



# Le problème de l'équivalence des transducteurs à pile déterministes

G. Sénizergues

LaBRI, Bordeaux university,

on 02/06/2022

Colloque ANR DELTA

## contents

- 1 Agrippa's trilemma
- 2 Integer vs boolean truth-values
- 3 The pushdown transducers
- 4 A first deduction system
- 5 A minimal deduction system
- 6 Extensions

# Agrippa's TRILEMMA

It is **impossible** to prove any assertion  $A$ :

- either the proof ends with some unproved statement: this is a **dogma** and it cannot be sure
- either the proof-construction **never finishes**; hence, after a finite amount of time we still are not sure of  $S$
- or the proof **loops**: such a way of reasoning can prove **false** statements.

[Agrippa, sceptical philosopher, 1st century]

Despite this opinion:

looping (a.k.a. self-proving or cyclic) proofs were used:

[B. Courcelle, 1983 :] equivalence of program-schemes

[D. Caucal, 1995 :] bisimulation of grammars

[G.S. MCU 1998 :] equivalence of formal languages (survey)

[D. Kuperberg, L.Pinault, D.Pous 2019 :] Jumping automata

[E. Hasard, D. Kuperberg 2022 :] Transfinite expressions.

In this talk: proofs are both cyclic and infinite

An **Idea** for showing soundness despite cyclicity:  
let  $\mathcal{A}$  be some set of assertions and

$$C : \mathcal{A} \rightarrow \mathbb{N} \cup \{\infty\}.$$

We assume that, for every rule

$$\frac{A_1, A_2, \dots, A_n}{B}$$

$$\inf\{C(A_1), C(A_2), \dots, C(A_n)\} \leq C(B)$$

$C(A) = \infty$  means  $v(A) = 1$

$C(A) < \infty$  means  $v(A) = 0$  and

the “cost” for finding a counter-example is  $C(A)$ .

Example 0:

$G = \langle \{a, b, c\}, \{S, T\}, P \rangle$  where  $P$  consists of the rules:

$$S \rightarrow aSb + c$$

$$T \rightarrow aTb + c$$

$Sb \equiv Tb$  can be proved by the following  $G$ -equality-proof

$$\begin{array}{c}
 \frac{}{a \equiv a} \text{ref} \quad \frac{}{Sb \equiv Tb} \text{sj} \\
 \frac{}{aSb \equiv aTb} \times \quad \frac{}{c \equiv c} \text{ref} \quad \frac{}{T \equiv aTb + c} \text{gr} \\
 \frac{}{aSb + c \equiv aTb + c} + \quad \frac{}{aTb + c \equiv T} \text{sym} \\
 \frac{}{S \equiv aSb + c} \text{gr} \quad \frac{}{aSb + c \equiv T} \text{trans} \\
 \frac{}{S \equiv T} \text{trans} \quad \frac{}{b \equiv b} \text{ref} \\
 \frac{}{Sb \equiv Tb} \times
 \end{array}$$



G-EQuality (schemes of) rules:

$$\frac{x \equiv y}{y \equiv x} \text{sym} \quad \frac{x \equiv y \quad y \equiv z}{x \equiv z} \text{trans} \quad \frac{x \equiv x' \quad y \equiv y'}{x + y \equiv x' + y'} +$$

G-EQuality (schemes of) **strict**-rules:

$$\frac{}{x \equiv x} \text{ref} \quad \frac{x \equiv x' \quad y \equiv y'}{x \cdot y \equiv x' \cdot y'} \times$$

G-EQuality **strict**-rules:

$$\overline{S \equiv \sum_{i=1}^n w_i} \text{gr}$$

Instanciations, for sym,trans,+,ref,×: by rational **languages**.

Instanciations, for gr: exactly one instance for each grammar rule.

## Definition

Let  $\mathcal{S}$  be some deduction system over a set of assertions  $\mathcal{A}$ .

$\mathcal{S}$  has two different sets of rules:

$\mathcal{R}$  :the set of large rules.

$\mathcal{S}$  :the set of strict rules;all the 0-ary rules (the axioms) are strict.

We call  **$\mathcal{S}$ -proof**, every set  $P \subseteq \mathcal{A}$  such that:

- every assertion  $p \in P$  has a proof-tree, within the system  $\mathcal{S}$ , with hypotheses in  $P$ ,
- such that every branch goes **through some strict rule** (terminating with an axiom is included)

NB: if  $A$  is an axiom,  $\{A\}$  is a proof

if  $A$  is not an axiom,  $\{A\}$  is not a proof.

A deduction system is called *sound* if, every provable judgment is true.

### Lemma

*If  $S$  is a deduction system which has only **increasing** (resp. **strictly increasing**) rules (resp. **strict rules**), then it is **sound**.*

NB: whether the proofs are finite or infinite is not relevant for soundness

# The pushdown transducers

Let  $\mathbf{H}$  be a group.

We call a *pushdown  $\mathbf{H}$ -automaton* on the alphabet  $X$  any 6-tuple

$$\mathcal{M} = \langle X, Z, Q, \delta, q_0, z_0 \rangle$$

$Z$  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

$\delta : QZ \times (X \cup \{\epsilon\}) \rightarrow \mathcal{P}_f(\mathbf{H} \times QZ^*)$ , is the transition mapping.

Let  $q, q' \in Q, \omega, \omega' \in Z^*, z \in Z, h \in \mathbf{H}, u \in X^*$  and  $a \in X \cup \{\epsilon\}$ .

We note

$$(qz\omega, h, au) \vdash_{\mathcal{M}} (q'\omega'\omega, h \cdot h', u)$$

if

$$(h', q'\omega') \in \delta(qz, a).$$

We note

$$q\omega \xrightarrow{(h,u)}_{\mathcal{M}} q'\omega'$$

if

$$(q\omega, 1_H, u) \vdash_{\mathcal{M}}^* (q'\omega', h, \epsilon).$$

Given some finite set  $F \subseteq QZ^*$  of configurations,

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

$$T(\mathcal{M}, F) \in \mathbb{B}\langle \langle H \times X^* \rangle \rangle.$$

Decision problem:

INPUT: Two deterministic *pushdown H-automata*  $\mathcal{M}_1, \mathcal{M}_2$

QUESTION:  $T(\mathcal{M}_1, F_1) = T(\mathcal{M}_2, F_2)$  ?

This problem is **decidable**:

[Ibarra-Rosier, IPL 1981 :] Case where both  $\mathcal{M}_i$  have no  $\varepsilon$ -transition and recognize by empty stack.

[Tomita-Seino TCS 1987 :] Case where  $\mathcal{M}_1$  has no  $\varepsilon$ -transition and recognizes by empty stack.

[G.S. ICALP 1999 :] general case.

The  $H$ -grammar  $G$ :

$$V = \{[p, z, q] \mid p, q \in Q, z \in Z\},$$

Rules:

$$[p, z, q] \rightarrow x \cdot h \cdot [p', z_1, p''] [p'', z_2, q]$$

if  $x \in X, (h, p'z_1z_2) \in \delta(pz, x)$

$$([p, z, q] \rightarrow x \cdot h \cdot [p', z', q])$$

if  $x \in X, (h, p'z') \in \delta(pz, x)$

$$([p, z, q], a \cdot h)$$

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



# Admissible series

A series  $S \in \mathbb{B}\langle\langle H * V^* \rangle\rangle$  is called *admissible* iff, every residual series  $T$  of  $S$  has one of the three following shapes:  $T = \emptyset$  or  $T = h$  or

$$T = \sum_{q \in Q} h \cdot [pzq] \cdot T_q$$

(intuitively: every residual of  $S$  has a unique “leftmost coefficient”  $h$  and “leftmost mode”  $pz$ ).

NB: the grammar  $G$  has rhs which are **admissible** polynomials; the **reduced** form of  $G$  still has this property.

The *norm* of a series  $S$  is defined by:  $\| S \|$  is the number of left-residuals of  $S$ , up to left-product by elements of  $H$ .

# Automaton action $\odot$

Let  $S \in H * V^*$ ,  $h \in H$ ,  $u \in X^*$ . We define:

$$S \odot (h, u) := h^{-1} \cdot \sum_{T \in H * V^*, S \rightarrow_{lm} u \cdot T} T.$$

This right-action is extended to all of  $\mathbb{B}\langle\langle H * V^* \rangle\rangle$  in such a way that it is  $\sigma$ -additive.

The map:  $\varphi : \mathbb{B}\langle\langle H * V^* \rangle\rangle \rightarrow \mathbb{B}\langle\langle H \times X^* \rangle\rangle$  is defined by:

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

The equivalence relation  $\equiv$  is defined by

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

Given two admissible rational series  $S, T$ , can we **decide** whether

$$S \equiv T?$$

# A first deduction system

Let  $K := F(U) * H$ , where  $U$  is a denumerable set of "parameters".

System  $\mathcal{K}_0$ 

$$\frac{(p, S, T)}{(p+1, S, T)} \quad \text{K0} \quad \frac{(p, S, T)}{(p, T, S)} \quad \text{K1}$$

$$\frac{(p, S, S'), (p, S', S'')}{(p, S, S'')} \quad \text{K2} \quad \frac{}{(0, S, S)} \quad \text{K3}$$

$$\frac{(p+1, S \odot x, T \odot x) | x \in X}{(p, S, T)} \quad \text{K4} \quad \frac{(p, S, S')}{(p+2, S \odot x, S' \odot x)} \quad \text{K5}$$

$$\frac{(p, S_1 \cdot T + S_2, T)}{(p, S_1^* \cdot S_2, T)} \quad \text{K6} \quad \frac{(p, S_1, T_1), (p, S_2, T_2)}{(p, S_1 + S_2, T_1 + T_2)} \quad \text{K7}$$

$$\frac{(p, S, S')}{(p, S \cdot T, S' \cdot T)} \quad \text{K8} \quad \frac{(p, T, T')}{(p, S \cdot T, S \cdot T')} \quad \text{K9}$$

The rules are obtained by instanciating by:

$$p \in \mathbb{N}, S, S', T, T' \in \text{ARB}(\langle K * V^* \rangle),$$

$$(S_1, S_2), (T_1, T_2) \in \text{ARB}_{1,2}(\langle K * V^* \rangle).$$

The strict rules are: K0,K3,K4,K8,K9.

If  $S, S' \in \text{ARB}(\langle H * V^* \rangle)$ , then:

$$\text{Div}(S, S') = \inf\{|u| \mid u \in X^*, \varphi(S)(u) \neq \varphi(S')(u)\}$$

$$C(p, S, S') = p + 2 * \text{Div}(S, S')$$

## Lemma

*There exists an integer  $D_2$  such that, given any assertion  $(0, S, T) \in \mathbb{N} \times \text{ARB}\langle \langle K * V^* \rangle \rangle \times \text{ARB}\langle \langle K * V^* \rangle \rangle$ , there exists a finite relative  $\mathcal{K}_0$ -proof  $P$  such that:*

- *$(0, S, T)$  is not an hypothesis of  $P$*
- *all hypotheses of  $P$  are of one of the forms:*
  - F1:  $(\pi', S', T')$  with  $\| S' \| \leq D_2, \| T' \| \leq D_2$ ,*
  - F2:  $(\pi', k, k')$  with  $k, k' \in K$ .*
- *for every  $\psi : K \rightarrow K$  such that  $\psi(S) \equiv \psi(T)$ , all leaves of  $P$  are mapped by  $\psi$  on **true** assertions.*

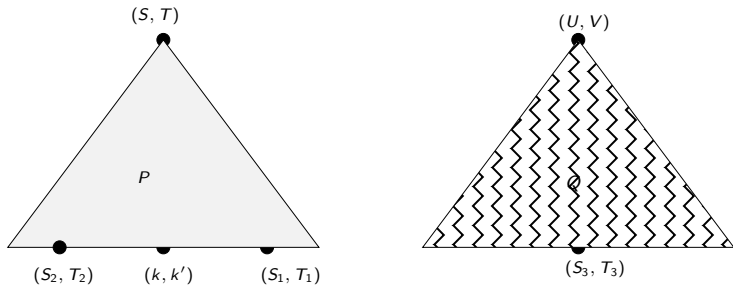


We define a notion of **regular** proof which is, roughly speaking a regular proof-tree, with a HDTOL labelling.

**Germ:**

A *germ* is a finite set of finite relative  $\mathcal{K}_0$ -proofs  $G$ , together with some “**gluing morphisms**” in  $\text{HOM}_H(K, K)$  between them and an “**evaluating morphism**”  $\psi \in \text{HOM}_H(K, H)$  such that:

for every  $P \in G$  and every leaf  $A$  of type (F1) of  $P$ , there exists a gluing morphism mapping the root  $B$  of some  $P' \in G$  into  $A$ .



and:  $\varphi_i : K \rightarrow K$  are morphisms such that

$$(S_1, T_1) = \varphi_1(U, V)$$

$$(S_2, T_2) = \varphi_2(S, T)$$

$$(S_3, T_3) = \varphi_3(S, T)$$

Figure: A germ of proof

# Gluing pattern

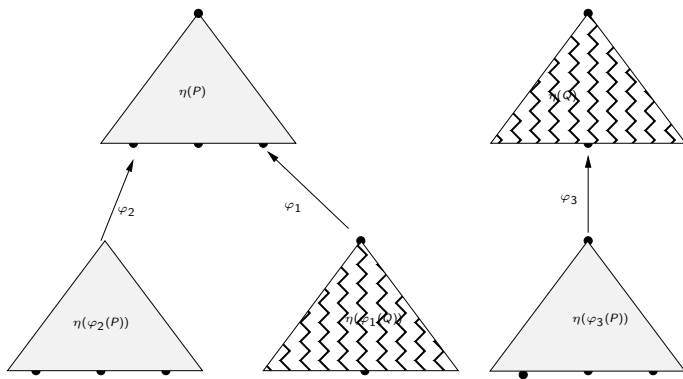
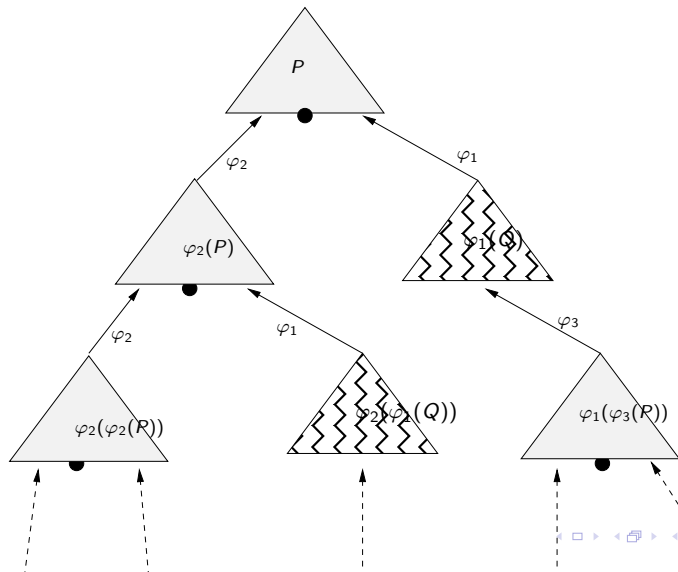


Figure: Gluings

# Regular proof



## Theorem

*Given a germ  $G$  and a morphism  $\psi : F(U) \rightarrow H$ , one can test whether  $(G, \psi)$  generates a  $\mathcal{K}_0$ -proof.*

Let  $G$  be a germ. This set  $G$  is a germ of proof iff all the hypotheses of form (F2) of these proofs are mapped to true equalities by the compositions of the gluing morphisms followed by the evaluating morphism.

This set of equalities is a “morphic” subset of  $F(U_G) * H$ . One can test whether two homomorphisms:  $F(U_G) * H \rightarrow H$  are equal over a morphic subset (adaptation of the case of homomorphisms into a free monoid over a HDT0L language).

[Culik-Karhumäki, TCS 1986

] [Guba,1985

] [Buchberger,RTA'85 .]

By Lemma we obtain the adequation

### Theorem

*Let  $S, T \in \text{DRB}\langle \langle H * V^* \rangle \rangle$ . Then  $S \equiv T$  if and only if the assertion  $(0, S, T)$  has a **regular proof** in the system  $\mathcal{K}_0$ .*

One can compute all the germs whose evaluating morphism  $\psi$  maps the root to the given pair under scrutiny;  
one can test each of them for generating a **proof** (within  $\mathcal{K}_0$ ).  
Thus the equality problem for dpdt is **decidable**.

# A minimal deduction system

Let  $K := F(U) * H$ , where  $U$  is a denumerable set of "parameters".

System  $\mathcal{M}_0$

		$\frac{(S, T)}{(T, S)}$	M1
$\frac{(S, S'), (S', S'')}{(S, S'')}$	M2	$\overline{(S, S)}$	M3
		$\frac{(S_1, T_1), (S_2, T_2)}{(S_1 + S_2, T_1 + T_2)}$	M7
$\frac{(S, S')}{(S \cdot T, S' \cdot T)}$	M8	$\frac{(T, T')}{(p, S \cdot T, S \cdot T')}$	M9



We add all the grammar-rules as axioms.

The rules are obtained by instanciating by:

$$S, S', T, T' \in \text{ARB} \langle \langle (K \times X^*) * V^* \rangle \rangle,$$
$$(S_1, S_2), (T_1, T_2) \in \text{ARB}_{1,2} \langle \langle (K \times X^*) * V^* \rangle \rangle.$$

The strict rules are: M3,M8,M9.

# EXTENSIONS

One can build a finitely generated group  $H$ , such that:

- the word problem for  $H$  is decidable
- the equivalence problem for DPDT from  $X^*$  to  $H$  is **undecidable**.

Problem solved by G.S., announced at MONS 2-4 March 1998, yet unpublished

NB: for generalized sequential mappings :  $X^* \rightarrow H$ , the equivalence problem is decidable **relatively to the word-problem** of  $H$ .

Test equivalence between two deterministic pushdown transducers:

$$X^* \rightarrow \mathcal{M}_{d,d}(\mathbb{Q}).$$

NB: some outputs might be **non-invertible**.

Open problem; ongoing research, some partial results

-  $S, T$  are non-deterministic admissible rational series, with coefficients in  $H$  (the field of quaternions).

Question:  $S \equiv T$ ?

Decidable

[GS Kyoto 2000]

-  $S, T$  are non-deterministic admissible rational series, with coefficients in a linear ring.

Question:  $S \equiv T$ ?

Open problem