx T$*, if and only if, there exists* $k \in K$ *such that* $S = k \cdot T$*.*

The right-action $\bullet : \mathsf{B}\langle\langle K * W^* \rangle\rangle \times K * W^* \to \mathsf{B}\langle\langle K * W^* \rangle\rangle$ is compatible with the equivalence $\approx$, therefore it induces a right-action over $\mathsf{B}\langle\langle K * W^* \rangle\rangle/\approx$ which is denoted by the same symbol $\bullet$.

Definition 4.2 *Let* $S \in \mathsf{B}\langle\langle K * W^* \rangle\rangle$*.* S *is said* left-deterministic *iff either*
(1) $S = \emptyset$ *or*
(2) $S \approx \epsilon$ *or*
(3) $\forall k \in K, A \in W, \beta, \gamma \in K * W^*, [k \cdot A \cdot \beta \leq S, \gamma \leq S] \Rightarrow \exists A' \in W, \beta' \in K * W^*, A \smile A'$ *and* $\gamma = k \cdot A' \cdot \beta'$*.*

A left-deterministic series S is said to have the type $\emptyset$ (resp. ϵ, $[A]_\smile$) if case (1) (resp. (2), (3)) occurs.

Remark 4.3 *We remind the reader that, for every* $u \in K * W^*, S \in \mathsf{B}\langle\langle K * W^* \rangle\rangle$*, "*$u \leq S$*" can be rephrased in the following different ways:*

- $S_u = 1$
- *the monomial* u *has a non-null coefficient in* S
- u *"belongs" to* S*, viewed as a subset of* $K * W^*$*.*

Definition 4.4 *Let* $S \in \mathsf{B}\langle\langle K * W^* \rangle\rangle$*.* S *is said* deterministic *iff, for every* $u \in K * W^*$*,* $S \bullet u$ *is left-deterministic.*

This notion extends the notion of deterministic series of $\mathsf{B}\langle\langle W^* \rangle\rangle$ introduced in [Sén97] as an extension to the infinite case of the notion of (finite) *set of associates* defined in [HHY79].
We denote by $\mathsf{DB}\langle\langle K * W^* \rangle\rangle$ the subset of deterministic boolean series over $K * W^*$.

Definition 4.5 *Let* $m \in \mathbb{N}, S \in \mathsf{B}_{1,m}\langle\langle\ K * W^*\ \rangle\rangle : S = (S_1, \cdots, S_m)$. *S is said* left-deterministic *iff either*
(1) $\forall i \in [1,m], S_i = \emptyset$ *or*
(2) $\exists i_0 \in [1,m], S_{i_0} \approx \epsilon$ *and* $\forall i \neq i_0, S_i = \emptyset$ *or*
(3) $\exists i_0 \in [1,m], S_{i_0} \neq \emptyset$ *and* $\forall i,j \in [1,m], \forall k \in K, A \in W, \beta, \gamma \in K * W^*, [k \cdot A \cdot \beta \leq S_i, \gamma \leq S_j] \Rightarrow \exists A' \in W, \beta' \in K * W^*, A \smile A'$ *and* $\gamma = k \cdot A' \cdot \beta'$.

A left-deterministic row-vector S is said to have the type $\emptyset$ (resp. (ϵ, i_0), $[A]_\smile$) if case (1) (resp. (2), (3)) occurs.

Definition 4.6 *Let* $m \geq 1, S \in \mathsf{B}_{1,m}\langle\langle\ K * W^*\ \rangle\rangle$. *S is said* deterministic *iff, for every* $u \in K * W^*$, $S \bullet u$ *is left-deterministic.*

We denote by $\mathsf{DB}_{1,m}\langle\langle\ K * W^*\ \rangle\rangle$ the subset of deterministic row-vectors of dimension m over $\mathsf{B}\langle\langle\ K * W^*\ \rangle\rangle$. Given $S \in \mathsf{B}_{1,m}\langle\langle\ K * W^*\ \rangle\rangle$ we denote by $\mathsf{Q}_1(S)$ the set of its left-unitary residuals:

$$\mathsf{Q}_1(S) = \{S \bullet u \mid u \in K * W^*, S \bullet u \text{ is left-unitary}\},$$

(see definition 2.2).

Definition 4.7 *Let* $S \in \mathsf{B}_{n,m}\langle\langle\ K * W^*\ \rangle\rangle$. *S is said* deterministic *iff, for every* $i \in [1,n]$, $S_{i,*}$ *is a deterministic row-vector.*

Let us define here handful notations for some particular deterministic row-vectors. We use the *Kronecker symbol* $\delta_{i,j}$ meaning ϵ if $i = j$ and $\emptyset$ if $i \neq j$. For every $1 \leq i \leq n$, we define the row-vector ϵ_i^n as: $\epsilon_i^n = (\epsilon_{i,j}^n)_{1 \leq j \leq n}$ where $\forall j, \epsilon_{i,j}^n = \delta_{i,j}$. We call *unit row-vector* any vector of the form ϵ_i^n.

Residuals and product

Lemma 4.8 *Let* $S \in \mathsf{DB}_{1,m}\langle\langle\ K * W^*\ \rangle\rangle, T \in \mathsf{B}_{m,1}\langle\langle\ K * W^*\ \rangle\rangle, u \in W^*$ *and* $U = S \cdot T$. *Exactly one of the following cases is true:*

(1) $\exists j, S_j \bullet u \not\approx \emptyset, S_j \bullet u \not\approx \epsilon$; *in this case* $U \bullet u = (S \bullet u) \cdot T$.

(2) $\exists j_0, \exists k \in K, \exists u', u'', u = u' \cdot u'', S_{j_0} \bullet u' = k$; *in this case* $U \bullet u = k \cdot T_{j_0} \bullet u''$.

(3) $\forall j, S_j \bullet u \approx \emptyset$ *and* $\forall u' \preceq u, S_j \bullet u' \not\approx \epsilon$; *in this case* $U \bullet u = \emptyset = (S \bullet u) \cdot T$.

Lemma 4.9 *For every* $S \in \mathsf{DB}_{n,m}\langle\langle\ K * W^*\ \rangle\rangle, T \in \mathsf{DB}_{m,s}\langle\langle\ K * W^*\ \rangle\rangle$, $S \cdot T \in \mathsf{DB}_{n,s}\langle\langle\ K * W^*\ \rangle\rangle$.

Lemma 4.10 *If $S \in \mathsf{B}\langle\langle\ K * W^*\ \rangle\rangle$ is rational then $\mathsf{Q}(S)/\approx$ is finite.*

Sketch of proof:
step 1 Let us assume, in this first step , that K is finitely generated.
Let $\hat{Y}$ be some finite alphabet and $\psi_K : \hat{Y}^* \to K$, be a surjective morphism. We consider the unique morphism $\psi : \hat{Y}^* * W^* = (\hat{Y} \cup W)^* \to K * W^*$ such that, $\psi_{|\hat{Y}^*} = \psi_K, \quad \psi_{|W^*} = \mathrm{Id}_{W^*}$. Let us consider $S \in \mathsf{B}\langle\langle\ K * W^*\ \rangle\rangle$. As ψ is surjective, there exists some $\hat{S} \in \mathsf{B}\langle\langle\ (\hat{Y} \cup W)^*\ \rangle\rangle$ such that

$$\psi(\hat{S}) = S.$$

We establish first that: for every $u \in K*W^*$, if $u = k_0 \cdot m_1 \cdots k_{i-1} \cdot m_i \cdots k_{\ell-1} \cdot m_\ell$, where

$$(k_0, m_1, \cdots, k_{i-1}, m_i, \cdots, k_{\ell-1}, m_\ell)$$

is a reduced sequence i.e. $k_i \in K, m_i \in W^*, m_i \neq \epsilon$ (for $i \in [1, \ell-1]$), $k_i \neq 1_K$ (for $i \in [1, \ell-1]$) and, in addition

$$m_\ell \neq \epsilon, \tag{23}$$

then

$$S \bullet u = \sum_{\substack{\hat{u} \in (\hat{X} \cup \hat{Y})^* \\ \psi(\hat{u}) = u}} \psi(\hat{S} \bullet \hat{u}). \tag{24}$$

On one hand it is clear that, if $\psi(\hat{u}) = u$ and $\hat{v} \in \hat{Y}^* * W^*$ is such that $\hat{v} \leq \hat{S} \bullet \hat{u}$, then $\hat{u} \cdot \hat{v} \leq \hat{S}$ hence $u \cdot \psi(\hat{v}) \leq S$, hence $\psi(\hat{v}) \leq S \bullet u$. This shows that

$$\sum_{\substack{\hat{u} \in (\hat{X} \cup \hat{Y})^* \\ \psi(\hat{u}) = u}} \psi(\hat{S} \bullet \hat{u}) \leq S \bullet u \tag{25}$$

Conversely, let $v \in K * W^*$ such that $v \leq S \bullet u$. Hence

$$u \cdot v \leq S$$

There exists $\hat{w} \in (\hat{Y} \cup W)^*$ such that

$$\psi(\hat{w}) = u \cdot v \text{ and } \hat{w} \leq \hat{S}.$$

But condition (23) on the reduced sequence defining u and the freeness of the factor W^* imply that $\hat{w}$ has at least one decomposition

$$\hat{w} = \hat{u} \cdot \hat{v} \tag{26}$$

with $\psi(\hat{u}) = u, \psi(\hat{v}) = v$. Hence

$$\hat{v} \leq \hat{S} \bullet \hat{u}$$

and

$$v \leq \psi(\hat{S} \bullet \hat{u}) \text{ where } \psi(\hat{u}) = u,$$

which shows that

$$S \bullet u \leq \sum_{\substack{\hat{u} \in (\hat{X} \cup \hat{Y})^* \\ \psi(\hat{u}) = u}} \psi(\hat{S} \bullet \hat{u}). \tag{27}$$

By (25,27), we have proved (24).
Let $S \in \mathsf{RB}\langle\langle\ K * W^*\ \rangle\rangle$ (we suppose now that S is *rational*). The series $\hat{S}$ in the above computations can be chosen rational too. By the well-known Myhill-Nerode's theorem, $\mathsf{Q}(\hat{S})$ is finite. It follows that the sum in the righthand-side of formula (24) takes only finitely many values when u varies. Now, given any $u' \in K * W^*$ either $u' \in K$ or $\exists k \in K, \exists u \in K * W^*$ such that $u' = u \cdot k$ and u fulfills the special condition (23). It follows that either $S \bullet u' \approx S$ or $S \bullet u' \approx S \bullet u$, where $S \bullet u$ belongs to the finite set of values analyzed above. We conclude that $\mathsf{Q}(S)/\approx$ is finite.
Step 2 Let us remove the assumption that K is finitely generated. Let $S \in \mathsf{RB}\langle\langle\ K * W^*\ \rangle\rangle$. As S is rational, it also belongs to some $\mathsf{RB}\langle\langle\ K_0 * W^*\ \rangle\rangle$ for some finitely generated subgroup K_0 of K. Hence we are reduced to step 1. □

Definition 4.11 *Let $\mathcal{M} =< K, W, Q, \delta, k_0, q_0, (Q'_j)_{1 \leq j \leq m} >$ be some finite m-K-automaton over W. $\mathcal{M}$ will be said deterministic iff it is W-deterministic (see conditions (1),(2) in §2.1) and it also fulfills: $\forall q \in Q, A, A' \in W, k, k' \in K, r, r' \in Q$,*

$$((q, A, k, r) \in \delta \text{ and } (q, A', k', r') \in \delta) \Rightarrow A \smile A'.$$

The new property introduced in this definition might be called $\smile$-determinism as opposed to W-determinism which was defined by (1)(2).
Let us call a matrix $S \in \mathsf{B}_{n,m}\langle\langle\ K * W^*\ \rangle\rangle$ *rational* iff every component $S_{i,j}$ for $i \in [1, n], j \in [1, m]$ is rational.
The equivalence $\approx$ is extended to matrices by: for all $S, T \in \mathsf{B}_{n,m}\langle\langle\ K * W^*\ \rangle\rangle$,

$$S \approx T \Leftrightarrow \exists k \in K, S = k \cdot T.$$

Let us denote by $\mathsf{Q}_1(S)$ the set of all residuals of S which are left-unitary. One can check that, when $S \in \mathsf{B}_{1,m}\langle\langle\ K * W^*\ \rangle\rangle$ is a deterministic row-vector, every residual $q \in \mathsf{Q}(S)$ has a unique representative in $\mathsf{Q}_1(S)$ modulo $\approx$.

Proposition 4.12 *Let $m \geq 1$, $S \in \mathsf{DB}_{1,m}\langle\langle\ K * W^*\ \rangle\rangle$. The following properties are equivalent:*
(1) S is rational
(2) $\mathsf{Q}(S)/\approx$ is finite
(3) S is recognized by some deterministic finite m-K-automaton

(Notice that we assume S is deterministic, in the sense of definition 4.6, in this proposition).
Sketch of proof:

(1) $\Rightarrow$ (2): The case $m = 1$ is implied by lemma 4.10.
Let us suppose that $m \geq 2$ and let S be rational. By lemma 4.10 the set

$$\{(S_{1,1} \bullet u, \ldots, S_{1,j} \bullet u, \ldots, S_{1,m} \bullet u) \mid u \in K * W^*\} \tag{28}$$

is finite. Let us suppose that $u, u' \in K * W^*$ are such that, $\exists k_1, \ldots, k_j, \ldots, k_m \in K$,

$$\forall j \in [1, m], S_{1,j} \bullet u = k_j \cdot S_{1,j} \bullet u'. \tag{29}$$

We know that $S \bullet u, S \bullet u'$ are both left-deterministic. If $S \bullet u$ has the type $\emptyset$, it is clear that we can choose $k_j = 1$ in the equalities (29).
If $S \bullet u$ has the type (ϵ, j_0), then $S \bullet u'$ has the same type, hence all the k_j's can be taken equal with k_{j_0}.
If $S \bullet u$ has the type $[A]_\smile$, for some $A \in W$, then $S \bullet u'$ has the same type:

$$S \bullet u' = k \cdot (A_1, \ldots, A_j, \ldots, A_m) \cdot T'$$

$$S \bullet u = (k_1 \cdot k \cdot A_1, \ldots, k_j \cdot k \cdot A_j, \ldots, k_m \cdot k \cdot A_m) \cdot T'$$

for some $A_j \in [A]_\smile, T' \in \mathsf{DB}_{m,m}\langle\langle\, K * W^* \,\rangle\rangle$. But the fact that $S \bullet u$ is left-deterministic implies that all the coefficients k_j corresponding to non-null components $S_{1,j} \bullet u$ must be equal. Hence we can choose all the coefficients k_j identical in equalities (29). It follows that equalities (29) are equivalent to

$$S \bullet u \approx S \bullet u',$$

which, together with the finiteness of the set (28), proves condition (2) of the lemma.
(2) $\Rightarrow$ (3): Let S fulfilling condition (2) of the lemma. Let us define a m-K-automaton by:

$$\mathcal{M} =< K, W, Q, \delta, k_0, q_0, (Q'_j)_{1 \leq j \leq m} >,$$

where

$$Q = \mathsf{Q}_1(S),$$

q_0 is the unique left-unitary residual S_0 such that $S \approx S_0$ while $k_0 \in K$ is chosen such that

$$S = k_0 \cdot S_0,$$

$$Q'_j = \{\epsilon_j^m\}, \text{ for every } j \in [1, m],$$

and the transition map, δ, is defined by:

$$\delta = \{(q, v, k, q') \in \mathsf{Q}_1(S) \times W \times K \times \mathsf{Q}_1(S) \mid q \bullet v = k \cdot q'\}.$$

As S is deterministic, every residual of S is proportionnal to some left-unitary residual, i.e. the map $\Pi_\approx : \mathsf{Q}_1(S) \to \mathsf{Q}(S)/\approx$ is bijective, hence condition (2) of the lemma implies that the above automaton is *finite*. Let us check that

$$\mathrm{S}(\mathcal{M})_{1,j} = S_{1,j}. \tag{30}$$

One can easily check that

$$\mathrm{S}(\mathcal{M}) \leq S. \tag{31}$$

Conversely, let $u \in K * W^*$ be a monomial such that $u \leq S_{1,j}$. u has a decomposition:

$$u = h_0 \cdot v_1 \cdot h_1 \cdots v_i \cdot h_i \cdots v_\ell \cdot h_\ell$$

where $v_i \in W, h_i \in K$. For every $i \in [0, \ell]$ we define

$$S^{(i)} = S \bullet (h_0 \cdot v_1 \cdot h_1 \cdots v_i \cdot h_i).$$

As S is deterministic,

$$h_0 = k_0 \tag{32}$$

and $S \bullet (h_0 \cdot v_1 \cdot h_1 \cdots v_i \cdot h_i)$ is left-deterministic of type $[v_{i+1}]_\smile$ (resp. ϵ_j^m when $i = \ell$), hence

$$S^{(i)} \in \mathsf{Q}_1(S), \quad (S^{(i)}, v_{i+1}, h_{i+1}, S^{(i+1)}) \in \delta$$

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

$$(S_0, v_1, h_1, S^{(1)}) \cdot (S^{(1)}, v_1, h_1, S^{(2)}) \cdots (S^{(i-1)}, v_i, h_i, S^{(i)}) \cdots (S_{\ell-1}, v_\ell, h_\ell, S^{(\ell)})$$

is a path in $\mathcal{M}$ from $S_0 = q_0$ to $S_\ell = \epsilon_j^m$. It follows that u, the left-product of k_0 (see equality (32)) by the label of this path, fulfills $\mathrm{S}(\mathcal{M})_{1,j} \geq u$. As this inequality is true for every monomial $u \leq S_{1,j}$, it follows that:

$$\mathsf{S}(\mathcal{M})_{1,j} \geq S_{1,j}. \tag{33}$$

By (31,33) , formula (30) is proved.
The definition of δ shows that $\mathcal{M}$ fulfills conditions (1) (2) of subsection 2.1. The hypothesis that S be deterministic implies that δ also fulfills the condition introduced in definition 4.11, i.e. that $\mathcal{M}$ is deterministic.
(3) $\Rightarrow$ (1): Let S fulfilling condition (3). Each component, $S_{1,j}$ is recognized by the finite K-automaton $\mathcal{M}_j =< K, W, Q, \delta, k_0, q_0, Q'_j >$, hence each component $S_{1,j}$ is rational.
□

Remark 4.13 *When S is merely taken in $\mathsf{B}_{1,m}\langle\langle\, K * W^* \,\rangle\rangle$ (and no longer assumed deterministic), then*

$$(3) \Leftrightarrow S \in \mathsf{DRB}_{1,m}\langle\langle\, K * W^* \,\rangle\rangle.$$

But, as soon as $m \geq 2$, everyone of the implications $(1) \Rightarrow (2), (1) \Rightarrow (3), (2) \Rightarrow (1), (2) \Rightarrow (3)$ fails for some vectors S.

Norm Condition (2) of proposition 4.12 suggests the following notion of *norm*. For every $S \in \mathsf{DB}_{n,m}\langle\langle\, K * W^* \,\rangle\rangle$, the norm of S is defined by:

$$\|S\| = \mathrm{Card}(\mathsf{Q}_r(S)/\approx) \in \mathsf{N} \cup \{\infty\}.$$

It follows from proposition 4.12 that a deterministic matrix $S \in \mathsf{DB}_{n,m}\langle\langle\, K * W^* \,\rangle\rangle$ is rational iff it has a finite norm.

Lemma 4.14 *Let $S \in \mathsf{DB}_{n,m}\langle\langle\, K * W^* \,\rangle\rangle, T \in \mathsf{DB}_{m,s}\langle\langle\, K * W^* \,\rangle\rangle$. Then $\|S \cdot T\| \leq \|S\| + \|T\|$.*

Generic series † We consider here the particular case where $K = \mathrm{F}(U) * H$, where H is some group and U is a denumerable set (we call it the set of *parameters* in the sequel). By $\mathrm{Hom}(K, K)$ we denote the monoid of all homomorphisms from K to K and by $\mathrm{Hom}_H(K, K)$ we denote the set of homomorphisms $\psi : K \to K$ which leave H pointwise invariant, i.e. such that: $\forall x \in H, \psi(x) = x$.

Definition 4.15 *Let $S, T \in \mathsf{DB}\langle\langle\ K * W^*\ \rangle\rangle$. S, T are said* similar *and we note $S \sim T$, if and only if, there exists a bijection $\Psi : \mathsf{Q}(S)/\approx\ \to\ \mathsf{Q}(T)/\approx$ such that, for every $q \in \mathsf{Q}(S), v \in W$,*

$$\Psi([q]_\approx \bullet v) = \Psi([q]_\approx) \bullet v.$$

Definition 4.16 *Let $S \in \mathsf{DB}\langle\langle\ K * W^*\ \rangle\rangle$. S is said* generic *if and only if for every monomials $\alpha \cdot v \cdot k \cdot \beta, \alpha' \cdot v' \cdot k' \cdot \beta' \leq S$, where $v, v' \in W, k, k' \in K, \alpha, \alpha', \beta, \beta' \in K * W^*$, β, β' left-unitary, such that $k = k'$ we have:*

$$k \in U, k' \in U, S \bullet \alpha = S \bullet \alpha' \text{ and } v = v'.$$

Intuitive idea: a deterministic rational series S is "generic" when all the transitions of its "minimal transducer" (i.e. the K-automaton exhibited in the proof of proposition 4.12) have the form (q, v, u_i, q') for some $u_i \in U$ and in addition, different transitions have different "outputs" u_i.

Lemma 4.17 *For every $S \in \mathsf{DB}\langle\langle\ K * W^*\ \rangle\rangle$ there exists $S_0 \in \mathsf{DB}\langle\langle\ K * W^*\ \rangle\rangle, \psi \in \mathrm{Hom}_H(K, K)$ such that: $S \sim S_0$, S_0 is generic and $\psi(S_0) = S$.*

(In the above statement we use the same letter for a group homomorphism $\psi : K \to K$ and its unique extension as a σ-additive semi-ring homomorphism $\mathsf{B}\langle\langle\ K * W^*\ \rangle\rangle \to \mathsf{B}\langle\langle\ K * W^*\ \rangle\rangle$ which leaves W pointwise invariant).

Lemma 4.18 *Let $S, T \in \mathsf{DB}\langle\langle\ K * W^*\ \rangle\rangle$ such that S, T are both generic and $S \sim T$. Then, there exists a bijection $\psi : U \to U$ inducing an automorphism $\psi \in \mathrm{Aut}(K, K)$ such that $\psi(S) = T$.*

Corollary 4.19 *Given a finite subset $U_0 \subseteq U$ and an integer $n \in \mathbb{N}$, the set*

$$\{S \in \mathsf{DB}\langle\langle\ \mathrm{F}(U_0) * H * W^*\ \rangle\rangle \mid S \text{ is generic }, \| S \| \leq n\}$$

is finite.

W=V Let $(W, \smile)$ be the structured alphabet $(V, \smile)$ associated with the H-dpda $\mathcal{M}$ and let K be a group containing H. We consider a bijective numbering of the elements of Q: $(q_1, q_2, \ldots, q_{n_Q})$. Some particular "vectorial" notions turn out to be useful:

- we define a Q-*series* to be a family $(S_q)_{q\in Q}$ such that the row-vector $(S_{q_1}, S_{q_2}, \ldots, S_{q_{n_Q}})$ is deterministic
- we define a Q-*form* to be a family $\Phi = (\Phi_q)_{q\in Q}$ of deterministic series.

Given a Q-series S and a Q-form Φ, their Q-product $S * \Phi$ is the deterministic series defined by $S * \Phi = \sum_{q\in Q} S_q \cdot \Phi_q$. If the Q-series $(S_q)_{q\in Q}$ is identified with the row-vector $(S_{q_1}, S_{q_2}, \ldots, S_{q_{n_Q}})$ and the Q-form $(\Phi_q)_{q\in Q}$ with the column-vector $(\Phi_{q_j})_{j\in[1,n_Q]}$, then the Q-product appears to be just the ordinary product of matrices.

Let us define here handful notations for some particular Q-series. For every $\omega \in Z^*, p, q \in Q$, $[p\omega q]$ is the deterministic series defined inductively by:

$$[p\epsilon q] = \emptyset \text{ if } p \neq q, [p\epsilon q] = \epsilon \text{ if } p = q,$$

$$[p\omega q] = \sum_{r\in Q} [pAr] \cdot [r\omega' q] \text{ if } \omega = A \cdot \omega' \text{ for some } A \in Z, \omega' \in Z^*.$$

By $[p\omega]$ we denote the Q-series: $[p\omega] = ([p\omega q])_{q\in Q}$. (In particular $[q_i] = \epsilon_i^{n_Q}$). By $[\omega]$ we denote the Q-matrix: $[\omega] = ([p\omega q])_{p\in Q, q\in Q}$. Here also we identify $[\omega]$ with the matrix $([p_i \omega q_j])_{1\leq i\leq n_Q, 1\leq j\leq n_Q} \in \mathsf{DB}_{n_Q,n_Q}\langle\langle\, K * V^* \,\rangle\rangle$.
The next lemmas relate the map ρ_ϵ and right-action $\odot$ with the right-action $\bullet$.

Lemma 4.20 *Let* $m \in \mathbb{N} - \{0\}, S \in \mathsf{DB}_{1,m}\langle\langle\, K * V^* \,\rangle\rangle$.

1. *there exists* $v \in V^*$ *such that* $\rho_\epsilon(S) = S \bullet v$.
2. $\rho_\epsilon(S) \in \mathsf{DB}_{1,m}\langle\langle\, K * V^* \,\rangle\rangle$.
3. $\rho_\epsilon(S) \equiv S$.

Lemma 4.21 *Let* $m \in \mathbb{N} - \{0\}, S \in \mathsf{DB}_{1,m}\langle\langle\, K * V^* \,\rangle\rangle, u \in X^*$. *One of the three following cases must occur:*
(1) $S \odot u \approx \emptyset^m$, *or*
(2) $S \odot u \approx \epsilon_j^m$, *for some* $j \in [1, m]$ *or*
(3) $\exists u_1, u_2 \in X^*, v_1 \in K * V^*, k \in K, q \in Q, A \in Z, \Phi\ Q - m - \text{form such that}$ $u = u_1 \cdot u_2, \rho_\epsilon(S) \odot u_1 = S \bullet v_1 = k \cdot [qA] * \Phi$ *and* $S \odot u = (k \cdot [qA] \odot u_2) * \Phi$.

Corollary 4.22 *Let* $S \in \mathsf{DB}\langle\langle\, K * V^* \,\rangle\rangle, k \in K, u \in X^*$. *Then* $S \odot (k, u) \in \mathsf{DB}\langle\langle\, K * V^* \,\rangle\rangle$.

Lemma 4.23 *Let* $S \in \mathsf{DB}_{1,m}\langle\langle\, K * V^* \,\rangle\rangle, T \in \mathsf{B}_{m,s}\langle\langle\, K * V^* \,\rangle\rangle, u \in X^+$ *and* $U = S \cdot T$. *Exactly one of the following cases is true:*

(1) $S \odot u \notin \{\emptyset^m\} \cup \{k \cdot \epsilon_j^m | k \in K, 1 \leq j \leq m\}$
in this case $U \odot u = (S \odot u) \cdot T$.

(2) $\exists j_0, \exists u', u'', u = u' \cdot u'', \exists k \in K, \rho_\epsilon(S \odot u') = k \cdot \epsilon^m_{j_0}$;
in this case $U \odot u = k \cdot \rho_\epsilon(T_{j_0} \odot u'')$.
(3) $\forall j, \forall u' \preceq u, S \odot u = \emptyset^m$ *and* $\rho_\epsilon(S \odot u') \neq \epsilon^m_j$;
in this case $U \odot u = \emptyset^s = (S \odot u) \cdot T$.

The particular letters $[p, e, q]$ for $p, q \in Q$ play a special role in sections 8 and 9: we use them as *marks* in the series (somehow like the ceilings of [Val74]). We define below a map ρ_e which removes the marks in the series. Let us define $\rho_e : \mathsf{B}\langle\langle\ K * V^*\ \rangle\rangle \longrightarrow \mathsf{B}\langle\langle\ K * V^*\ \rangle\rangle$ as the unique substitution such that:

$$\rho_e([p, e, q]) = \epsilon \quad \text{if } p = q, \quad \rho_e([p, e, q]) = \emptyset \quad \text{if } p \neq q, \quad \rho_e([p, z, q]) = [p, z, q] \quad \text{if } z \neq e.$$

Lemma 4.24 *For every* $S \in \mathsf{DB}\langle\langle\ K * V^*\ \rangle\rangle$, $\rho_e(S) \in \mathsf{DB}\langle\langle\ K * V^*\ \rangle\rangle$ *and* $\|\rho_e(S)\| \leq \|S\|$.

Equivalence on row-vectors Let us consider the componentwise extension of φ to row-vectors. For every $m \in \mathbb{N} - \{0\}, S \in \mathsf{B}_{1,m}\langle\langle\ K * V^*\ \rangle\rangle$ we define $\varphi(S) \in \mathsf{B}_{1,m}\langle\langle\ K * V^*\ \rangle\rangle$ by:

$$\forall j \in [1, m], \varphi(S)_{1,j} = \varphi(S_{1,j}).$$

We then extend $\equiv$ to $\bigcup_{1 \leq m} \mathsf{B}_{1,m}\langle\langle\ K * V^*\ \rangle\rangle$ by: for every $m \in \mathbb{N} - \{0\}, S, S' \in \mathsf{B}_{1,m}\langle\langle\ K * V^*\ \rangle\rangle$

$$S \equiv S' \Leftrightarrow \varphi(S) = \varphi(S'). \tag{34}$$

Let us consider the structured alphabet $(X, \smile)$ where the equivalence $\smile$ is the coarsest one: $\forall x, y \in X, x \smile y$.

Lemma 4.25 *Let* $m \in \mathbb{N} - \{0\}, S \in \mathsf{DB}_{1,m}\langle\langle\ K * V^*\ \rangle\rangle, j \in [1, m]$. *Then*
(1) $\varphi(S) \in \mathsf{DB}_{1,m}\langle\langle\ X^*\ \rangle\rangle$.
(2) $\varphi(S) = \epsilon^m_j \Leftrightarrow \rho_\epsilon(S) = \epsilon^m_j$.

Corollary 4.26 *Let* $m \in \mathbb{N} - \{0\}, S, S' \in \mathsf{DB}_{1,m}\langle\langle\ K * V^*\ \rangle\rangle$. *Then* $S \equiv S'$ *if and only if,* $\forall k \in K, \forall u \in X^*, \forall j \in [1, m]$,

$$\rho_\epsilon(S \odot (k, u)) = \epsilon^m_j \Leftrightarrow \rho_\epsilon(S' \odot (k, u)) = \epsilon^m_j.$$

Definition 4.27 *For every* $m \in \mathbb{N} - \{0\}, S, S' \in \mathsf{DB}_{1,m}\langle\langle\ K * V^*\ \rangle\rangle$ *we define:* $\mathrm{Div}(S, S') = \inf\{|u|, u \in X^*, \exists k \in K, \exists j \in [1, m], \rho_\epsilon(S \odot (k, u)) = \epsilon^m_j \Leftrightarrow \rho_\epsilon(S' \odot (k, u)) \neq \epsilon^m_j\}$.

(We recall that $\inf(\emptyset) = \infty$.)

From corollary 4.26 and definition 4.27 one can see that

$$\mathrm{Div}(S, S') = \infty \Leftrightarrow S \equiv S'. \tag{35}$$

Vectors and their supports In the following we denote by $\odot_{\mathsf{B}}$ the right-action of X^* over $\mathsf{DB}_{1,m}\langle\langle\ V^*\ \rangle\rangle$ defined by the automaton $\mathcal{M}_{\mathsf{B}}$ obtained from $\mathcal{M}$ by sending very element of H on 1. Let us also denote by $\mathrm{Div}_{\mathsf{B}}(S, S')$ the divergence of two series in $\mathsf{DB}_{1,m}\langle\langle\ V^*\ \rangle\rangle$ defined by the action $\odot_{\mathsf{B}}$.

Lemma 4.28 *Let* $m \in \mathbb{N} - \{0\}, \boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathsf{DB}_{1,m}\langle\langle\ K * V^*\ \rangle\rangle$ *and* $S \in \mathsf{DB}_{m,1}\langle\langle\ K * V^*\ \rangle\rangle$ *such that* $\boldsymbol{\alpha} \cdot S \equiv \boldsymbol{\beta} \cdot S$ *and* $\forall j \in [1, m], S_j \not\equiv \emptyset$. *Then*

1. $(\boldsymbol{\alpha} \equiv \boldsymbol{\beta}) \Leftrightarrow (\mathrm{supp}(\boldsymbol{\alpha}) \equiv_{\mathsf{B}} \mathrm{supp}(\boldsymbol{\beta}))$.
2. $\mathrm{Div}(\boldsymbol{\alpha}, \boldsymbol{\beta}) = \mathrm{Div}_{\mathsf{B}}(\mathrm{supp}(\boldsymbol{\alpha}), \mathrm{supp}(\boldsymbol{\beta}))$.

Proof: Point (1) is clearly a consequence of point (2). Let us prove point (2).
Step 1
In a first step, we assume that all vectors $\boldsymbol{\alpha}, \boldsymbol{\beta}, S$ are ϵ-free. Let us suppose that

$$\mathrm{supp}(\boldsymbol{\alpha}) \odot_{\mathsf{B}} u = \epsilon_j^m \Leftrightarrow \mathrm{supp}(\boldsymbol{\beta}) \odot_{\mathsf{B}} u \neq \epsilon_j^m$$

then, there exists $k \in K$ such that

$$\boldsymbol{\alpha} \odot (k, u) = \epsilon_j^m \Leftrightarrow \boldsymbol{\beta} \odot (k, u) \neq \epsilon_j^m.$$

conversely, suppose now that

$$\boldsymbol{\alpha} \odot (k, u) = \epsilon_j^m \text{ while } \boldsymbol{\beta} \odot (k, u) \neq \epsilon_j^m. \tag{36}$$

If $\boldsymbol{\beta} \odot (k, u) = k' \cdot \epsilon_j^m$, for some $k' \in K$, then, by lemma 4.23,

$$S_j \equiv k' \cdot S_j,$$

hence, as $S_j \not\equiv \emptyset$,

$$k' = 1.$$

Hence

$$\boldsymbol{\alpha} \odot (k, u) = \epsilon_j^m \text{ while } (\forall k' \in K, \boldsymbol{\beta} \odot (k, u) \neq k' \cdot \epsilon_j^m). \tag{37}$$

which is also equivalent to

$$\mathrm{supp}(\boldsymbol{\alpha}) \odot_{\mathsf{B}} u = \epsilon_j^m \text{ while } \mathrm{supp}(\boldsymbol{\beta}) \odot_{\mathsf{B}} u \neq \epsilon_j^m. \tag{38}$$

Taking into account the fact that $\boldsymbol{\alpha}, \boldsymbol{\beta}$ play symetric roles, we can conclude that: for every $u \in X^*, j \in [1, m]$

$$\exists k \in K, \boldsymbol{\alpha} \odot (k, u) = \epsilon_j^m \Leftrightarrow \boldsymbol{\beta} \odot (k, u) \neq \epsilon_j^m$$

if and only if

$$\mathrm{supp}(\boldsymbol{\alpha}) \odot_{\mathsf{B}} u = \epsilon_j^m \Leftrightarrow \mathrm{supp}(\boldsymbol{\beta}) \odot_{\mathsf{B}} u \neq \epsilon_j^m.$$

It follows that

$$\mathrm{Div}(\boldsymbol{\alpha}, \boldsymbol{\beta}) = \mathrm{Div}_{\mathsf{B}}(\mathrm{supp}(\boldsymbol{\alpha}), \mathrm{supp}(\boldsymbol{\beta})).$$

Step 2
We consider now the general case where some vector $\boldsymbol{\alpha}, \boldsymbol{\beta}, S$ might be ϵ-bound. By lemma 4.20, point (2),

$$\rho_\epsilon(\boldsymbol{\alpha}), \rho_\epsilon(\boldsymbol{\beta}) \in \mathsf{DB}_{1,m}\langle\langle\ K * V^*\ \rangle\rangle, \rho_\epsilon(S) \in \mathsf{DB}_{m,1}\langle\langle\ K * V^*\ \rangle\rangle$$

and by lemma 4.20, point (3),

$$\boldsymbol{\alpha} \equiv \rho_\epsilon(\boldsymbol{\alpha}), \boldsymbol{\beta} \equiv \rho_\epsilon(\boldsymbol{\beta}), S \equiv \rho_\epsilon(S).$$

One can also check that: for every $\boldsymbol{\gamma} \in \mathsf{DB}_{m,1}\langle\langle\ K * V^*\ \rangle\rangle$

$$\mathrm{supp}(\rho_\epsilon(\gamma)) = \rho_{\mathsf{B},\epsilon}(\mathrm{supp}(\gamma)).$$

Hence the lemma in the general case follows from the lemma in the ϵ-free case. $\Box$

Operations on row-vectors
Let K be a group and $(W, \smile)$ be some structured alphabet. We introduce two new operations on row-vectors and prove some technical lemmas about them.
Given $A, B \in \mathsf{B}_{1,m}\langle\langle\ K*W^*\ \rangle\rangle$ and $1 \leq j_0 \leq m$ we define the vectors $C = A\Box_{j_0}B$ and $A' = \Box^*_{j_0}(A)$ as follows:
if $A = (a_1, \ldots, a_j, \ldots, a_m), B = (b_1, \ldots, b_j, \ldots, b_m)$ then
$C = (c_1, \ldots, c_j, \ldots, c_m)$ where

$$c_j = a_j + a_{j_0} \cdot b_j \text{ if } j \neq j_0\ ,\ \ c_j = \emptyset \text{ if } j = j_0.$$

$A' = (a'_1, \ldots, a'_j, \ldots, a'_m)$ where

$$a'_j = a^*_{j_0} \cdot a_j \text{ if } j \neq j_0\ ,\ \ a'_j = \emptyset \text{ if } j = j_0.$$

Lemma 4.29 *Let $A, B \in \mathsf{B}_{1,m}\langle\langle\ K * W^*\ \rangle\rangle$ and $1 \leq j_0 \leq m$.*

1. *if A, B are deterministic, then $A\Box_{j_0}B$ is deterministic and* $\|A\Box_{j_0}B\| \leq \|A\| + \|B\|$.
2. *if A is deterministic, then $\Box^*_{j_0}(A)$ is deterministic and $\|\Box^*_{j_0}(A)\| \leq \|A\|$.*

4.2 Deterministic spaces

We adapt here the key-idea of [Mei89, Mei92] to series.

Definitions Let $(W, \smile)$ be some structured alphabet and let us consider the set $E = \mathsf{DRB}\langle\langle\ K * W^*\ \rangle\rangle$. A series $U = \sum_{i=1}^{n} \gamma_i \cdot U_i$ where $\boldsymbol{\gamma} \in \mathsf{DRB}_{1,n}\langle\langle\ K * W^*\ \rangle\rangle$, $U_i \in \mathsf{DRB}\langle\langle\ K * W^*\ \rangle\rangle$ is called a *linear combination* of the U_i's. We call *deterministic space* of rational series (d-space for short) any subset V of E which is closed under finite linear combinations. Given any set $\mathcal{G} = \{U_i | i \in I\}$, one can check that the set V of all (finite) linear combinations of elements of $\mathcal{G}$ is a d-space (by lemma 4.9) and that it is the smallest d-space containing $\mathcal{G}$. Therefore we call V the d-space *generated* by $\mathcal{G}$ and we call $\mathcal{G}$ a *generating set* of V (we note $\mathsf{V} = \mathsf{V}(\{U_i | i \in I\})$). (Similar definitions can be given for *families* of series).

We let now $W = V$ and K be an extension of H. Following an analogy with classical linear algebra, we develop now a notion corresponding to a kind of *linear independence* of the images by φ of the given series . Let us extend the equivalence relation $\equiv$ to d-spaces by: for every d-spaces $\mathsf{V}_1, \mathsf{V}_2$, $\mathsf{V}_1 \equiv \mathsf{V}_2 \Leftrightarrow \forall i, j \in \{1,2\}, \forall S \in \mathsf{V}_i, \exists S' \in \mathsf{V}_j, S \equiv S'$.

Lemma 4.30 *Let $S_1, \ldots, S_j, \ldots, S_m \in \mathsf{DRB}\langle\langle\ K * V^*\ \rangle\rangle$. The following are equivalent*

1. $\exists \boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathsf{DRB}_{1,m}\langle\langle\ K * V^*\ \rangle\rangle, \boldsymbol{\alpha} \not\equiv \boldsymbol{\beta}$, *such that*
$$\sum_{1 \le j \le m} \alpha_j \cdot S_j \equiv \sum_{1 \le j \le m} \beta_j \cdot S_j,$$
2. $\exists j_0 \in [1,m], \exists \boldsymbol{\gamma} \in \mathsf{DRB}_{1,m}\langle\langle\ K * V^*\ \rangle\rangle, (\forall k \in K, \boldsymbol{\gamma} \not\equiv k \cdot \epsilon^m_{j_0})$, *such that*
$$S_{j_0} \equiv \sum_{1 \le j \le m} \gamma_j \cdot S_j,$$
3. $\exists j_0 \in [1,m], \exists \boldsymbol{\gamma}' \in \mathsf{DRB}_{1,m}\langle\langle\ K * V^*\ \rangle\rangle, \gamma'_{j_0} \equiv \emptyset$, *such that*
$$S_{j_0} \equiv \sum_{1 \le j \le m} \gamma'_j \cdot S_j,$$
4. $\exists j_0 \in [1,m]$, *such that*
$$\mathsf{V}((S_j)_{1 \le j \le m}) \equiv \mathsf{V}((S_j)_{1 \le j \le m, j \ne j_0}).$$

The equivalence between (1),(2) and (3) was first proved in [Mei89, lemma 11 p.589 [3]], in the case where $H = K = \{1\}$ and the S_j's are configurations $q_j \omega$, with the same ω.

Terminology: a row-vector $\gamma \in \mathsf{DRB}_{1,m}\langle\langle\ K * V^*\ \rangle\rangle$ is said *invertible* iff it is right-invertible i.e. $\exists \gamma' \in \mathsf{DRB}_{m,1}\langle\langle\ K * V^*\ \rangle\rangle$ such that $\gamma \cdot \gamma' = \epsilon$. This condition is equivalent to: $\exists k \in K, j \in [1,m], \gamma = k \cdot \epsilon^m_j$.

Proof:

Let use the notation $S = (S_j)_{1 \le j \le m} \in \mathsf{DRB}_{m,1}\langle\langle\ K * V^*\ \rangle\rangle$.

Step 1

[3] numbering of the english version

In this first step, we assume that all the vectors $\boldsymbol{\alpha}, \boldsymbol{\beta}, S$ are ϵ-free.
$(1) \Rightarrow (2)$**:**
By lemma 4.26 and our ϵ-freeness assumption, we can define a word $u \in X^*$ by:

$$u = \min\{v \in X^*, \exists k \in K, \exists j \in [1,m], \boldsymbol{\alpha} \odot (k,v) = \epsilon_j^m \Leftrightarrow \boldsymbol{\beta} \odot (k,v) \neq \epsilon_j^m\}.$$

Let $j_0 \in [1,m], k \in K$, such that

$$\boldsymbol{\alpha} \odot (k,u) = \epsilon_{j_0}^m \Leftrightarrow \boldsymbol{\beta} \odot (k,u) \neq \epsilon_{j_0}^m.$$

case 1: $S_{j_0} \equiv \emptyset$
In this case, point (2) of the lemma is fulfilled by $\boldsymbol{\gamma} = \emptyset^m$.
case 2: $S_{j_0} \not\equiv \emptyset$
Let us suppose , for example, that

$$\boldsymbol{\alpha} \odot (k,u) = \epsilon_{j_0}^m \text{ while } \boldsymbol{\beta} \odot (k,u) \neq \epsilon_{j_0}^m. \tag{39}$$

As $\equiv$ is preserved by the action $\odot$ (see lemma 2.3):

$$(\boldsymbol{\alpha} \cdot S) \odot (k,u) \equiv (\boldsymbol{\beta} \cdot S) \odot (k,u). \tag{40}$$

Let us examine successively the left-handside and the right-handside of equivalence (40). Using lemma 4.23 we obtain:

$$(\boldsymbol{\alpha} \cdot S) \odot (k,u) = S_{j_0}. \tag{41}$$

Let $u' \prec u$. By minimality of u, $\boldsymbol{\beta} \odot u'$ is invertible iff $\boldsymbol{\alpha} \odot u'$ is invertible. But if $\boldsymbol{\alpha} \odot u'$ is invertible, then $\boldsymbol{\alpha} \odot u = \emptyset^m$, which is false. Hence $\boldsymbol{\beta} \odot u'$ is not invertible. By lemma 4.23, it follows that

$$(\boldsymbol{\beta} \cdot S) \odot (k,u) = (\boldsymbol{\beta} \odot (k,u)) \cdot S. \tag{42}$$

Let us plug equalities (41) and (42) in equivalence (40) and let us define $\boldsymbol{\gamma} = \boldsymbol{\beta} \odot (k,u)$. We obtain:

$$S_{j_0} \equiv \boldsymbol{\gamma} \cdot S. \tag{43}$$

Let us check that $\forall k \in K, \boldsymbol{\gamma} \not\equiv k \cdot \epsilon_{j_0}^m$. Suppose, for sake of contradiction, that:

$$\boldsymbol{\gamma} \equiv k' \cdot \epsilon_{j_0}^m, \text{ where } k' \in K. \tag{44}$$

If (44) is valid, equivalence (43) would lead to:

$$S_{j_0} \equiv k' \cdot S_{j_0},$$

hence, as $S_{j_0} \not\equiv \emptyset$, to $k' = 1$. Equivalence (44) would then read:

$$\boldsymbol{\gamma} \equiv \epsilon_{j_0}^m$$

which, as $\boldsymbol{\gamma}$ is ϵ-free, would imply

$$\boldsymbol{\gamma} = \epsilon_{j_0}^m. \tag{45}$$

But (45) contradicts (39). Hence point (2) of the lemma is fulfilled by $\boldsymbol{\gamma}$.
(2) $\Rightarrow$ (3):

$$S_{j_0} \equiv \gamma_{j_0} \cdot S_{j_0} + (\sum_{j \neq j_0} \gamma_j \cdot S_j), \quad \text{where } \forall k \in K, \gamma_{j_0} \not\equiv k.$$

By rule (K6) of the deduction system $\mathcal{K}_0$ (which is just a natural extension of the well-known Arden's lemma), we can deduce from the above equivalence:

$$S_{j_0} \equiv \sum_{j \neq j_0} \gamma_{j_0}^* \gamma_j \cdot S_j = \Box_{j_0}^*(\gamma) \cdot S.$$

Taking $\gamma' = \Box_{j_0}^*(\gamma)$ we obtain

$$S_{j_0} \equiv \gamma' \cdot S \text{ where } \gamma'_{j_0} = \emptyset.$$

(3) $\Rightarrow$ (4):
Let us denote by $\hat{S}$ the vector $(S_1, \ldots, S_{j_0-1}, S_{j_0+1} \ldots, S_m) \in \mathsf{DB}_{m-1,1}\langle\langle\ K * V^*\ \rangle\rangle$. If $T = \boldsymbol{\alpha} \cdot S$ then $T \equiv (\boldsymbol{\alpha} \Box_{j_0} \boldsymbol{\gamma}') \cdot \hat{S}$.
(4) $\Rightarrow$ (1):
Let us suppose (4) is true for some integer j_0. The element S_{j_0} is clearly equivalent (mod $\equiv$) to two linear combinations of the S_j's with non-equivalent vectors of coefficients (mod $\equiv$). Hence (1) is true.
Step 2
We consider now the general case where some vector $\boldsymbol{\alpha}, \boldsymbol{\beta}, S$ might be ϵ-bound. By lemma 4.20, point (2),

$$\rho_\epsilon(\boldsymbol{\alpha}), \rho_\epsilon(\boldsymbol{\beta}) \in \mathsf{DRB}_{1,m}\langle\langle\ K * V^*\ \rangle\rangle, \rho_\epsilon(S) \in \mathsf{DRB}_{m,1}\langle\langle\ K * V^*\ \rangle\rangle$$

and by lemma 4.20, point (3),

$$\boldsymbol{\alpha} \equiv \rho_\epsilon(\boldsymbol{\alpha}), \boldsymbol{\beta} \equiv \rho_\epsilon(\boldsymbol{\beta}), S \equiv \rho_\epsilon(S).$$

Hence the lemma in the general case follows from the lemma in the ϵ-free case. $\Box$

4.3 Height, defect and linearity

We define here notions of height and defect (for deterministic rational series) and a subsequent notion of (d, d')-linearity which will play a crucial role in section 9. We then relate these "size notions" with the notion of norm.

Definitions Let $S \in \mathsf{DRB}\langle\langle K * V^* \rangle\rangle$. We call *linear decomposition of* S any pair $([p\omega], \Phi)$ where $p \in Q, \omega \in Z^*, \Phi \in \mathsf{DB}_{Q,1}\langle\langle K * V^* \rangle\rangle$ such that

$$S \approx [p\omega] * \Phi.$$

We denote by $\mathcal{D}(S)$ the set of all linear decompositions of S. We define the *right-defect* of S ($\mathrm{rd}(S)$ in short) by

$$\mathrm{rd}(S) = \min\{\|\Phi\| \mid \exists p \in Q, \omega \in Z^*, ([p\omega], \Phi) \in \mathcal{D}(S)\}.$$

One can easily see that the right-defect of S is finite and not greater than $\|S\|$. We call *minimal* decomposition of S any decomposition $([p_0\omega_0], \Phi_0)$ which makes the triple $(p, |\omega|, \|\Phi\|)$ minimal for the right-to-left lexicographic ordering in $Q \times \mathbb{N} \times \mathbb{N}$ [4]. We then define the *linear-height* of S (noted $|S|$) as the integer $|S| = |\omega_0|$ (and it is clear that $\mathrm{rd}(S) = \|\Phi_0\|$).
The height and right-defect of a Q-form can be defined similarly. We say that S is *marked* iff S contains some occurrence of some letter $[p, e, q] \in V$ (we assumed the existence of such a "dummy " letter e in Z in section 2.3).

Definition 4.31 *Let $S \in \mathsf{DRB}\langle\langle K * V^* \rangle\rangle$ and $d' \in \mathbb{N}$.*

1. *S is said $(0, d')$-linear iff $\mathrm{rd}(S) \leq d'$ and S is not marked*
2. *if $d \in \mathbb{N} - \{0\}$, S is said (d, d')-linear iff it is $(0, d')$-linear or it has a decomposition $S \approx \sum_{q \in Q}[phq] \cdot [qeq] \cdot \Phi_q$ where every Φ_q is a $(0, d')$-linear series and $|h| \leq d$.*

In case (2) we call the series Φ_q the d'-linear components of S. In case (1) we consider that S itself is the unique d'-linear component of S. It should be clear that the d'-linear components are independent of the value of d (for d large enough) and that the set of d'-linear components is uniquely defined. We denote by $\mathsf{DBlin}^{d'}\langle\langle K * V^* \rangle\rangle$ (resp. $\mathsf{DRBlin}^{d'}\langle\langle K * V^* \rangle\rangle$) the set of series in $\mathsf{DB}\langle\langle K * V^* \rangle\rangle$ (resp. $\mathsf{DRB}\langle\langle K * V^* \rangle\rangle$) which are $(0, d')$-linear.
Examples:
No series can be $(0-0)$-linear. S is $(0, 1)$-linear iff $S = \emptyset$. S is $(0, 2)$-linear iff it has the form $S \approx \sum_{q \in Q'}[p\omega q]$ for some $p \in Q, Q' \subseteq Q, \omega \in (Z - \{e\})^*$.
Hence one can view the $(0, d)$-linear series as series which have a structure " not too far" from the *linear* structure of the configurations of the initial H-dpda $\mathcal{M}$.
(We illustrate on figure 1 the above definitions).

4.4 Height and norm

Lemma 4.32 *Let $S \in \mathsf{DRB}\langle\langle K * V^* \rangle\rangle, x \in X, d, d' \in \mathbb{N}, k \in K$.*

1. $\mathrm{rd}(S \odot x) \leq \mathrm{rd}(S)$,
2. *S is (d, d')-linear $\Rightarrow$ $S \odot x$ is $(d + 1, d')$-linear,*
3. $\|S \odot x\| \leq \|S\| + |Q|$,
4. $\|k \cdot S\| = \|S\|$.

[4] non-unicity can occur for this minimal decomposition only in case $|\omega| = 0$

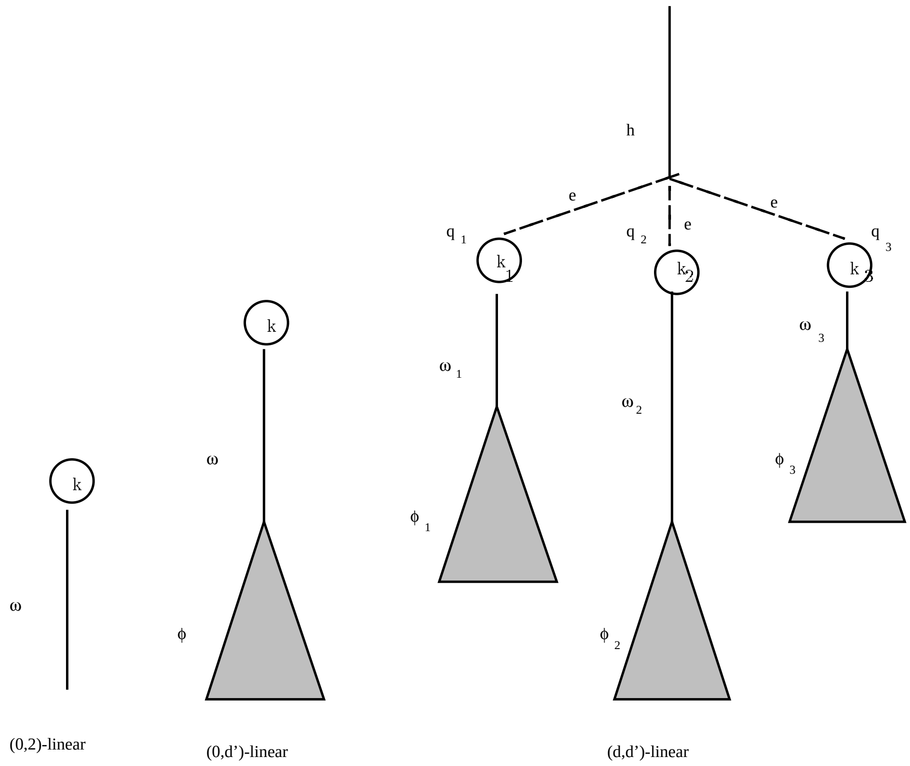

Fig. 1. (d, d')-linearity.

Here $|Q|$ denotes the cardinality of the set Q.

Lemma 4.33 *Let $\omega \in Z^+, A', A \in Z, p \in Q$, $\Phi \in \mathsf{DB}_{Q,1}\langle\langle\, K * V^* \,\rangle\rangle$. If $\|[A] * \Phi\| > \|\Phi\|$, then $\|[\omega A] * \Phi\| = |Q| \cdot |\omega| + \|[A] * \Phi\|$ and $\|[pA'\omega A] * \Phi\| = 1 + |Q| \cdot |\omega| + \|[A] * \Phi\|$.*

The following lemma serves as a crucial technical argument in section 9.

Lemma 4.34 *Let $U = [ph] * \Phi, U' = U \odot u$ where $p \in Q, h \in Z^*, |h| \geq 1, \Phi$ is a $Q-$ form , $|\Phi| \geq 1, u \in X^*, |u| \leq k$. Let us suppose that $\|U'\| \geq 1 + k \cdot |Q| + \|\Phi\|$. Then*
$U' \approx ([ph] \odot u) * \Phi$ where $[ph] \odot u \approx [q\omega]$ for some $q \in Q, |\omega| \geq k$.

Intuitive meaning: If U is a deterministic rational series admitting a decomposition over the Q-form Φ and, $U \odot u$ has a sufficiently large norm (compared to $\|\Phi\|$ and $|u|$), then the action of u on U cannot have "touched" the form Φ.

4.5 Derivations

A sequence of deterministic series $S_0, S_1, \ldots, S_n$ is a *derivation* iff there exist $x_1, \ldots, x_n \in X$ such that $S_0 \odot x_1 = S_1, \ldots, S_{n-1} \odot x_n = S_n$. If $u = x_1 \cdot x_2 \cdot \ldots \cdot x_n$ we call $S_0, S_1, \ldots, S_n$ the derivation *associated* with (S, u).
For every $u \in X^*$ we define the binary relation $\uparrow (u)$ over $\mathsf{DB}\langle\langle\, K * V^* \,\rangle\rangle$ by: for every $S, S' \in \mathsf{DB}\langle\langle\, K * V^* \,\rangle\rangle, S \uparrow (u) S' \Leftrightarrow \exists A \in Z, \omega \in Z^+, p, q \in Q, \Phi \in \mathsf{DB}_{Q,1}\langle\langle\, K * V^* \,\rangle\rangle, h_1 \in K, h_2 \in H$ such that

$$S = h_1 \cdot [pA] * \Phi, \ \ [pA] \odot u = h_2 \cdot [q\omega], \ \ S' = (h_1 \cdot h_2) \cdot [q\omega] * \Phi.$$

A derivation $S_0, S_1, \ldots, S_n$ is said to be *stacking* iff it is the derivation associated to a pair (S, u) such that $S = S_0$ and $S_0 \uparrow (u) S_n$.

5 Deduction systems

5.1 General deduction systems

We follow here the general philosophy of [HHY79, Cou83]. Let us call *deduction system* any triple

$$\mathcal{D} = < \mathcal{A}, J, \vdash\!\!- >$$

where $\mathcal{A}$ is a denumerable set called the *set of assertions*, J, the *cost function* is a mapping $\mathcal{A} \rightarrow \mathbb{N} \cup \{\infty\}$ and $\vdash\!\!-$, the *deduction relation* is a subset of $\mathcal{P}_f(\mathcal{A}) \times \mathcal{A}$; $\mathcal{A}$ is given with a fixed bijection with $\mathbb{N}$ (an "encoding" or "Gödel numbering") so that the notions of recursive subset, recursively enumerable subset, recursive function, ... over $\mathcal{A}, \mathcal{P}_f(A)$,... are defined, up to this fixed bijection ; we assume that $\mathcal{D}$ satisfies the following axioms:
(A 1) $\vdash\!\!-$ is recursively enumerable
(A 2) $\forall (P, A) \in \vdash\!\!-$, $(\inf\{J(p), p \in P\} < J(A))$ or $(J(A) = \infty)$.
We use here the well-ordered set $\mathbb{N}_\infty = \mathbb{N} \cup \{\infty\}$ which is obtained by adding a maximum element ∞ to the set of natural integers $\mathbb{N}$. We recall that $\inf(\emptyset) = \infty$.The operation $+$ is defined as the extension of the usual addition over $\mathbb{N}$ by:

$$\forall x \in \mathbb{N}_\infty, x + \infty = \infty + x = \infty.$$

In the sequel we use the notation $P \vdash\!\!- A$ for $(P, A) \in \vdash\!\!-$. We call *proof* in the system $\mathcal{D}$, *relative to the set of hypotheses* $\mathcal{H} \subseteq \mathcal{A}$, any subset $P \subseteq \mathcal{A}$ fulfilling : $\forall p \in P, (\exists Q \subseteq P, Q \vdash\!\!- p)$ or $(p \in \mathcal{H})$. We call P a *proof* iff $\forall p \in P, (\exists Q \subseteq P, Q \vdash\!\!- p)$ (i.e. iff P is a proof relative to $\emptyset$).
We think of an assertion A such that $J(A) = \infty$ as a *true* assertion while we think of an assertion A such that $J(A) < \infty$ as a *false* assertion where the *cost* necessary to discover a *witness* of its falsity is the number $J(A)$ (this was the general idea exposed in [Cou83, p.193]).

Lemma 5.1 *Let P be a proof relative to $\mathcal{H} \subseteq J^{-1}(\infty)$ and $A \in P$. Then $J(A) = \infty$.*

In other words : if an assertion is provable from true hypotheses, then it is true.

Lemma 5.2 *: Let $\mathcal{D}$ be a deduction system. Then, the set of finite $\mathcal{D}$-proofs is recursively enumerable.*

In order to define deduction relations from more elementary ones, we set the following definitions. Let $\vdash\!\!- \subseteq \mathcal{P}_f(\mathcal{A}) \times \mathcal{A}$. For every $P, Q \in \mathcal{P}_f(\mathcal{A})$ we set:
$P \overset{[0]}{\vdash\!\!-} Q$ iff $P \supseteq Q$; $P \overset{[1]}{\vdash\!\!-} Q$ iff $\forall q \in Q, \exists R \subseteq P, R \vdash\!\!- q$; $P \overset{<0>}{\vdash\!\!-} Q$ iff $P \overset{[0]}{\vdash\!\!-} Q$; $P \overset{<1>}{\vdash\!\!-} Q$ iff $\forall q \in Q, (\exists R \subseteq P, R \vdash\!\!- q)$ or $(q \in P)$; $P \overset{<n+1>}{\vdash\!\!-} Q$ iff $\exists R \in \mathcal{P}_f(A), P \overset{<1>}{\vdash\!\!-} R$ and $R \overset{<n>}{\vdash\!\!-} Q$ (for every $n \geq 0$).; $\overset{<*>}{\vdash\!\!-} = \bigcup_{n \geq 0} \overset{<n>}{\vdash\!\!-}$.
Given $\vdash\!\!-_1, \vdash\!\!-_2 \subseteq \mathcal{P}_f(\mathcal{A}) \times \mathcal{P}_f(\mathcal{A})$, for every $P, Q \in \mathcal{P}_f(\mathcal{A})$ we set : $P(\vdash\!\!-_1 \circ \vdash\!\!-_2)Q$ iff $\exists R \subseteq \mathcal{A}, (P \vdash\!\!-_1 R) \wedge (R \vdash\!\!-_2 Q)$.

5.2 Systems $\mathcal{K}_0, \mathcal{H}_0$ †

Let $(H,\cdot),(K,\cdot)$ be two groups, with $H < K$ (i.e. H is a subgroup of K), such that K has a denumerable set of generators and a decidable word-problem. We define here a particular deduction system $\mathcal{H}_0$ "Taylored for the equivalence problem for H-dpda's" and also an auxiliary more general deduction system $\mathcal{K}_0$.

Given a fixed H-dpda $\mathcal{M}$ over the terminal alphabet X, we consider the variable alphabet V associated to $\mathcal{M}$ (see §2.4), a denumerable alphabet U (we call it the alphabet of *parameters*), the group $K = \mathrm{F}(U) * H$ and the set $\mathsf{DRB}\langle\langle\ K * V^*\ \rangle\rangle$ (the set of Deterministic Rational Boolean series over $K * V^*$).
The set of assertions is defined by :

$$\mathcal{A} = \mathbb{N} \times \mathsf{DRB}\langle\langle\ K * V^*\ \rangle\rangle \times \mathsf{DRB}\langle\langle\ K * V^*\ \rangle\rangle$$

i.e. an assertion is here a *weighted equation* over $\mathsf{DRB}\langle\langle\ K * V^*\ \rangle\rangle$.
The "cost-function" $J : \mathcal{A} \to \mathbb{N} \cup \{\infty\}$ is defined by :

$$J(n, S, S') = n + 2 \cdot \mathrm{Div}(S, S').$$

(We recall $\mathrm{Div}(S, S')$ is introduced in definition 4.27). Let us notice that:

$$J(n, S, S') = \infty \Longleftrightarrow S \equiv S'.$$

We define a binary relation $|\!\!\vdash\!\!- \subset \mathcal{P}_f(\mathcal{A}) \times \mathcal{A}$, the *elementary deduction relation*, as the set of all the pairs having one of the following forms:

(K0)

$$\{(p, S, T)\} \;|\!\!\vdash\!\!-\; (p+1, S, T)$$

for $p \in \mathbb{N}, S, T \in \mathsf{DRB}\langle\langle\ K * V^*\ \rangle\rangle$,

(K1)

$$\{(p, S, T)\} \;|\!\!\vdash\!\!-\; (p, T, S)$$

for $p \in \mathbb{N}, S, T \in \mathsf{DRB}\langle\langle\ K * V^*\ \rangle\rangle$,

(K2)

$$\{(p, S, S'), (p, S', S'')\} \;|\!\!\vdash\!\!-\; (p, S, S'')$$

for $p \in \mathbb{N}, S, S', S'' \in \mathsf{DRB}\langle\langle\ K * V^*\ \rangle\rangle$,

(K3)

$$\emptyset \;|\!\!\vdash\!\!-\; (0, S, S)$$

for $S \in \mathsf{DRB}\langle\langle\ K * V^*\ \rangle\rangle$,

(K'3)

$$\emptyset \;|\!\!\vdash\!\!-\; (0, S, T)$$

for $S \in \mathsf{DRB}\langle\langle\ K * V^*\ \rangle\rangle, T \in \{\emptyset, \epsilon\}, S \equiv T$,

(K4)

$$\{(p+1, S \odot x, T \odot x) \mid x \in X\} \;|\!\!\vdash\!\!-\; (p, S, T)$$

for $p \in \mathbb{N}, S, T \in \mathsf{DRB}\langle\langle\ K * V^*\ \rangle\rangle, (\forall k \in K, S \not\equiv k \wedge T \not\equiv k)$,

(K5)

$$\{(p, S, S')\} \mid\!\vdash\!\!- (p+2, S \odot x, S' \odot x)$$

for $p \in \mathbb{N}, S, T \in \mathsf{DRB}\langle\langle\ K * V^*\ \rangle\rangle, x \in X$,

(K6)

$$\{(p, S \cdot T' + S', T')\} \mid\!\vdash\!\!- (p, S^* \cdot S', T')$$

for $p \in \mathbb{N}, (S, S') \in \mathsf{DRB}_{1,2}\langle\langle\ K * V^*\ \rangle\rangle, T' \in \mathsf{DRB}\langle\langle\ K * V^*\ \rangle\rangle, (\forall k \in K, S \not\equiv k)$,

(K7)

$$\{(p, S, S'), (p, T, T')\} \mid\!\vdash\!\!- (p, S + T, S' + T')$$

for $p \in \mathbb{N}, (S, T), (S', T') \in \mathsf{DRB}_{1,2}\langle\langle\ K * V^*\ \rangle\rangle$,

(K8)

$$\{(p, S, S')\} \mid\!\vdash\!\!- (p, S \cdot T, S' \cdot T)$$

for $p \in \mathbb{N}, S, S', T \in \mathsf{DRB}\langle\langle\ K * V^*\ \rangle\rangle$,

(K9)

$$\{(p, T, T')\} \mid\!\vdash\!\!- (p, S \cdot T, S \cdot T')$$

for $p \in \mathbb{N}, S, T, T' \in \mathsf{DRB}\langle\langle\ K * V^*\ \rangle\rangle$,

(K10)

$$\emptyset \mid\!\vdash\!\!- (0, S, \rho_\epsilon(S))$$

for $S \in \mathsf{DRB}\langle\langle\ K * V^*\ \rangle\rangle$,

(K11)

$$\emptyset \mid\!\vdash\!\!- (0, S, \rho_e(S))$$

for $S \in \mathsf{DRB}\langle\langle\ K * V^*\ \rangle\rangle$.

Though we did not prove this result formally, it should be clear that the operations $+, \cdot, \Box_1^*, \rho_\epsilon$ and ρ_e over $\mathsf{DRB}_{1,m}\langle\langle\ K * V^*\ \rangle\rangle$ correspond to some computable functions on deterministic finite m-K-automata and that the equality in $\mathsf{DRB}_{1,m}\langle\langle\ K * V^*\ \rangle\rangle$ corresponds to some computable predicate on pairs of deterministic finite m-K-automata (i.e. the equivalence problem for deterministic finite m-K-automata is decidable [5]). Hence, modulo an encoding of $\bigcup_{m \geq 1} \mathsf{DRB}_{1,m}\langle\langle\ K * V^*\ \rangle\rangle$ into integers, based on deterministic finite m-K-automata, the above set of rules is recursively enumerable. Let us define $\vdash\!\!-$ by : for every $P \in \mathcal{P}_f(\mathcal{A}), A \in \mathcal{A}$,

$$P \vdash\!\!- A \Longleftrightarrow P \overset{<*>}{\mid\!\vdash\!\!-} \circ \overset{[1]}{\mid\!\vdash\!\!-}_{0,3,4,10,11} \circ \overset{<*>}{\mid\!\vdash\!\!-} \{A\},$$

where $\mid\!\vdash\!\!-_{0,3,4,10,11}$ is the relation defined by $K0, K3, K'3, K4, K10, K11$ only. We let

$$\mathcal{K}_0 =< \mathcal{A}, J, \vdash\!\!- > .$$

We define $\mathcal{H}_0$ as the system obtained by replacing K by H in the above definitions.

[5] this property is true as soon as K has a decidable word-problem, which was assumed in this subsection

Lemma 5.3 *: $\mathcal{K}_0, \mathcal{H}_0$ are deduction systems.*

$\mathcal{K}_0$ is "compatible with homomorphisms" in the following sense

Lemma 5.4 *For every $P \in \mathcal{P}(\mathcal{A}), q \in \mathcal{A}$ and every homomorphism $\psi \in \mathrm{Hom}_H(K, K)$, if $P \models\!\!- q$ then $\psi(P) \models\!\!- \psi(q)$.*

(We recall that $\mathrm{Hom}_H(K, K)$ is the set of homomorphisms $\psi : K \to K$ which leave H pointwise invariant: $\forall x \in H, \psi(x) = x$.)

Corollary 5.5 *For every $P \in \mathcal{P}(\mathcal{A})$ and every homomorphism $\psi \in \mathrm{Hom}_H(K, K)$, if P is a $\mathcal{K}_0$-proof then $\psi(P)$ is a $\mathcal{K}_0$-proof too.*

For every integer $t \in \mathbb{N}$, we denote by $\tau_t : \mathcal{A} \to \mathcal{A}$ the translation on the weights:

$$\forall p \in \mathbb{N}, S, T \in \mathsf{DRB}\langle\langle\ K * V^*\ \rangle\rangle, \tau_t(p, S, T) = (p + t, S, T).$$

5.3 Regular proofs †

In this subsection, we fix $H = \mathrm{GL}_n(\mathbb{Q}), K = \mathrm{F}(U) * H$, where $n \in \mathbb{N}$, U is the set of parameters (see §4.1).
We introduce a notion of *regular* proof. Such proofs might be infinite but exhibit some regularities which make them resemble on one hand regular trees (in the usual sense) and on the other hand , DTOL languages (see §3.1). Such proofs are completely described by finite structures that we call *germs of proofs* (definition 5.9) and the set of germs of proofs is *recursively enumerable* (proposition 5.13).

Let us use the notation $\mathrm{Par}(S) \subseteq U$ for the set of parameters occuring in a given series S. The notation is extended to assertions and sets of assertions in the natural way: if $p = (\pi, S, T)$, and $P \subseteq \mathcal{A}$,

$$\mathrm{Par}(p) = \mathrm{Par}(S) \cup \mathrm{Par}(T),\ \ \mathrm{Par}(P) = \bigcup_{p \in P} \mathrm{Par}(p).$$

Definition 5.6 (germs) *We call a H-germ any 9-tuple $G = (n, \alpha, \beta, \gamma, (P_i)_{0 \le i \le n}, (A_i)_{0 \le i \le n}, (B_{i,j})_{0 \le i \le n, 0 \le j \le \alpha(i)}, (C_{i,k})_{0 \le i \le n, 0 \le k \le \beta(i)}, (\psi_{i,j})_{0 \le i \le n, 0 \le j \le \alpha(i)})$ such that*

1. *n is a non-negative integer,*
2. *α, β are two integer mappings: $[0, n] \to \mathbb{N}$,*
3. *γ is a mapping: $\{(i, j) \in \mathbb{N} \times \mathbb{N} \mid 0 \le i \le n, 0 \le j \le \alpha(n)\} \to [0, n]$,*
4. *every P_i is a finite subset of $\mathcal{A}$,*
5. *$A_i, B_{i,j}, C_{i,k}$ are assertions belonging to P_i ,*
6. *let $U_i = \mathrm{Par}(A_i)$, $U_G = \cup_{0 \le i \le n} U_i, K_G = \mathrm{F}(U_G) * H$; $U_0 = \emptyset$ and every assertion of P_i belongs to $\mathbb{N} \times \mathsf{DRB}\langle\langle\ K_i * V^*\ \rangle\rangle \times \mathsf{DRB}\langle\langle\ K_i * V^*\ \rangle\rangle$*
7. *every assertion $C_{i,k}$ has the form:*

$$C_{i,k} = (\pi_{i,k}, S_{i,k}, T_{i,k})$$

where $\mathrm{supp}(S_{i,k}) = \mathrm{supp}(T_{i,k}) = \epsilon$, *8.* $A_i \notin \{B_{i,j} \mid 0 \leq j \leq \alpha(i)\} \cup \{C_{i,k} \mid 0 \leq k \leq \beta(i)\}$,

9. P_i *is a proof relative to the set of hypotheses* $\{B_{i,j} \mid 0 \leq j \leq \alpha(i)\} \cup \{C_{i,k} \mid 0 \leq k \leq \beta(i)\}$,

10. $\psi_{i,j} \in \mathrm{Hom}_H(K_{\gamma(i,j)}, K_i)$ *and there exists some non-negative integer* $t \in \mathbb{N}$ *such that*

$$\tau_t(\psi_{i,j}(A_{\gamma(i,j)})) = B_{i,j}.$$

Definition 5.7 (rational sets of homomorphisms) *Let G be a H-germ defined as in definition 5.6. We define rational subsets $(\mathcal{R}_i)_{0\leq i\leq n}$ of $\mathrm{Hom}_H(K, K)$ by*

$$\mathcal{R}_i = \{\psi_{i_0,j_0} \circ \psi_{i_1,j_1} \cdots \circ \psi_{i_\ell,j_\ell} \mid i_0 = 0, \ell \geq 0, \forall k \in [0, \ell], 0 \leq j_k \leq \alpha(i_k),$$
$$\forall k \in [0, \ell - 1] i_{k+1} = \gamma(i_k, j_k) \text{ and } i = \gamma(i_\ell, j_\ell)\}.$$

Definition 5.8 *Let G be a H-germ. We define the* set of assertions *associated with G, as the set:*

$$\mathsf{P}(G) = \bigcup_{\substack{\psi_i \in \mathcal{R}_i \\ 0 \leq i \leq n}} \psi_i(P_i).$$

Definition 5.9 (germs of proofs) *Let G be a H-germ. G is called a* germ of proof *iff, for every $i \in [0, n], k \in [0, \beta(i)], \psi_i \in \mathcal{R}_i$,*

$$\psi_i(S_{i,k}) = \psi_i(T_{i,k}).$$

(We recall the assertions $S_{i,k}, T_{i,k}$ are part of the definition of G, see definition 5.6, point (7)).

Lemma 5.10 *Let G be a H-germ. For every $i \in [0, n], \psi_i \in \mathcal{R}_i$ and every parameter $u \in U_i$,*

$$\psi_i(u) \in H.$$

Proof: Let us consider some $i \in [0, n]$, some $u \in U_i$ and some morphism:

$$\psi_i = \psi_{i_0,j_0} \circ \psi_{i_1,j_1} \cdots \circ \psi_{i_\ell,j_\ell}$$

where $i_0 = 0, \ell \geq 0, (\forall k \in [0, \ell], 0 \leq j_k \leq \alpha(i_k), \forall k \in [0, \ell-1] i_{k+1} = \gamma(i_k, j_k))$ and $i = \gamma(i_\ell, j_\ell)$. By point (10) of definition 5.6, one can prove by induction on $\ell - k$ that, for every $0 \leq k \leq \ell$:

$$\mathrm{Par}(\psi_{i_k,j_k} \circ \cdots \circ \psi_{i_\ell,j_\ell}(u)) \subseteq U_{i_k}. \tag{46}$$

Taking $k = 0$ in statement (46) and using the fact that $i_0 = 0$ and $U_0 = \emptyset$ (point (6) of definition 5.6) we obtain:

$$\mathrm{Par}(\psi_i(u)) = \emptyset, \tag{47}$$

hence $\psi_i(u) \in H$. $\square$

Lemma 5.11 *Let G be a H-germ. If G is a germ of proof, then $\mathsf{P}(G)$ is a $\mathcal{H}_0$-proof.*

Proof: Let G be a germ of proof.
1 Let us prove that $\mathsf{P}(G)$ is a $\mathcal{K}_0$-proof.
Let $p \in \mathsf{P}(G)$. There exists some $i \in [0, n], \psi_i \in \mathcal{R}_i$ such that $p \in \psi_i(P_i)$. Let $p_i \in P_i$ such that

$$p = \psi_i(p_i),$$

and let us consider a decomposition

$$\psi_i = \psi_{i_0,j_0} \circ \psi_{i_1,j_1} \cdots \circ \psi_{i_\ell,j_\ell} \tag{48}$$

satisfying the conditions of definition 5.7. We distinguish 3 cases and show that, in every case,

$$\mathsf{P}(G) \mid\!\!\!-\!\!- \, p \tag{49}$$

case 1 $p_i \in P_i - \{B_{i,j} \mid 0 \leq j \leq \alpha(i)\} - \{C_{i,k} \mid 0 \leq j \leq \beta(i)\}$.
As P_i is a proof with hypothesis $\{B_{i,j} \mid 0 \leq j \leq \alpha(i)\} \cup \{C_{i,k} \mid 0 \leq j \leq \beta(i)\}$,

$$P_i \mid\!\!\!-\!\!- \, p_i.$$

By lemma 5.4, it follows that

$$\psi_i(P_i) \mid\!\!\!-\!\!- \, \psi_i(p_i),$$

which, as $\mathsf{P}(G) \supseteq \psi_i(P_i)$, implies (49).
case 2 $p_i = B_{i,j}$, for some $j \in [0, \alpha(i)]$.
Let us define

$$i' = \gamma(i,j), \tag{50}$$
$$\psi_{i'} = \psi_i \circ \psi_{i,j} \tag{51}$$

By point (10) of definition 5.6, there exists $t \in \mathbb{N}$ such that

$$\tau_t(\psi_{i,j}(A_{\gamma(i,j)})) = B_{i,j},$$

hence, by left-composition with ψ_i:

$$\tau_t(\psi_{i'}(A_{i'})) = \psi_i(B_{i,j}) = p.$$

By lemma 5.4,

$$\psi_{i'}(P_{i'}) \mid\!\!\!-\!\!- \, \psi_{i'}(A_{i'}), \tag{52}$$

and by $(K0)$ we have

$$\psi_{i'}(A_{i'}) \overset{<*>}{|\!\vdash\!\!-} \tau_t(\psi_{i'}(A_{i'})) = p. \tag{53}$$

By composition of (52) and (53) we obtain:

$$\psi_{i'}(P_{i'}) \vdash\!\!- p. \tag{54}$$

As $\gamma(i_\ell, j_\ell) = i$ (because decomposition (48) satisfies definition 5.7) and $\gamma(i,j) = i'$ (by (50)), we know that

$$\psi_{i'} \in \mathcal{R}_{i'}. \tag{55}$$

By (55) $\mathsf{P}(G) \supseteq \psi_{i'}(P_{i'})$ and by (54), (49) is proved.
case 3 $p_i = C_{i,k}$, for some $k \in [0, \beta(i)]$.
Hence $p = (\pi_{i,k}, S_{i,k}, T_{i,k})$ and, by definition 5.9

$$\psi_i(S_{i,k}) = \psi_i(T_{i,k}).$$

By rule $(K3)$ we get that $\emptyset \vdash\!\!- p$, which implies (49).
2 Let us prove that G is a $\mathcal{H}_0$-proof.
By point (1) of this proof, $\mathsf{P}(G)$ is a $\mathcal{K}_0$-proof and by lemma 5.10 all the assertions of $\mathsf{P}(G)$ contain no parameter, hence $\mathsf{P}(G)$ is a $\mathcal{H}_0$-proof. □

Definition 5.12 (regular proofs) *Let $P \subseteq \mathbb{N} \times \mathsf{DRB}\langle\langle\, H * V^* \,\rangle\rangle \times \mathsf{DRB}\langle\langle\, H * V^* \,\rangle\rangle$. P is called a* regular *proof iff there exists some germ of proof G such that $P = \mathsf{P}(G)$.*

(Lemma 5.11 shows that regular proofs are indeed $\mathcal{H}_0$-proofs).

Lemma 5.13 *The set of all germs of proof is recursively enumerable.*

Proof:
1 Let G be a H-germ. Let us show that one can decide whether G is a germ of proof or not.
By points (5,6,7) of definition 5.6, every $S_{i,j}, T_{i,j}$ are elements of the group $K_i \subseteq K_G$. Let us fix some $i \in [0,n]$ and let us consider the subset L_i of K_G defined by:

$$L_i = \{\psi_i(S_{i,j} T_{i,j}^{-1}) \mid \psi_i \in \mathcal{R}_i\}.$$

Let us notice that the condition of definition 5.9 is equivalent to

$$L_i = \{1_K\}. \tag{56}$$

Let us consider $\mathbf{1}_G \in \mathrm{Hom}(K_G, H)$, $\Pi_G \in \mathrm{Hom}(K_G, H)$ defined by:

$$\forall x \in K_G, \mathbf{1}_G(x) = 1_H, \;\; \forall u \in U_G, \Pi_G(u) = 1_H, \;\; \forall h \in H, \Pi_G(h) = h.$$

By lemma 5.10 every $\psi_i \in \mathcal{R}_i$ maps K_i into H. Hence (56) is equivalent to

$$\forall x \in L_i, \mathbf{1}_G(x) = \Pi_G(x). \tag{57}$$

For every $\psi_{i,j} \in \mathrm{Hom}_H(K_{\gamma(i,j)}, K_i)$ we consider an extension $\tilde{\psi}_{i,j} \in \mathrm{Hom}_H(K_G, K_G)$ defined by $\forall u \in U_G - U_{\gamma(i,j)}, \tilde{\psi}_{i,j}(u) = 1_H$ and let us define $\tilde{\mathcal{R}}_i$ by the same formula as in definition 5.7 where every $\psi_{i,j}$ is replaced by the corresponding $\tilde{\psi}_{i,j}$.

$$L_i = \{\psi_i(S_{i,j}T_{i,j}^{-1}) \mid \psi_i \in \tilde{\mathcal{R}}_i\},$$

hence L_i is a morphic subset of the finitely generated monoid K_G. By theorem 3.5, L_i has a test-set F_i with respect to H and F_i can be computed. Hence (57) reduces to the finite set of verifications:

$$\forall x \in F_i, \mathbf{1}_G(x) = \Pi_G(x). \tag{58}$$

Hence one can test whether G is a germ of proof or not.
2 As the set of finite $\mathcal{K}_0$-proofs is recursively enumerable (lemma 5.2), the set of H-germs is recursively enumerable and, by part (1) of this proof, the set of germs of proofs is recursively enumerable too. □

5.4 Strategies

The key-statement of this work is that, when $H = \mathrm{GL}_n(\mathbb{Q})$, every true assertion $A \in \mathbb{N} \times \mathsf{DRB}\langle\langle\, H * V^* \,\rangle\rangle \times \mathsf{DRB}\langle\langle\, H * V^* \,\rangle\rangle$ (i.e. a true assertion which contains no occurence of parameter) has a regular $\mathcal{H}_0$-proof (theorem 10.3), which is a kind of completeness property for the deduction system $\mathcal{H}_0$. We prove this completeness result by exhibiting a "strategy" $\mathcal{S}$ which, for every true assertion (π, S, S') without parameters, constructs a regular $\mathcal{H}_0$-proof of this assertion.

General definitions Let $\mathcal{D} = < \mathcal{A}, H, \mid\!\!-\!\!- >$ be a deduction system. We call a *strategy* for $\mathcal{D}$ any partial map $\mathcal{S} : \mathcal{A}^+ \to \mathcal{A}^*$ such that :
(S1) if $\mathcal{S}(A_1 A_2 \cdots A_n) = B_1 \cdots B_m$ then

$$\{B_j \mid 1 \le j \le m\} \cup \{A_i \mid 1 \le i \le n-1\} \mid\!\!-\!\!- A_n,$$

(S2) if $\mathcal{S}(A_1 A_2 \cdots A_n) = B_1 \cdots B_m$ then

$$\inf\{J(A_i) \mid 1 \le i \le n\} = \infty \Longrightarrow \inf\{J(B_j) \mid 1 \le j \le m\} = \infty.$$

Given a strategy $\mathcal{S}$, we define $\mathcal{T}(\mathcal{S}, A)$, the proof-tree associated to the strategy $\mathcal{S}$ and the assertion A as the unique tree t such that :
$\varepsilon \in dom(t)$, $t(\varepsilon) = A$, and, for every path $x_0 x_1, \cdots x_{n-1}$ in t, with labels $t(x_i) = A_{i+1}$ (for $0 \le i \le n-1$) if x_{n-1} has m sons $x_{n-1} \cdot 1, \cdots . x_{n-1} \cdot m \in \mathrm{dom}(t)$ with labels $t(x_{n-1} \cdot j) = B_j$ (for $1 \le j \le m$) then

$$\begin{aligned}
&(\forall i \in [1, n-1], A_i \neq A_n \ \text{ and } \ \mathcal{S}(A_1 \cdots A_n) = B_1 \cdots B_m) \text{ or}\\
&(\exists i \in [1, n-1], A_i = A_n \ \text{ and } \ m = 0) \text{ or}\\
&\quad (A_1 \cdots A_n \notin \mathrm{dom}(\mathcal{S}) \ \text{ and } \ m = 0).
\end{aligned} \tag{59}$$

(Notice that "x_{n-1} is a leaf" $\Leftrightarrow m = 0 \Leftrightarrow (\mathcal{S}(A_1 \cdots A_n) = \varepsilon$ or $\exists i \in [\,1\,,\ n-1\,], A_i = A_n$ or $A_1 \cdots A_n \notin dom(\mathcal{S})))$.
We call x_{n-1} an *open* leaf of the proof-tree iff

$$\forall i \in [1, n-1], A_i \neq A_n \text{ and } A_1 \cdots A_n \notin dom(\mathcal{S}),$$

and we call it a *closed* leaf otherwise.
(Notice that this notion of open (resp. closed) leaf is relative not only to the given tree and leaf but also to the given strategy. As we use it very seldom, this lack of rigor in the terminology will be harmless).

Lemma 5.14 *If $\mathcal{S}$ is a strategy for the deduction-system $\mathcal{D}$ then, for every true assertion A*
(1) the set of labels of $\mathcal{T}(\mathcal{S}, A)$ is a $\mathcal{D}$-proof, relative to the set of labels of the leaves of $\mathcal{T}(\mathcal{S}, A)$.
(2) every label of a leaf is true.

Case of $\mathcal{K}_0$ †

As well as the deduction relation $\mid\!\!\!-\!\!-_{\mathcal{K}_0}$ (see lemma 5.4), a strategy might be "compatible with homomorphisms".

Definition 5.15 *Let $\mathcal{S}$ be a strategy for $\mathcal{K}_0$. We call $\mathcal{S}$ a homomorphic strategy (*Hom-*strategy for short) iff for every assertion $A \in \mathcal{A}$ and every homomorphism $\psi \in \mathrm{Hom}_H(K, K)$,*

$$\mathcal{S}(\psi(A)) = \psi(\mathcal{S}(A)),$$

where the map ψ used in lefthand-side (resp. righthand-side) is the natural extension of ψ to assertions (resp. to trees labelled by assertions).

6 Triangulations

Let $(V, \smile)$ be the structured alphabet associated with some H-dpda $\mathcal{M}$ (as defined in section 2.3) and let K be some extension of H. Let $S_1, S_2, \cdots, S_d$ be a family of deterministic series over $K * V^*$.

Let us consider a sequence $\mathcal{S}$ of n "weighted" linear equations :

$$(\mathcal{E}_i) : p_i, \sum_{j=1}^{d} \alpha_{i,j} S_j \ , \ \sum_{j=1}^{d} \beta_{i,j} S_j$$

where $p_i \in \mathbb{N}$, and $A = (\alpha_{i,j}), B = (\beta_{i,j})$ are deterministic rational matrices of dimension (n, d), with indices $m \leq i \leq m+n-1, 1 \leq j \leq d$. For any weighted equation, $\mathcal{E} = (p, S, S')$, we recall the "cost" of this equation is :

$$J(\mathcal{E}) = p + 2 \cdot \mathrm{Div}(S, S').$$

We associate to such a system another system of equations, $\mathrm{INV}(\mathcal{S})$, which "translates the equations of $\mathcal{S}$ into equations over $(\alpha_{i,j}, \beta_{i,j})$ only" [6]. The general idea of the construction of INV consists in iterating the transformation used in the proof of (1) $\Rightarrow$ (2) $\Rightarrow$ (3) in lemma 4.30, i.e. the classical idea of *triangulating* a system of linear equations. Of course we must deal with the weights and relate the construction with the deduction system $\mathcal{K}_0$. Let us assume here that

$$\forall j \in [1, d], S_j \not\equiv \emptyset. \tag{60}$$

and

$$\forall i \in [m, m+n-1], \forall j \in [1, d], \alpha_{i,j}, \beta_{i,j} \text{ are } \epsilon - \text{free}. \tag{61}$$

(These two assumptions will be weakened at the end of the section).
We assume X is endowed with a total ordering, $\leq$. We denote by the same symbol $\leq$ its short-lex extension over X^*.

Let us define $\mathrm{INV}(\mathcal{S})$, $\mathrm{W}(\mathcal{S}) \in \mathbb{N} \cup \{\perp\}$, $\mathrm{D}(\mathcal{S}) \in \mathbb{N}$ by induction on n. $\mathrm{W}(\mathcal{S})$ is the *weight* of $\mathcal{S}$. $\mathrm{D}(\mathcal{S})$ is the *weak codimension* of $\mathcal{S}$.
Case 1 : $\mathrm{supp}(\alpha_{m,*}) \equiv_{\mathsf{B}} \mathrm{supp}(\beta_{m,*})$[7].

$$\mathrm{INV}(\mathcal{S}) = ((W(\mathcal{S}), \alpha_{m,j}, \beta_{m,j}))_{1 \leq j \leq d}, \ \mathrm{W}(\mathcal{S}) = p_m - 1, \ \mathrm{D}(\mathcal{S}) = 0.$$

Case 2 : $\mathrm{supp}(\alpha_{m,*}) \not\equiv_{\mathsf{B}} \mathrm{supp}(\beta_{m,*}), n \geq 2, p_{m+1} - p_m \geq 2 \cdot \mathrm{Div}_{\mathsf{B}}(\mathrm{supp}(\alpha_{m,*}), \mathrm{supp}(\beta_{m,*})) + 1$.
Let

$$u = \min\{v \in X^*, \exists j \in [1, d], \mathrm{supp}(\alpha_{m,*} \odot v) = \epsilon_j^d \Leftrightarrow \mathrm{supp}(\beta_{m,*} \odot v) \neq \epsilon_j^d\}.$$

[6] When $K = H = \{1\}$ the function INV is exactly the one used in [Sén98b]; it was introduced there as an "elaborated version" of the *inverse* systems defined in [Mei89, Mei92] in the case of a single equation.

[7] Given any matrix $\gamma \in \mathsf{DB}_{I,J}\langle\langle M \rangle\rangle$ and $i \in I$, by $\gamma_{i,*}$ we mean the row vector $(\gamma_{i,j})_{j \in J}$.

Let $j_0 \in [1, d]$ and $k \in K$ such that:

$(\alpha_{m,*} \odot (k, u) = \epsilon^d_{j_0}$ and $\beta_{m,*} \odot (k, u) \not\approx \epsilon^d_{j_0})$ or $(\alpha_{m,*} \odot (k, u) \not\approx \epsilon^d_{j_0}$ and $\beta_{m,*} \odot (k, u) = \epsilon^d_{j_0})$.

Subcase 1 : $\alpha_{m,j_0} \odot (k, u) = \varepsilon, \beta_{m,j_0} \odot (k, u) \not\approx \varepsilon$.
Let us consider the weighted equation

$$(p_m + 2 \cdot |u|, S_{j_0}, \sum_{j=1}^{d} (\beta_{m,j_0} \odot (k, u))^* (\beta_{m,j} \odot (k, u)) S_j)$$

and define a new system of weighted equations $\mathcal{S}' = (\mathcal{E}'_i)_{m+1 \leq i \leq m+n-1}$ by :

$$\begin{aligned}(\mathcal{E}'_i) = (p_i, & \textstyle\sum_{j \neq j_0} [\alpha_{i,j} + \alpha_{i,j_0} (\beta_{m,j_0} \odot (k, u))^* (\beta_{m,j} \odot (k, u))] S_j \\ & \textstyle\sum_{j \neq j_0} [\beta_{i,j} + \beta_{i,j_0} (\beta_{m,j_0} \odot (k, u))^* (\beta_{m,j} \odot (k, u))] S_j),\end{aligned}$$

(where the above equation is seen as an equation between two linear combinations of the S_j's, $1 \leq j \leq d$). We then define:

$$\mathrm{INV}(\mathcal{S}) = \mathrm{INV}(\mathcal{S}'), \mathrm{W}(\mathcal{S}) = \mathrm{W}(\mathcal{S}'), \mathrm{D}(\mathcal{S}) = \mathrm{D}(\mathcal{S}') + 1.$$

Subcase 2 : $\alpha_{m,j_0} \odot (k, u) \not\approx \varepsilon, \beta_{m,j_0} \odot (k, u) = \varepsilon$
(analogous to subcase 1 by interchanging the roles of α and β).
Case 3 : $\mathrm{supp}(\alpha_{m,*}) \not\equiv_{\mathsf{B}} \mathrm{supp}(\beta_{m,*}), n = 1$.
We then define:

$$\mathrm{INV}(\mathcal{S}) = \perp, \mathrm{W}(\mathcal{S}) = \perp, \mathrm{D}(\mathcal{S}) = 0,$$

where $\perp$ is a special symbol which can be understood as meaning "undefined".
Case 4 : $\mathrm{supp}(\alpha_{m,*}) \not\equiv_{\mathsf{B}} \mathrm{supp}(\beta_{m,*}), n \geq 2, p_{m+1} - p_m \leq 2 \cdot \mathrm{Div}_{\mathsf{B}}(\mathrm{supp}(\alpha_{m,*}), \mathrm{supp}(\beta_{m,*}))$.
We then define:

$$\mathrm{INV}(\mathcal{S}) = \perp, \mathrm{W}(\mathcal{S}) = \perp, \mathrm{D}(\mathcal{S}) = 0,$$

Lemma 6.1 *: Let $\mathcal{S}$ be a system of linear equations. If $\mathrm{INV}(\mathcal{S}) \neq \perp$ then, $\forall \mathcal{E} \in \mathrm{INV}(\mathcal{S}), \mathcal{E}$ is a weighted linear equation with deterministic coefficients.*

Lemma 6.2 *: Let $\mathcal{S}$ be a system of linear equations. If $\mathrm{INV}(\mathcal{S}) \neq \perp$ then $\mathrm{INV}(\mathcal{S}) = (\bar{\mathcal{E}}_j)_{1 \leq j \leq d}$ fulfills:*

1. $\{\bar{\mathcal{E}}_j \mid 1 \leq j \leq d\} \cup \{\mathcal{E}_i \mid m \leq i \leq m + \mathrm{D}(\mathcal{S}) - 1\} \models \mathcal{E}_{m+\mathrm{D}(\mathcal{S})}$

2. $\min\{J(\mathcal{E}_i) \mid m \leq i \leq m + \mathrm{D}(\mathcal{S})\} = \infty \Longrightarrow \min\{J(\bar{\mathcal{E}}_j) \mid 1 \leq j \leq d\} = \infty$.

Sketch of proof: Point (1) can be established by same means as in the boolean case (see [Sén98b, lemma 5.2]).
Point (2) is clear, when case 1 occurs, as a consequence of lemma 4.28 and assumption (60). The general case can then be deduced inductively as in [Sén98b, lemma 5.2]. □

Lemma 6.3 *: Let $\mathcal{S}$ be a system of linear equations and $\psi \in \mathrm{Hom}_H(K, K)$. Then $\mathrm{INV}(\psi(\mathcal{S})) = \psi(\mathrm{INV}(\mathcal{S}))$ and $\mathrm{D}(\psi(\mathcal{S})) = \mathrm{D}(\mathcal{S})$, where ψ is extended to systems of equations in the natural way and $\psi(\perp) = \perp$.*

Proof: Let us notice the two following facts:
for every $\gamma \in \mathsf{DRB}\langle\langle\ K * V^*\ \rangle\rangle$, $k \in K, u \in X^*, \psi \in \mathrm{Hom}_H(K, K)$:

$$\mathrm{supp}(\gamma) = \mathrm{supp}(\psi(\gamma)) \tag{62}$$

$$\psi(\gamma \odot (k, u)) = \psi(\gamma) \odot (\psi(k), u) \tag{63}$$

By facts (62,63), the case (and subcase) fulfilled by $\psi(\mathcal{S})$ is the same as the the case (and subcase) fulfilled by $\mathcal{S}$. By fact (63) the system $(\psi(\mathcal{S}))'$ introduced in case 2 coincides with the system $\psi(\mathcal{S}')$. Inductively, it follows that $\mathrm{INV}(\psi(\mathcal{S})) = \psi(\mathrm{INV}(\mathcal{S}))$. □

Lemma 6.4 *: Let $\mathcal{S}$ be a system of linear equations satisfying the hypothesis of case 2. Then, $\forall i \in [m+1, m+n-1]$,*
$\parallel \alpha'_{i,*} \parallel \leq \parallel \alpha_{i,*} \parallel + \parallel \beta_{m,*} \parallel + \mid Q \mid \mid u \mid, \parallel \beta'_{i,*} \parallel \leq \parallel \beta_{i,*} \parallel + \parallel \beta_{m,*} \parallel + \mid Q \mid \mid u \mid$.

Let us consider the function F defined by :

$F(d, n) = max\{\mathrm{Div}_{\mathsf{B}}(A, B) \mid A, B \in \mathsf{DRB}_{1,d}\langle\langle\ V^*\ \rangle\rangle, \parallel A \parallel \leq n, \parallel B \parallel \leq n, A \not\equiv B\}$.
For every integer parameters $d, K_1, K_2, K_3, K_4 \in \mathbb{N} - \{0\}$, we define integer sequences $(\delta_i, \ell_i, L_i, s_i, S_i, \Sigma_i)_{m \leq i \leq m+n-1}$ by :

$$\delta_m = 0, \ell_m = 0, L_m = K_2, s_m = K_3 \cdot K_2 + K_4, S_m = 0, \Sigma_m = 0, \tag{64}$$

and for every $m \leq i \leq m+n-2$,

$$\begin{array}{ll} \delta_{i+1} = 2 \cdot F(d, s_i + \Sigma_i) + 1, & \ell_{i+1} = 2 \cdot \delta_{i+1} + 3, \\ L_{i+1} = K_1 \cdot (L_i + \ell_{i+1}) + K_2, & s_{i+1} = K_3 \cdot L_{i+1} + K_4, \\ S_{i+1} = s_i + \Sigma_i + \mid Q \mid F(d, s_i + \Sigma_i), & \Sigma_{i+1} = \Sigma_i + S_{i+1}. \end{array} \tag{65}$$

For every weighted, deterministic rational linear equation $\mathcal{E} = (p, \sum_{j=1}^d \alpha_j S_j\ ,\ \sum_{j=1}^d \beta_j S_j)$, we define

$$\parallel\mid \mathcal{E} \parallel\mid = max\{\parallel \boldsymbol{\alpha} \parallel, \parallel \boldsymbol{\beta} \parallel\}.$$

Lemma 6.5 *Let $\mathcal{S} = (\mathcal{E}_i)_{m \leq i \leq m+d-1}$ be a system of d weighted linear equations such that $J(\mathcal{E}_i) = \infty$ (for every i) and:*

(1) $\forall i \in [m, m+d-1], \parallel\mid \mathcal{E}_i \parallel\mid \leq s_i$
(2) $\forall i \in [m, m+d-2], \mathrm{W}(\mathcal{E}_{i+1}) - \mathrm{W}(\mathcal{E}_i) \geq \delta_{i+1}$.

Then $\mathrm{INV}(\mathcal{S}) \neq \perp, \mathrm{D}(\mathcal{S}) \leq d-1, \forall \mathcal{E} \in \mathrm{INV}(\mathcal{S}), \parallel\mid \mathcal{E} \parallel\mid \leq \Sigma_{m+\mathrm{D}(\mathcal{S})} + s_{m+\mathrm{D}(\mathcal{S})}$.

All the definitions and lemmas can be easily extended to the more general case where assumptions (60,61) are replaced by the weaker assumption that:

$$\exists j \in [1, d], S_j \not\equiv \emptyset, \tag{66}$$

(using the same techniques as in [Sén98b, section 5.2]).

7 Constants

Let us define some integers which are *constant* in the sense that they depend on the H-dpda $\mathcal{M}$ only. For every $S \in \mathsf{DB}\langle\langle\, H * V^* \,\rangle\rangle$, $\nu(S)$ is defined as $\nu(S) = \mathrm{Div}(S, \emptyset)$.

$k_0 = \max\{\nu([pAq]) \mid p, q \in Q, A \in Z, [pAq] \not\equiv \emptyset\}$, $k_1 = \max\{2k_0 + 1, 3\}$,
$D_1 = 4k_0 + 3$, $k_2 = (D_1 + 4) \cdot k_1 + k_0 + 1$,
$K_1 = k_1 + 1$, $K_2 = (D_1 + 1) \cdot k_1^2 + (D_1 + 1) \cdot k_1 + 1$,
$K_3 = k_0|Q|$, $K_4 = k_0 \cdot |Q|^2 + (k_2 + k_1 + 7) \cdot |Q| + 3$,
$d_0 = 2 \cdot |Q| \cdot (\mathrm{Card}(X^{\leq k_1}) + 1)$.

We consider now the integer sequences $(\delta_i, \ell_i, L_i, s_i, S_i, \Sigma_i)_{m \leq i \leq m+n-1}$ defined by the relations (64,65) of section 6 where the parameters $d, K_1, \ldots, K_4$ are chosen to be the above constants and $m = 1, n = d_0, d = d_0$.
The two integers below are *constant* in a weaker sense: they depend on the H-dpda $\mathcal{M}$ *and* an initial true assertion $A_0 = (\Pi_0, S_0^-, S_0^+)$.

$$D_2 = \max\{\Sigma_{d_0} + s_{d_0}, \|S_0^-\|, \|S_0^+\|\}, \quad N_0 = 1 + (k_2 + 2)|Q| + D_2,$$

8 Strategies for $\mathcal{K}_0$ †

Let H, K be two groups as in §5.2. Let us define strategies for the particular system $\mathcal{K}_0$ associated with $\mathcal{M}$ and K.
We define first auxiliary strategies $T_\emptyset, T_A, T_B, T_C$ and then derive some compound strategies from them. Let us fix here some total ordering on $X : x_1 < x_2 < \cdots < x_\alpha$ and also some total ordering $\leq$ of type ω on $\mathcal{A}$ (inherited from the usual well-ordering of $\mathbb{N}$ by the fixed encoding). From these orderings one can construct in the usual way an ordering of type ω on the sets $X^*, \mathcal{A}^*$ and $\mathbb{N}^* \times (\mathsf{DRB}\langle\langle\ K * V^*\ \rangle\rangle)^*$.

$T_\emptyset$: $T_\emptyset(A_1A_2\cdots A_n) = B_1\cdots B_m$ iff $\exists S, T, A_n = (p, S, T), p \geq 0, S \equiv T \equiv \emptyset$ and $m = 0$

T_A: $T_A(A_1\cdots A_n) = B_1\cdots B_m$ iff

$$A_n = (p, S, T), m = \mid X \mid, B_1 = (p{+}1, S\odot x_1, T\odot x_1), \cdots, B_m = (p{+}1, S\odot x_m, T\odot x_m),$$

where $\forall k \in K, S \not\equiv k, T \not\equiv k$.

T_B^+: $T_B^+(A_1\cdots A_n) = B_1\cdots B_m$ iff $n \geq k_1 + 1, A_{n-k_1} = (\pi, \overline{U}, U')$, (where $\overline{U}$ is unmarked)

$$U' = h' \cdot \sum_{q\in Q} [\overline{p}Aq] \cdot V_q \quad (\text{ for some } h' \in K, \overline{p} \in Q, A \in Z, V_q \in \mathsf{DB}\langle\langle\ K * V^*\ \rangle\rangle)$$

$A_i = (\pi + k_1 + i - n, U_i, U_i')$ for $n - k_1 \leq i \leq n$,
$(U_i)_{n-k_1\leq i\leq n}$ is a derivation, $(U_i')_{n-k_1\leq i\leq n}$ is a stacking derivation (see §4.5),

$$U_n' = h' \cdot \sum_{q\in Q} h \cdot [p\tau q] \cdot V_q, \quad \text{for some } h \in H, p \in Q, \tau \in Z^+,$$

$m = 1, B_1 = (\pi + k_1 - 1, V, V'), V = U_n$,

$$V' = h' \cdot \sum_{q\in Q'} h \cdot [p\tau q] \cdot [qeq] \cdot (\overline{U} \odot (h_q, u_q)),$$

where $Q' = \{q \in Q \mid [\overline{p}Aq] \not\equiv \emptyset\}, \forall q \in Q'$,

$$(h_q, u_q) = \min\{(h, u) \in K \times X^*, (h' \cdot [\overline{p}Aq]) \odot (h, u) = \epsilon\}.$$

T_B^-: T_B^- is defined in the same way as T_B^+ by exchanging the left series (S^-) and right series (S^+) in every assertion (p, S^-, S^+).

T_C: $T_C(A_1\cdots A_n) = B_1\cdots B_m$ iff there exists $d \in [1, d_0], D \in [\ 0\ ,\ d-1\ ], S_1, S_2, \cdots, S_d \in \mathsf{DRB}\langle\langle\ K * V^*\ \rangle\rangle, 1 \leq \kappa_1 < \kappa_2 < \cdots < \kappa_{D+1} = n$, such that,

(C1) every equation $(\mathcal{E}_i) = (p_{\kappa_i}, S^-_{p_{\kappa_i}}, S^+_{p_{\kappa_i}})$, for $1 \leq i \leq D{+}1$, is a weighted equation over $S_1, S_2, \cdots, S_d$,

(C2) $\mathcal{S} = (\mathcal{E}_i)_{1\leq i\leq D+1}$ is such that, $\mathrm{INV}(\mathcal{S}) \neq \perp, \mathrm{D}(\mathcal{S}) = D$ and $\|| \mathrm{INV}(\mathcal{S}) \||\leq \Sigma_{d_0} + s_{d_0}$, (C3) $(\kappa_1, \kappa_2, \cdots, \kappa_{D+1}, S_1, \cdots, S_d) \in \mathbb{N}^* \times (\mathsf{DRB}\langle\langle K * V^* \rangle\rangle)^*$ is the minimal vector satisfying conditions (C1,C2) for the given sequence $(A_1 \cdots A_n)$ and

(C4) $B_1 \cdots B_m = \rho_e(\mathrm{INV}(\mathcal{S}))$ (where ρ_e is the obvious extension of ρ_e to pairs of series and then to sequences of weighted equations; in other words the result of T_C is $\mathrm{INV}(\mathcal{S})$ where the marks have been removed).

Lemma 8.1 *: $T_\emptyset, T_A, T_B, T_C$ are $\mathcal{K}_0$-strategies and they are homomorphic.*

(The notion of *homomorphic* strategy is introduced by definition 5.15).
Sketch of proof: The fact that $T_\emptyset, T_A, T_B, T_C$ are $\mathcal{K}_0$-strategies can be proved by a straightforward adaptation of the proof of lemmas 7.1,7.2 of [Sén98b].
$T_\emptyset$ is clearly homomorphic.
In order to prove that T_A, T_B are homomorphic, it is sufficient to use the equation (63) noticed in §6.
Lemma 6.3 shows that T_C is homomorphic. □
Let us define the strategy $\mathcal{S}_{AB}$ by: for every $W = A_1 A_2 \cdots A_n$,

(1) if $W \in \mathrm{dom}(T_\emptyset)$, then $\mathcal{S}_{AB}(W) = T_\emptyset(W)$,
(2) elsif $W \in \mathrm{dom}(T_B^+)$, then $\mathcal{S}_{AB}(W) = T_B^+(W)$,
(3) elsif $W \in \mathrm{dom}(T_B^-)$, then $\mathcal{S}_{AB}(W) = T_B^-(W)$,
(4) elsif $W \in \mathrm{dom}(T_A)$, then $\mathcal{S}_{AB}(W) = T_A(W)$,
(5) else $\mathcal{S}_{AB}(W)$ is undefined.

The strategy $\mathcal{S}_{ABC}$ is defined by: for every $W = A_1 A_2 \cdots A_n$,

(1) if $W \in \mathrm{dom}(T_\emptyset)$, then $\mathcal{S}_{ABC}(W) = T_\emptyset(W)$,
(2) elsif $A_1 A_2 \cdots A_{n-1} \in \mathrm{dom}(T_C)$ then $\mathcal{S}_{ABC}(W)$ is undefined,
(3) elsif $W \in \mathrm{dom}(T_C)$, then $\mathcal{S}_{ABC}(W) = T_C(W)$,
(4) elsif $W \in \mathrm{dom}(T_B^+)$, then $\mathcal{S}_{ABC}(W) = T_B^+(W)$,
(5) elsif $W \in \mathrm{dom}(T_B^-)$, then $\mathcal{S}_{ABC}(W) = T_B^-(W)$,
(6) elsif $W \in \mathrm{dom}(T_A)$, then $\mathcal{S}_{ABC}(W) = T_A(W)$,
(7) else $\mathcal{S}_{ABC}(W)$ is undefined.

Lemma 8.2 *$\mathcal{S}_{ABC}, \mathcal{S}_{AB}$ are Hom-strategies for $\mathcal{K}_0$.*

9 Tree analysis

This section is devoted to the analysis of the proof-trees τ produced by the strategy $\mathcal{S}_{AB}$ defined in section 8. The main results are lemma 9.7 and 9.8 whose combination asserts that if some branch of τ is infinite, then the transformation T_C is defined on some finite prefix of this branch. This key technical result will ensure termination of the strategy $\mathcal{S}_{ABC}$ (see section 10).
We assume throughout this section that an assertion A_0 is fixed and we use the numbers D_2, N_0 deduced from the pair $\mathcal{M}, A_0$ (see section 7). (Notice that the assertion A_0 itself does not interfer with this section except through these "constants" D_2, N_0).

9.1 General properties

The next lemma just shows that the *weight* and the *depth* of a given node are closely related.

Lemma 9.1 *: Let τ be a proof-tree associated to the strategy $\mathcal{S}_{AB}$. Let $x, x' \in dom(\tau), x \leq x'$. Then $\mid W(x') - W(x) \mid \leq |x'| - |x| \leq 2 \cdot (W(x') - W(x)) + 3$.*

We fix throughout the remaining of this section a tree

$$\tau = \mathcal{T}(\mathcal{S}_{AB}, (\pi_0, U_0^-, U_0^+))$$

(i.e. τ is the proof tree associated to the assertion $(\pi_0, U_0^-, U_0^+))$ by the strategy $\mathcal{S}_{AB}$). We suppose that

$$\mathrm{rd}(U_0^-) \leq D_2, \quad \mathrm{rd}(U_0^+) \leq D_2, \quad U_0^-, U_0^+ \text{ are both unmarked .} \tag{67}$$

and also that

$$\exists \psi \in \mathrm{Hom}_H(K, K), \quad \psi(U_0^-) \equiv \psi(U_0^+). \tag{68}$$

We recall that, formally, τ is a map $\mathrm{dom}(\tau) \to \mathbb{N} \times \mathsf{DRB}\langle\langle\ K * V^*\ \rangle\rangle \times \mathsf{DRB}\langle\langle\ K * V^*\ \rangle\rangle$ such that $\mathrm{dom}(\tau) \subseteq \{1, \ldots, |X|\}^*$ is closed under prefix and under "left-brother" (i.e. $w \cdot (i+1) \in \mathrm{dom}(\tau) \Rightarrow w \cdot i \in \mathrm{dom}(\tau)$). We denote by $pr_{2,3}$: $\mathbb{N} \times \mathsf{DRB}\langle\langle\ K * V^*\ \rangle\rangle \times \mathsf{DRB}\langle\langle\ K * V^*\ \rangle\rangle \to \mathsf{DRB}\langle\langle\ K * V^*\ \rangle\rangle \times \mathsf{DRB}\langle\langle\ K * V^*\ \rangle\rangle$ the projection $(\pi, U, U') \mapsto (U, U')$. By τ_s we denote the tree obtained from τ by forgetting the weights: $\tau_s = \tau \circ pr_{2,3}$. We establish some linearity properties of the labels of τ.

Lemma 9.2 *For every label (π, U^-, U^+) of τ,*

(1) U^α is (D_1, D_2)-linear (for $\alpha \in \{-, +\}$)
(2) if U^α is unmarked, then U^α is $(0, D_2)$-linear
(3) $\exists \alpha \in \{-, +\}, U^\alpha$ is unmarked.

We show now that the tree τ is somewhat "smooth" in the sense that its labels cannot be varying in a too chaotic way along a given branch. We shall establish that every infinite branch must contain at least d labels (U, U') belonging to the same deterministic space V of dimension $d \leq d_0$ with coordinates not greater than s_{d_0} (over some fixed generating family of cardinality d). Our analysis distinguishes between two types of infinite branchs: those which contain an infinite "N-stacking sequence" and those which contain an infinite "N-bounded sequence".

Let us define now these technical notions. For every $U, U' \in \mathsf{DRB}\langle\langle K * V^* \rangle\rangle$ we set:

$$|||U||| = \max\{\|\tilde{U}\|, \ \tilde{U} \in \mathsf{Q}(U) \text{ and } \tilde{U} \text{ is unmarked }\}, \ |||(U, U')||| = \max\{|||U|||, |||U'|||\}.$$

Let $x \in \mathrm{dom}(\tau)$. We define now a kind of norm on nodes which in some sense "erases" the short-term variations of $|||(*, *)|||$:

$$\mathrm{N}(x) = \max\{|||\tau_s(x(j))|||, j \in \mathbb{N}, |x| - k_1 \leq j \leq |x|\}.$$

Lemma 9.3 *Let $(x_i)_{i \in I}$ (where I is a beginning section of $\mathbb{N}$) be some branch of τ.*

(1) The function $N : I \rightarrow \mathbb{N}$ is $(k_0 \cdot |Q|)$-up-Lipschitz.
(2) The restriction $N : J \rightarrow \mathbb{N}$ to any interval $J \subseteq I$ such that neither T_B^-, nor T_B^+ occur in J, is $|Q|$-up-Lipschitz.

Let $\sigma = (x_i)_{i \in I}$ be a path in τ, where $I \subseteq \mathbb{N}$ is a non-empty interval and $i_0 = \min\{I\}$. We call σ a *N-stacking sequence* iff:

$$\forall i \in I, \mathrm{N}(x_i) \geq \mathrm{N}(x_{i_0}) \text{ and } \mathrm{N}(x_{i_0}) \geq N_0. \tag{69}$$

We call σ a *N-bounded sequence* iff I is infinite and:

$$\mathrm{Card}\{i \in I, \mathrm{N}(x_i) < N_0\} = \infty. \tag{70}$$

9.2 N-stacking sequences

From now on and until the end of subsection 9.2, we fix a N-stacking sequence $\sigma = (x_i)_{i \in I}$ and we suppose I is infinite. Let us use the simplified notations $\mathrm{N}(i)$ for $\mathrm{N}(x_i)$ and let us note $\tau_s(x_i) = (U_i^-, U_i^+)$.

Lemma 9.4 $\forall i \in \mathbb{N}, \exists j \in [i, i + k_1], |||\ (U_j^-, U_j^+)\ ||| \geq \mathrm{N}(i_0)$.

Proof: This follows from the fact that $\mathrm{N}(i + k_1) \geq \mathrm{N}(i_0)$. □
We let

- $i_1 = \min\{i \in [i_0 - k_1, i_0] \cap \mathbb{N},\ |||\ (U_i^-, U_i^+)\ ||| \geq \mathrm{N}(i_0) - (k_2 - k_0)|Q|\}$, if no T_B^α occurs in $[i_0 - k_1, i_0]$
- and i_1 is the unique element of $[i_0 - k_1, i_0] \cap \mathbb{N}$ where some T_B^α occurs otherwise.

For every $\alpha \in \{-,+\}$, we define a Q-series $[p^\alpha \omega^\alpha]$ and a Q-form Φ^α as follows.
case 1: $U^\alpha_{i_1}$ is unmarked and $\|U^\alpha_{i_1}\| \geq \mathrm{N}(i_0) - (k_2 - k_0)|Q|$.
As $\mathrm{rd}(U^\alpha_{i_1}) \leq D_2$, $U^\alpha_{i_1}$ has a minimal decomposition: $U^\alpha_{i_1} \approx [p^\alpha \omega^\alpha_1] * \Phi^\alpha_1$ with $\|\Phi^\alpha_1\| \leq D_2$. Using the inequality $\|U^\alpha_{i_1}\| \geq \mathrm{N}(i_0) - (k_2+1)|Q| \geq D_2$, we conclude that ω^α_1 admits a decomposition $\omega^\alpha_1 = \omega^\alpha \omega^\alpha_2$ such that

$$U^\alpha_{i_1} \approx [p^\alpha \omega^\alpha] * \Phi^\alpha, \;\; \Phi^\alpha = [\omega^\alpha_2] * \Phi^\alpha_1, \tag{71}$$

with

$$\mathrm{N}(i_0) - (k_2+1)|Q| \leq \|\Phi^\alpha\| < \mathrm{N}(i_0) - k_2|Q|, \;\; \|\Phi^\alpha\| \geq D_2 + |Q|, \;\; |\Phi^\alpha| \geq 1. \tag{72}$$

case 2: $U^\alpha_{i_1}$ is marked and $\||\, U^\alpha_{i_1} \,\|| \geq \mathrm{N}(i_0) - (k_2 - k_0)|Q|$.
Hence $U^\alpha_{i_1}$ can be written as $U^\alpha_{i_1} \approx \Sigma_{q \in Q'} [p^\alpha_1 \mu^\alpha_1 q] \cdot [qeq] \cdot (\overline{U^\alpha_{i_1}} \odot (h_q, u_q))$ for some $p^\alpha_1 \in Q, Q' \subseteq Q, 1 \leq |\mu^\alpha_1| \leq D_1, h_q \in K, |u_q| \leq k_0, \overline{U^\alpha_{i_1}} = U^{-\alpha}_j, j < i_1$.
Let $q \in Q'$ such that $\||\, U^\alpha_{i_1} \,\|| = \|\overline{U^\alpha_{i_1}} \odot (h_q, u_q)\|$. We have:

$$\|\overline{U^\alpha_{i_1}}\| \geq \|\overline{U^\alpha_{i_1}} \odot (h_q, u_q)\| - |u_q||Q| \geq \mathrm{N}(i_0) - (k_2 - k_0)|Q| - k_0|Q| = \mathrm{N}(i_0) - k_2|Q|.$$

From this inequality we conclude, as in case 1, that $\overline{U^\alpha_{i_1}}$ has a decomposition:

$$\overline{U^\alpha_{i_1}} \approx [p^\alpha \omega^\alpha] * \Phi^\alpha, \tag{73}$$

with

$$\mathrm{N}(i_0) - (k_2+1)|Q| \leq \|\Phi^\alpha\| < \mathrm{N}(i_0) - k_2|Q|, \;\; \|\Phi^\alpha\| \geq D_2 + |Q|, \;\; |\Phi^\alpha| \geq 1. \tag{74}$$

case 3: $\||\, U^\alpha_{i_1} \,\|| < \mathrm{N}(i_0) - (k_2 - k_0)|Q|$. In this case , $[p^\alpha \omega^\alpha], \Phi^\alpha$ are both undefined.

Let us remark that, by the inequality $\||\, (U^-_{i_1}, U^+_{i_1}) \,\|| \geq \mathrm{N}(i_0) - (k_2 - k_1)|Q|$, there exists at least one $\alpha \in \{-,+\}$ such that $[p^\alpha \omega^\alpha], \Phi^\alpha$ are both defined. Let us define now the following sets of series and d-spaces of series:

$$\mathcal{G}_0 = \{\Phi^\alpha_q \odot u \mid q \in Q, u \in X^{\leq k_0}\} \cup \{\rho_\varepsilon(\Phi^\alpha_q) \mid q \in Q\}, \tag{75}$$

$$W^\alpha = \mathsf{V}((\Phi^\alpha_q)_{q \in Q}), \;\; V^\alpha = \mathsf{V}(\mathcal{G}_0), \tag{76}$$

for every $\alpha \in \{-,+\}$;

$$\bar{V} = V^- + V^+, \;\; \tilde{W} = W^- \cup W^+, \;\; \tilde{V} = V^- \cup V^+, \tag{77}$$

where , for every d-spaces V_1, V_2, $V_1 + V_2$ denotes the smallest d-space containing $V_1 \cup V_2$. We illustrate on figure 2 the above definitions. The band

$$\{U \in \mathsf{DRB}\langle\langle\, K * V^* \,\rangle\rangle | \mathrm{N}(i_0) - 2k_1|Q| \leq \||\, U \,\||\}$$

is a *full security band* in the sense that every U^α_i in this band *belongs to* $\bar{V}$ (lemma 9.5). The band

$$\{U \in \mathsf{DRB}\langle\langle\, K * V^* \,\rangle\rangle | \;\; \mathrm{N}(i_0) - (k_2 - k_0)|Q| \leq \||\, U \,\|| < \mathrm{N}(i_0)\}$$

is a *security band* in the sense that if $[U^\alpha_j$ is in this band , $j < i$, U^α_i belongs to the full security band, and $U^\alpha_j \longrightarrow U^\alpha_i]$, then U^α_j *belongs to* $\bar{V}$ (property $\mathcal{P}(\alpha, i, j)$ established in the proof of lemma 9.5).

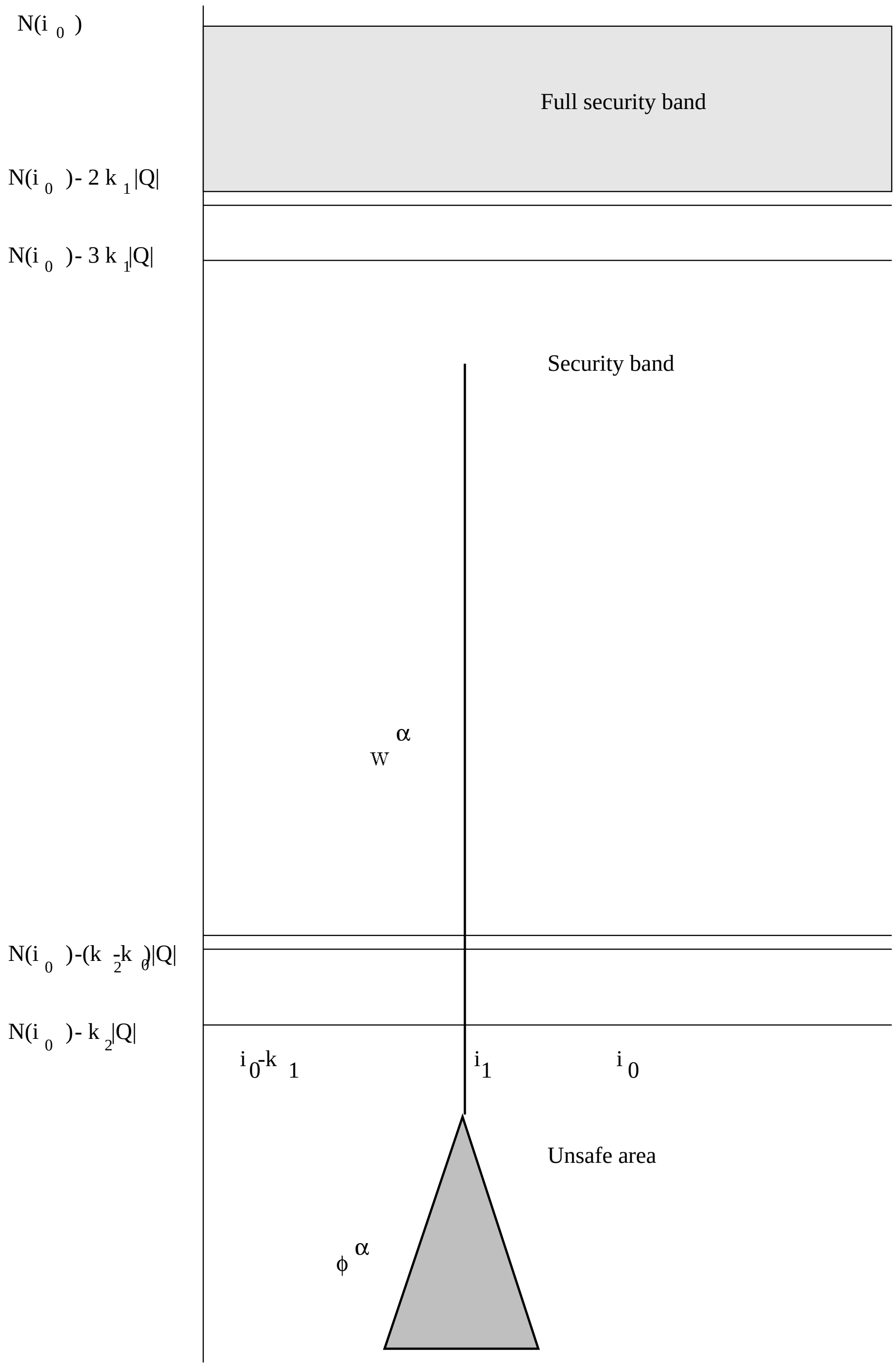

Fig. 2. the generating family.

Lemma 9.5 *Let $i \geq i_1, \alpha \in \{-,+\}$ such that $||| U_i^\alpha ||| \geq \mathrm{N}(i_0) - 2k_1|Q|$. Then $U_i^\alpha \in \bar{V}$.*

Sketch of proof: Let us consider the following property $\mathcal{P}(\alpha, i, j)$:
$\{j \leq i$ and $||| U_i^\alpha ||| \geq \mathrm{N}(i_0) - 2 \cdot k_1 \cdot |Q|$ and no T_B^α occurs in $[j+1, i]\} \Longrightarrow$
$\{($ if U_j^α is unmarked then $U_j^\alpha \in \tilde{W})$ and
(if U_j^α is marked then, there exists some $\alpha' \in \{-,+\}$ such that ,
every linear component of U_j^α is in $(W^{\alpha'} \cap \mathsf{DRBlin}^{D_2}\langle\langle K * V^* \rangle\rangle) \odot X^{<1,k_0>})\}$.
(Here we denote by $X^{<m,m'>}$ the set $\{u \in X^*, m \leq |u| \leq m'\}$). We prove by lexicographic induction on the pair (i,j) that:

$$\forall i \geq i_1, \forall j \geq i_1, [\forall \alpha \in \{-,+\}, \mathcal{P}(\alpha, i, j)].$$

□

Let us define a new space of series by: $\mathcal{G}_1 = (\theta_j)_{1 \leq j \leq d}$ where

$$\{\theta_j | 1 \leq j \leq d\} = \bigcup_{\alpha \in \{-,+\}} \{\Phi_q^\alpha \odot u | \ q \in Q, u \in X^{\leq k_1}\} \cup \{\rho_\epsilon(\Phi_q^\alpha), \ \ q \in Q\},$$

(one can notice that $d \leq d_0$), and

$$\bar{V}_1 = \mathsf{V}(\mathcal{G}_1).$$

Lemma 9.6 *Let $L > 0$. There exists $i \in [i_0 + L, i_0 + K_1 \cdot L + K_2]$ such that, for every $\alpha \in \{-,+\}$, there exists a deterministic rational vector $(\beta_{i,j}^\alpha)_{1 \leq j \leq d}$ fulfilling*

(1) $U_i^\alpha = \sum_{j=1}^d \beta_{i,j}^\alpha \theta_j$
(2) $||\beta_{i,*}^\alpha|| \leq K_3 \cdot (i - i_0) + K_4$.

By *iteration* of lemma 9.6 we obtain the following lemma.

Lemma 9.7 *There exists $i_0 \leq \kappa_1 < \kappa_2 < \ldots < \kappa_d$ and deterministic rational vectors $(\beta_{i,j}^\alpha)_{1 \leq j \leq d}$ (for every $i \in [1, d]$) such that*

(0)$W(\kappa_1) \geq 1$,
(1)$\forall i, \forall \alpha, U_{\kappa_i}^\alpha = \sum_{j=1}^d \beta_{i,j}^\alpha \theta_j \in \overline{V_1}$,
(2)$\forall i, \forall \alpha, ||\beta_{i,*}^\alpha|| \leq s_i$,
(3)$\forall i, W(\kappa_{i+1}) - W(\kappa_i) \geq \delta_{i+1}$.

where the sequences $(\delta_i, \ell_i, L_i, s_i, S_i, \sigma_i)$ are those defined by relations (64, 65) in section 6, $K_1, \ldots, K_4$ are the constants defined in section 7, and $m = 1, n = d$.

9.3 N-bounded sequences †

Let us fix now a N-bounded sequence $\sigma = (x_i)_{i \in I}$. By hypothesis

$$I' = \{i \in I, \mathrm{N}(x_i) < N_0\}$$

is infinite. Let us take now $d = |Q| + 1$. (One can notice that $d \leq d_0$).

Lemma 9.8 *There exists a family of series $(\theta_j)_{1 \leq j \leq d}$, a sequence of elements of I, $i_0 \leq \kappa_1 < \kappa_2 < \ldots < \kappa_d$ and deterministic rational vectors $(\beta^{\alpha}_{i,j})_{1 \leq j \leq d}$ (for every $i \in [1, d]$) such that*

(0) $W(\kappa_1) \geq 1$,
(1) $\forall i, \forall \alpha, U^{\alpha}_{\kappa_i} = \sum_{j=1}^{d} \beta^{\alpha}_{i,j} \theta_j$,
(2) $\forall i, \forall \alpha, ||\beta^{\alpha}_{i,*}|| \leq s_i$,
(3) $\forall i, W(\kappa_{i+1}) - W(\kappa_i) \geq \delta_{i+1}$.

In order to prove lemma 9.8 we state a stronger version of lemma 9.2.

Lemma 9.9 *For every label (π, U^-, U^+) of τ, one of the following 3 cases is true*

(1) $\exists \alpha', \alpha'' \in \{+, -\}, \exists k, k' \in K, u, u' \in X^*$, *such that:*
$U^+ = U_0^{\alpha'} \odot (k, u)$, $U^- = U_0^{\alpha''} \odot (k', u')$
(2) $\exists \alpha' \in \{+, -\}, \exists k \in K, u \in X^*, p \in Q, \omega \in Z^{\leq D_1}$, $\forall q \in Q, \exists k_q \in K, u_q \in X^*$, *such that:*
$U^+ = U_0^{\alpha'} \odot (k, u)$, $U^- \approx \sum_{q \in Q} [p\omega q] \cdot [qeq] \cdot U_0^{\alpha'} \odot (k_q, u_q)$
(3) $\exists \alpha' \in \{+, -\}, \exists k \in K, u \in X^*, p \in Q, \omega \in Z^{\leq D_1}$, $\forall q \in Q, \exists k_q \in K, u_q \in X^*$, *such that:*
$U^+ \approx \sum_{q \in Q} [p\omega q] \cdot [qeq] \cdot U_0^{\alpha'} \odot (k_q, u_q)$, $U^- = U_0^{\alpha'} \odot (k, u)$,

Let us prove lemma 9.8 now.
Proof: From the formula given in lemma 9.9, it follows that, for every $i \in I$, there exists a family of left-unitary series $(\theta_{i,j})_{1 \leq j \leq d}$, where

$$\theta_{i,j} \approx U_0^{\alpha_{i,j}} \odot (k_{i,j}, u_{i,j}) \text{ for some } \alpha_{i,j} \in \{+, -\}, k_{i,j} \in K, u_{i,j} \in X^*$$

and two deterministic rational vectors $(\gamma^{\alpha}_{i,j})_{1 \leq j \leq d}$ (for $\alpha \in \{+, -\}$) such that

$$\forall \alpha, U^{\alpha}_i = \sum_{j=1}^{d} \gamma^{\alpha}_{i,j} \cdot \theta_{i,j}, \tag{78}$$

and

$$\forall \alpha, ||\gamma^{\alpha}_{i,*}|| \leq s_1. \tag{79}$$

(It suffices to define the signs $\alpha_{i,j}$ and pairs $(k_{i,j}, u_{i,j})$ from the signs α', α'' and the pairs $(k, u), (k', u'), \ldots, (k_q, u_q)$ occuring in lemma 9.9 and to take the left-unitary representative of $U_0^{\alpha_{i,j}} \odot (k_{i,j}, u_{i,j})$ modulo($\approx$)).

Using lemma 4.21 and the fact that the $U_0^{\alpha'}$ are rational , we deduce that the set

$$\{U_0^{\alpha'} \odot (k,u) \mid \alpha' \in \{+,-\}, k \in K, u \in X^*, \|U_0^{\alpha'} \odot (k,u)\| < N_0\}/\approx$$

is finite. Hence there exists an infinite subset $I'' \subseteq I'$ and a fixed family $(\theta_j)_{1 \le j \le d}$ such that:

$$\forall i \in I'', (\theta_{i,j})_{1 \le j \le d} = (\theta_j)_{1 \le j \le d} \tag{80}$$

As I'' is infinite, and, by lemma 9.1 $\lim_{i \to \infty} W(i) = \infty$ there exists a finite sequence $\kappa_1 < \kappa_2 < \ldots < \kappa_d$ of elements of I'' fulfilling:

$$W(\kappa_1) \ge 1, \tag{81}$$

and

$$\forall i \in [1,d], W(\kappa_{i+1}) - W(\kappa_i) \ge \delta_{i+1}. \tag{82}$$

By statements (78,80,79,81,82), the lemma is proved. $\square$

10 Completeness of $\mathcal{H}_0$ †

We fix here $H = \mathrm{GL}_n(\mathbb{Q})$, $K = \mathrm{F}(U) * H$, as in §5.3. We show a completeness result: every true assertion $A_0 \in \mathcal{A}$ which has no occurence of parameter, has a regular $\mathcal{H}_0$-proof (theorem 10.3).

Lemma 10.1 *: Let $A \in \mathbb{N} \times \mathsf{DRB}\langle\langle\, K * V^* \,\rangle\rangle \times \mathsf{DRB}\langle\langle\, K * V^* \,\rangle\rangle$,$A$ unmarked and let $\psi \in \mathrm{Hom}_H(K, K)$ such that $J(\psi(A)) = \infty$. Then the tree $\mathcal{T}(\mathcal{S}_{ABC}, A)$ is finite.*

Proof: Let

$$A = (\Pi_0, S_0^-, S_0^+) \text{ be an unmarked assertion,} \tag{83}$$

and suppose that $\psi \in \mathrm{Hom}_H(K, K)$ is such that

$$J(\psi(A)) = \infty. \tag{84}$$

We consider all the contants associated to the pair $(\mathcal{M}, A)$ in section 7. Let us suppose that:

$$t = \mathcal{T}(\mathcal{S}_{ABC}, A) \text{ is infinite.} \tag{85}$$

We shall establish that hypothesis (85) leads to a contradiction.
By Koenig's lemma, t contains an infinite branch whose (infinite) labelling word is $A_0 A_1 \cdots A_n \cdots$ (where $A_0 = A$). By point (2) of the definition of $\mathcal{S}_{ABC}$, this branch is also a branch of the tree $t' = \mathcal{T}(\mathcal{S}_{AB}, A_0)$. By the definition of D_2 and hypothesis (83) this tree t' fulfills the property (67) assumed throughout section 9. By hypothesis (84), t' also fulfills the property (68) assumed throughout section 9. Let us then apply the results of section 9.

case 1:$A_0 A_1 \cdots A_n \cdots$ contains an infinite N-stacking sequence $\sigma = (A_{i_0+n})_{n \geq 0}$. By lemma 9.7, σ contains a subsequence $(A_{\kappa_1}, \ldots, A_{\kappa_i}, \ldots, A_{\kappa_d})$ with $d \leq d_0$ fullfilling hypothesis (1)(2) of lemma 6.5. As $T_\emptyset$ does not occur on this branch, assumption (66) must also be fulfilled by the sequence $\mathcal{S} = (A_{\kappa_i})_{1 \leq i \leq d}$. The conclusion of lemma 6.5 shows that, if we chose $D = \mathrm{D}(\mathcal{S})$, conditions (C1)(C2) of the definition of T_C are fulfilled. It follows that some finite prefix of $A_0 A_1 \cdots A_{\kappa_d}$ fulfills conditions (C1)(C2)(C3)(C4) i.e. belongs to $\mathrm{dom}(T_C)$. The priority ordering used in the definition of T_C (section 8) then implies that either $T_\emptyset$ or T_C occurs at some $n \geq 0$. But $T_\emptyset$ cannot occur on an infinite branch and, by condition (2) in the definition of $\mathcal{S}_{ABC}$, neither can T_C. We have reached a contradiction.

case 2:$A_0 A_1 \cdots A_n \cdots$ contains no infinite N-stacking sequence.
This means that the set $\{n \in \mathbb{N} \mid \mathrm{N}(x_n) < N_0\}$ is infinite, i.e. that $\sigma = (A_i)_{i \geq 0}$ is a N-bounded sequence (see definition (70)). Replacing lemma 9.7 by lemma 9.8 in the above arguments, we reach the same contradiction. In both cases we have established that (85) is impossible. □

Lemma 10.2 *Let* $A' \in \mathbb{N} \times \mathsf{DRB}\langle\langle\ K * V^*\ \rangle\rangle \times \mathsf{DRB}\langle\langle\ K * V^*\ \rangle\rangle$ *and* $D \in \mathbb{N}$.
Let us suppose that:
– $A' = (\pi', S', T')$ *where* $\| S' \| \leq D$, $\| T' \| \leq D$,
– A' *is unmarked and* ϵ*-free,*
– $\exists \psi \in \mathrm{Hom}_H(K, K)$ *such that* $J(\psi(A')) = \infty$.
Let x *be an open leaf of the tree* $t = \mathcal{T}(\mathcal{S}_{ABC}, A')$ *with*

$$t(x) = (\pi, S, T).$$

Then, one of the following two cases must occur:
(1) $\forall k \in K, S \not\equiv k, T \not\equiv k,\ \| S \| \leq D,\ \| T \| \leq D$
(2) $S \in K, T \in K$ *and* $\psi(S) = \psi(T)$.

From now on, we call open leaf of type (1) (resp. (2)) any open leaf satisfying case (1) (resp. (2)) of this lemma.

Theorem 10.3 *Let* $A_0 \in \mathbb{N} \times \mathsf{DRB}\langle\langle\ H * V^*\ \rangle\rangle \times \mathsf{DRB}\langle\langle\ H * V^*\ \rangle\rangle$. *If* A_0 *is true (i.e.* $J(A_0) = \infty$*) then* A_0 *has some regular* $\mathcal{H}_0$*-proof.*

Which might be rephrased as: the system $\mathcal{H}_0$ is "regularly"-complete.
Proof:
1 Let us treat first the case where A_0 is unmarked and $\epsilon - free$.
Let D_2 be *the* integer associated with $(\mathcal{M}, A_0)$ as defined in section 7.
Let $\bar{U} = \{u_1, u_2, \ldots, u_{D_2^2}\} \subseteq U$ be a subset of parameters with D_2^2 elements, $\bar{K} = \mathrm{F}(\bar{U}) * H$. Let us consider the sets

$$\mathcal{F}(D_2) = \{S \in \mathsf{DRB}\langle\langle\ \bar{K} * V^*\ \rangle\rangle \mid\ \| S \| \leq D_2, S \text{ is unmarked, } \epsilon\text{-free, generic and } S \notin K\},$$

$$\mathcal{FA}(D_2) = \{(0, S, T) \mid S, T \in \mathcal{F}(D_2), \exists \psi \in \mathrm{Hom}_H(K, K),\ \ \psi(S) \equiv \psi(T)\},$$

and let $A_1, A_2, \ldots, A_n$ be a numbering of $\mathcal{FA}(D_2)$. For every $i \in [0, n]$ we define:

$$\begin{aligned} t_i &= \mathcal{T}(\mathcal{S}_{ABC}, A_i), \\ \bar{P}_i &= \mathrm{im}(t_i), \\ \alpha(i) &= \text{ the cardinality of the set of open leaves of type (1) in } t_i, \\ \beta(i) &= \text{ the cardinality of the set of open leaves of type (2) in } t_i, \end{aligned}$$

$(\bar{B}_{i,j})_{0 \leq i \leq n, 0 \leq j \leq \alpha(i)}$ is an enumeration of the set of open leaves of type (1) in t_i,

$$B_{i,j} = \rho_e(\bar{B}_{i,j}), \text{ for every } 0 \leq i \leq n, 0 \leq j \leq \alpha(i)$$

$$P_i = \bar{P}_i - \{\bar{B}_{i,j} \mid\ 0 \leq i \leq n, 0 \leq j \leq \alpha(i)\} \cup \{B_{i,j} \mid\ 0 \leq i \leq n, 0 \leq j \leq \alpha(i)\},$$

$(C_{i,k})_{0 \leq i \leq n, 0 \leq k \leq \beta(i)}$ is an enumeration of the set of open leaves of type (2) in t_i,

$(\gamma(i,j), \psi_{i,j})$ is the smallest pair in $[0, n] \times \mathrm{Hom}_H(\bar{K}, \bar{K})$ having the property that

$$\psi_{i,j}(A_{\gamma(i,j)}) = B_{i,j}.$$

The existence of such a pair $(\gamma(i,j),\psi_{i,j})$ follows from lemma 4.17 and the fact that every generic series of norm $\leq D_2$ uses at most D_2^2 parameters, hence belongs to $\mathcal{F}(D_2)$, up to a renaming of the parameters.
Let us consider the 9-tuple

$$G=(n,\alpha,\beta,\gamma,(P_i)_{0\leq i\leq n},(A_i)_{0\leq i\leq n},(B_{i,j})_{0\leq i\leq n,0\leq j\leq\alpha(i)},(C_{i,k})_{0\leq i\leq n,0\leq k\leq\beta(i)},(\psi_{i,j})_{0\leq i\leq n,0\leq j\leq\alpha(i)}).$$

The above definitions ensure that G is a H-germ. Let us check that G is a germ of proof.
Let us consider some open leaf x of type 2 in t_i:

$$t_i(x)=C_{i,k}=(\pi_{i,k},S_{i,k},T_{i,k})$$

where $S_{i,k},T_{i,k}\in K$. Let $\psi\in\mathcal{R}_i$:

$$\psi=\psi_{i_0,j_0}\circ\psi_{i_1,j_1}\cdots\circ\psi_{i_\ell,j_\ell}$$

where the conditions of definition 5.7 are met. As

$$J(A_0)=\infty \tag{86}$$

and $\mathcal{S}_{ABC}$ is a $\mathcal{K}_0$ strategy (lemma 8.2), by lemma 5.14 and lemma 4.24,

$$J(B_{i_0,j_0})=J(\bar{B}_{i_0,j_0})=\infty \tag{87}$$

i.e., by definition of ψ_{i_0,j_0}

$$J(\psi_{i_0,j_0}(A_{i_1}))=\infty, \tag{88}$$

(notice that τ_t transforms true assertions into true assertions). By the same arguments, for every $k'\in[0,\ell-1]$, the hypothesis that

$$J(\psi_{i_0,j_0}\circ\cdots\circ\psi_{i_{k'},j_{k'}}(A_{\gamma(i_{k'},j_{k'})}))=\infty \tag{89}$$

implies that

$$J(\psi_{i_0,j_0}\circ\cdots\circ\psi_{i_{k'},j_{k'}}\circ\psi_{i_{k'+1},j_{k'+1}}(A_{i_{k'+1}}))=\infty \tag{90}$$

Properties (86) and [(89) $\Rightarrow$ (90)] show, by induction , that

$$J(\psi_{i_0,j_0}\circ\cdots\circ\psi_{i_\ell,j_\ell}(A_i))=\infty. \tag{91}$$

Here again, as $\mathcal{S}_{ABC}$ is a $\mathcal{K}_0$ strategy (lemma 8.2), lemma 5.14 and equality (91) imply that $J(\psi_i(C_{i,k}))=\infty$, i.e.

$$\psi_i(S_{i,k})\equiv\psi_i(T_{i,k}). \tag{92}$$

Since $S_{i,k},T_{i,k}$ belong to K, (92) can be rewritten:

$$\psi_i(S_{i,k})=\psi_i(T_{i,k}). \tag{93}$$

2 By part (1) $\rho_e(\rho_\epsilon(A_0))$ has a regular $\mathcal{H}_0$-proof P and, due to rules $(K10)$, $(K11)$, $P\cup\{A_0\}$ is a regular $\mathcal{H}_0$-proof of A_0. It follows that every true assertion A_0 has a regular $\mathcal{H}_0$-proof. □

Theorem 10.4 *Let $H = \mathrm{GL}_n(\mathbb{Q})$ for some $n \in \mathbb{N}$. The equivalence problem for deterministic H-pushdown automata is decidable.*

Proof: Let $\mathcal{M}$ be some H-dpda. The equivalence relation $\equiv$ on $\mathsf{DRB}\langle\langle\ H * V^*\ \rangle\rangle$ (where V is the structured alphabet associated to the given $\mathcal{M}$) has a recursively enumerable complement (this is an easy adaptation of the corresponding well-known fact for boolean automata; this adaptation is valid as soon as H has a decidable word-problem). By theorem 10.3 and lemma 5.13 $\equiv$ is recursively enumerable too. Hence $\equiv$ is recursive. In addition, the system $\mathcal{H}_0$ associated with $\mathcal{M}$ is computable from $\mathcal{M}$, hence the theorem follows. □

Corollary 10.5 *Let H be a free group with finite basis Y ($H = \mathrm{F}(Y)$ for some finite alphabet Y). The equivalence problem for deterministic H-pushdown automata is decidable.*

Proof: By [LS77, prop.12.3 p.167] the two matrices

$$a = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix},$$

generate a free subgroup of rank 2 of $\mathrm{GL}_2(\mathbb{Q})$. Choosing $n = 2$ in theorem 10.4, we obtain the decidability of the equivalence problem for deterministic H-pushdown automata, with $H = \mathrm{F}(\{a, b\})$. As every free group of finite rank is embeddable in $\mathrm{F}(\{a, b\})$, the corollary follows. □

Corollary 10.6 *Let $H = Y^*$, the free monoid with finite basis Y, for some finite alphabet Y. The equivalence problem for deterministic H-pushdown automata is decidable.*

Proof: As Y^* is embedded in $\mathrm{F}(Y)$, this corollary follows directly from corollary 10.5. □

References

[BR88] J. Berstel and C. Reutenauer. *Rational Series and their Languages.* Springer, 1988.

[Buc85] B. Buchberger. Basic features and development of the critical-pair/completion algorithm. In *Proceedings 1st RTA*, pages 1–45. LNCS 202, 1985.

[CK86a] K. CulikII and J. Karhumäki. The equivalence of finite-valued transducers (on HDTOL languages) is decidable. *Theoretical Computer Science*, pages 71–84, 1986.

[CK86b] K. CulikII and J. Karhumäki. Synchronizable deterministic pushdown automata and the decidability of their equivalence. *Acta Informatica 23*, pages 597–605, 1986.

[Cou83] B. Courcelle. An axiomatic approach to the Korenjac-Hopcroft algorithms. *Math. Systems theory*, pages 191–231, 1983.

[Cul90] K. CulikII. New techniques for proving the decidability of equivalence problems. *Theoretical Computer Science*, pages 29–45, 1990.

[Gub85] V.S. Guba. A solution of Ehrenfeucht's conjecture. *unpublished note*, 1985.

[Har78] M.A. Harrison. *Introduction to Formal Language Theory.* Addison-Wesley, Reading, Mass., 1978.

[Her26] G. Herman. Die frage der unendlichen vielen schritte in der theorie der polynomideale. *Math. Ann. 95*, pages 736–788, 1926.

[HHY79] M.A. Harrison, I.M. Havel, and A. Yehudai. On equivalence of grammars through transformation trees. *TCS 9*, pages 173–205, 1979.

[Hil90] D. Hilbert. Über die theorie der algebraischen formen. *Math. Ann. 36*, pages 473–534, 1890.

[IR81] O.H. Ibarra and L. Rosier. On the decidability of equivalence problem for deterministic pushdown transducers. *Information Processing Letters 13*, pages 89–93, 1981.

[Kro87] D. Krob. Monoïdes et semi-anneaux complets. *Semi-group forum*, pages 323–339, 1987.

[Lis96] L.P. Lisovik. Hard sets methods and semilinear reservoir method with applications. In *Proceedings 23rd ICALP*, pages 229–231. Springer, LNCS 1099, 1996.

[LS77] R.C. Lyndon and P.E. Schupp. *Combinatorial Group Theory.* Springer Verlag, 1977.

[Mei89] Y.V. Meitus. The equivalence problem for real-time strict deterministic pushdown automata. *Kibernetika 5 (in russian, english translation in Cybernetics and Systems analysis)*, pages 14–25, 1989.

[Mei92] Y.V. Meitus. Decidability of the equivalence problem for deterministic pushdown automata. *Kibernetika 5 (in russian, english translation in Cybernetics and Systems analysis)*, pages 20–45, 1992.

[RS80] G. Rozenberg and A. Salomaa. *The Mathematical Theory of L-systems.* Academic Press, New-York, 1980.

[Sén97] G. Sénizergues. L(A) = L(B)? In *Proceedings INFINITY 97*, pages 1–26. Electronic Notes in Theoretical Computer Science 9, URL: http://www.elsevier.nl/locate/entcs/volume9.html, 1997.

[Sén98a] G. Sénizergues. The equivalence problem for deterministic pushdown transducers into abelian groups. In *Proceedings MFCS'98*, pages 305–315. Springer, LNCS 1450, 1998.

[Sén98b] G. Sénizergues. L(A) = L(B)? Technical report, LaBRI, Université Bordeaux I, 1998. Improved version of report 1161-97, submitted to TCS, accessible at URL, http://www.labri.u-bordeaux.fr/~ges, pages 1-166, april 1998.

[TS89] E. Tomita and K. Seino. A direct branching algorithm for checking the equivalence of two deterministic pushdown transducers, one of which is real-time strict. *Theoretical Computer science*, pages 39–53, 1989.

[Val74] L.G. Valiant. The equivalence problem for deterministic finite-turn pushdown automata. *Information and Control 25*, pages 123–133, 1974.

This article was processed using the LaTeX macro package with LLNCS style