

# Word problem and equations on $\mathcal{R}$ -trivial monoids

J. Almeida\*, M. Zeitoun\*\*

\* CMUP, Univ. Porto

\*\* LIAFA, CNRS & Univ. Paris 7

# “Long words” [Bloom, Choffrut '01]

Labeled posets with two operations

- series concatenation  $P \cdot Q$ , order extension where  $P < Q$ .
- $\omega$ -power  $P^\omega = \omega \times P$  under lexicographic order.

The algebra  $P(A)$  of such posets over  $A$  satisfies

- $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
- $(x \cdot y)^\omega = x \cdot (y \cdot x)^\omega$
- $(x^n)^\omega = x^\omega$  for  $n \geq 1$ .

$W(A)$  = sub-algebra generated by singletons  $\{a\}$ ,  $a \in A$ .

# Long words: results

- **Periodicity:** let  $w$  be a labeled ordinal. TFAE
  - $w \in W(A)$ ,
  - $w$  can be written has an  $\omega$ -term.
  - $|w| < \omega^\omega$  and  $w$  has a finite number of tails,
- The variety  $\mathcal{V}$  generated by  $P(A)$  is equal to the variety generated by  $W(A)$ , admits  $W(A)$  as free algebra and is **defined by the identities**
  - $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
  - $(x \cdot y)^\omega = x \cdot (y \cdot x)^\omega$
  - $(x^n)^\omega = x^\omega$  for  $n \geq 1$ .
- The variety  $\mathcal{V}$  has **no finite basis** of identities.
- **Word problem:** equality of  $\omega$ -terms  $u, v$  can be tested in  $O(|u|^2|v|^2)$ -time.

The problem and results of the talk look very similar.

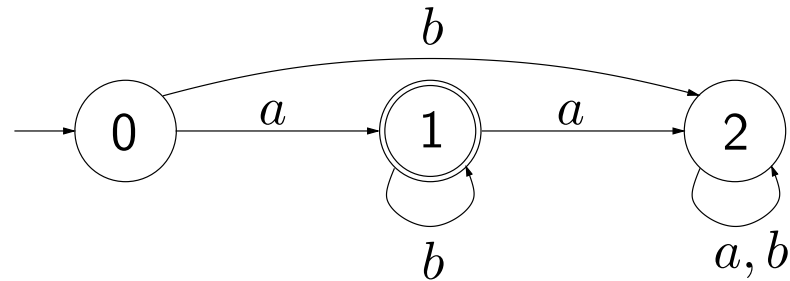
Different motivations (from semigroup theory).

# Rational languages and monoids

Rational language  $ab^*$



Minimal automaton



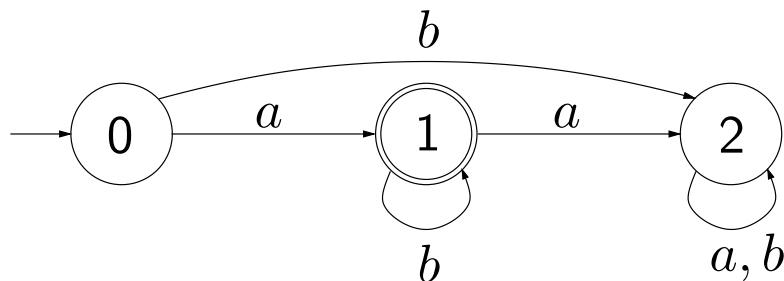
# Rational languages and monoids

Rational language  $ab^*$

Combinatorial properties



Minimal automaton



Syntactic monoid

	0	1	2
$a$	1	2	2
$b$	2	1	2

$$\{\varepsilon, a, b, a^2\}$$

$$ab = a, ba = a^2,$$

$$b^2 = b$$

Algebraic properties

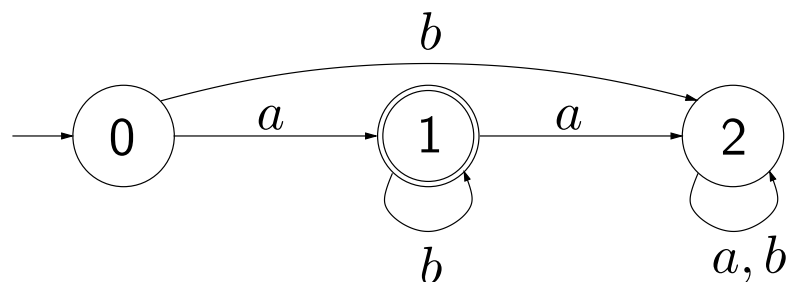
# Rational languages and monoids

Rational language  $ab^*$

Combinatorial properties



Minimal automaton



Syntactic monoid

	0	1	2
a	1	2	2
b	2	1	2

$\{\varepsilon, a, b, a^2\}$

$ab = a, ba = a^2,$

$b^2 = b$

Algebraic properties

**Ex. Combinatorial:**  $\in$  dot-depth  $n \leftrightarrow$  **algebraic:**  $\in V_n$  [PW95], built from simple classes using operators.

Decomposition in group-free/group automata  $\leftrightarrow$  Krohn-Rhodes complexity.

## Some related classes

Class of languages	Class of semigroups/monoids	
Star-free ( $\cup, \setminus, \cdot, \{a\}$ )	Aperiodic monoids <b>A</b> [Sch65]	$x^\omega = x^\omega x$
Increasing mappings	$\mathcal{R}$ -trivial monoids <b>R</b> [Eil?]	$(xy)^\omega = (xy)^\omega x$
Piecewise testable	$\mathcal{J}$ -trivial monoids <b>J</b> [S81]	$\mathbf{R} \cap (xy)^\omega = (yx)^\omega$
Suffix testable	Right zero semigroups <b>D</b>	$xy^\omega = y^\omega$
Level $n$ of Until hierarchy	Characterization involving <b>R, D</b> + operators [TW96]	
Unambiguous languages	<b>DA</b> [Sch76]	
Factor languages	Locally trivial semigroups <b>LI</b>	
Level $n$ of U-S hierarchy	Characterization involving <b>DA, LI</b> + operators [TW02]	

Eilenberg Varieties of languages  $\leftrightarrow$  Pseudovarieties of monoids

## Word problem for $\omega$ -terms

Pseudovariety: Class of finite monoids closed under **finite** product, submonoid, quotient. **Ex.** groups, aperiodic monoids, commutative monoids.

Finite monoid  $M$ .  $m \in M$   $\{m, m^2, m^3, \dots\}$  contains a unique idempotent  $m^\omega$ .

$F_A^\omega$ :  $\omega$ -monoid of  **$\omega$ -terms** on  $A$ . **Ex.**  $(a^\omega b a a)^\omega a$ .

A morphism  $\eta : A^* \rightarrow M$ . can be extended from  $F_A^\omega$  to  $M$ :  $\eta(u^\omega) = (\eta(u))^\omega$ .

$M \models u = v$  ( $u, v \in F_A^\omega$ ) iff for all  $\eta : A^* \rightarrow M$ ,  $\eta(u) = \eta(v)$ .

**Ex.** Groups are monoids satisfying  $xy^\omega = y^\omega x = x$ .

Aperiodic monoids **A** are those satisfying  $x^\omega x = x^\omega$ .

Commutative monoids are those satisfying  $xy = yx$ .

# Word problem for $\omega$ -terms

Pseudovariety: Class of finite monoids closed under **finite** product, submonoid, quotient. **Ex.** groups, aperiodic monoids, commutative monoids.

Finite monoid  $M$ .  $m \in M$   $\{m, m^2, m^3, \dots\}$  contains a unique idempotent  $m^\omega$ .

$F_A^\omega$ :  $\omega$ -monoid of  **$\omega$ -terms** on  $A$ . **Ex.**  $(a^\omega b a a)^\omega a$ .

A morphism  $\eta : A^* \rightarrow M$ . can be extended from  $F_A^\omega$  to  $M$ :  $\eta(u^\omega) = (\eta(u))^\omega$ .

$M \models u = v$  ( $u, v \in F_A^\omega$ ) iff for all  $\eta : A^* \rightarrow M$ ,  $\eta(u) = \eta(v)$ .

**Ex.** Groups are monoids satisfying  $xy^\omega = y^\omega x = x$ .

Aperiodic monoids **A** are those satisfying  $x^\omega x = x^\omega$ .

Commutative monoids are those satisfying  $xy = yx$ .

**Word problem** for  $\omega$ -terms on **V**: given  $u, v \in F_A^\omega$ , decide whether **V**  $\models u = v$ .

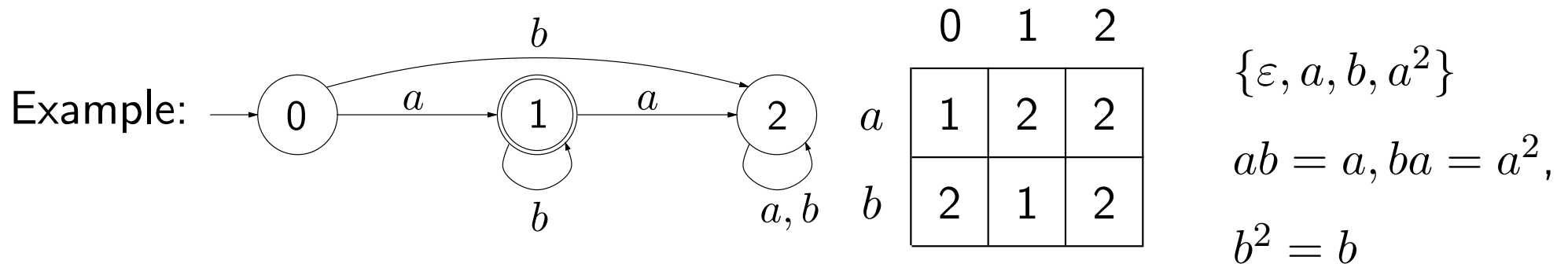
ie,  $\forall M \in \mathbf{V}$  and  $\eta : A^* \rightarrow M$   $\eta(u) = \eta(v)$

# $\mathcal{R}$ -trivial monoids

Important pv: syntactical methods working for  $\mathcal{R}$  often work for the larger pv  $\mathcal{DA}$

Monoids generated by classes of transformations on a finite chain

- either the class of total increasing transformations [Eil?].
- or that of partial increasing + order preserving [Hig95].



A monoid  $M$  is  $\mathcal{R}$ -trivial iff for all  $x, y \in M$ ,  $(xy)^\omega = (xy)^\omega x$ .

## $\omega$ -terms over $R$

**Lemma** [AA89] Let  $u, v \in F_A^\omega$  such that

- $u = u_1 a u_2$ ,  $\text{alph}(u_1) = \text{alph}(u) \setminus \{a\}$
- $v = v_1 b v_2$ ,  $\text{alph}(v_1) = \text{alph}(v) \setminus \{b\}$ .

Then  $R \models u = v$  iff  $a = b$ ,  $R \models u_1 = v_1$  and  $R \models u_2 = v_2$ .

$F_A^\omega R = F_A^\omega / \sim$  where  $u \sim v$  iff  $R \models u = v$ .

The **left basic factorization**  $(u_1, a, u_2)$  of  $u \in F_A^\omega R$  is given by

$$u = u_1 a u_2 \text{ with } \text{alph}(u_1) = \text{alph}(u) \setminus \{a\}$$

Example:

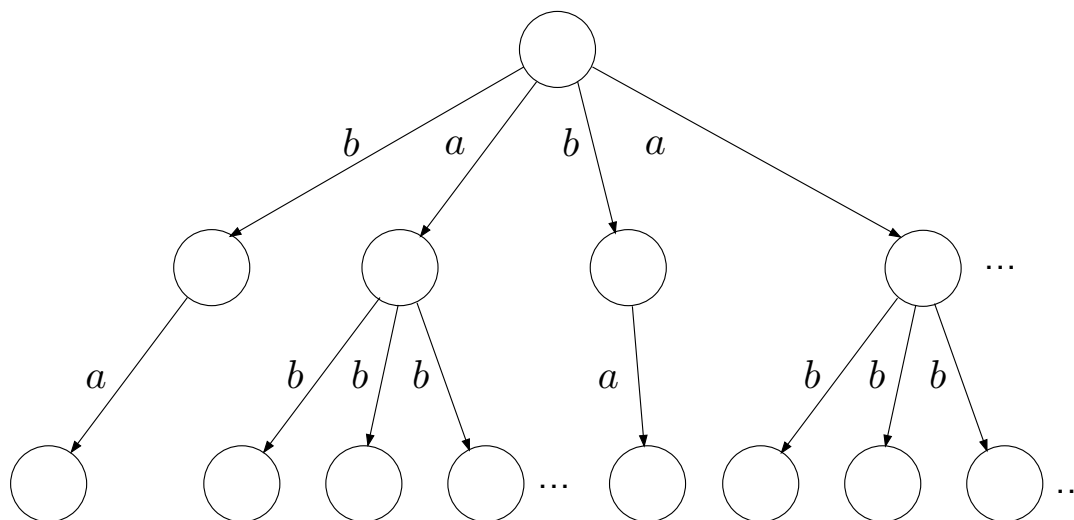
$$\begin{aligned} (ab^\omega ca)^\omega &= (ab^\omega ca)(ab^\omega ca)^\omega \\ &= \underbrace{ab^\omega}_{u_1} \cdot c \cdot \underbrace{a(ab^\omega ca)^\omega}_{u_2} \end{aligned}$$

# Representations of $\omega$ -terms over $\mathcal{R}$

Idea: iterate the left-basic factorization on both  $u_1$  and  $u_2$  [AW97]

- As labeled ordinals  $(ab^\omega a)^\omega : a \underbrace{bbbb \dots}_\omega \underbrace{aa \underbrace{bbbb \dots}_\omega \underbrace{aa \underbrace{bbbb \dots}_\omega \dots}_\omega}$

- As edge labeled trees



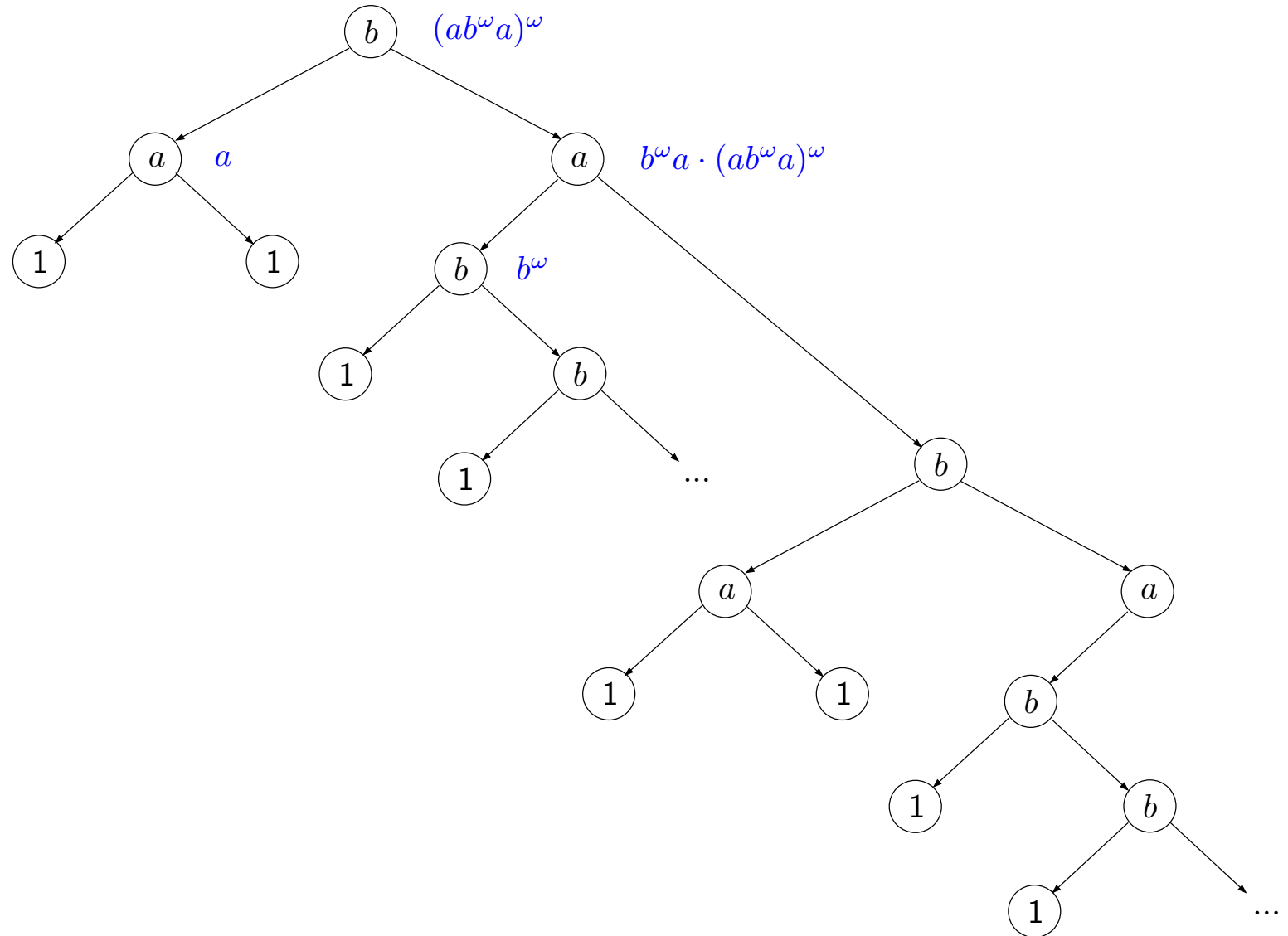
- For the  $\omega$ -word problem: as binary trees.

# Representation of $\omega$ -terms over $\mathcal{R}$ by binary trees

$u = u_1 \cdot a \cdot u_2 \rightsquigarrow \text{tree } \mathcal{T}(u)$  • Label the root by  $a$

- Iterate on the left with  $u_1$ , on the right with  $u_2$ .

Example:  $(ab^\omega a)^\omega$

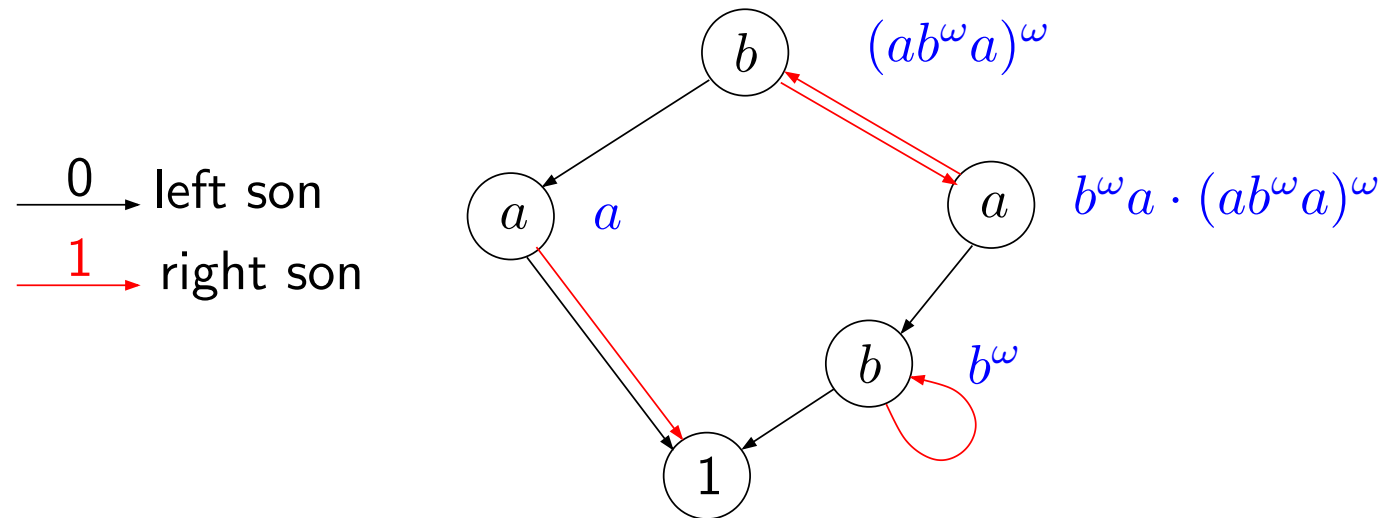


# Minimal folding of R-trees

**Proposition** For any  $\omega$ -term  $u$ , the tree  $\mathcal{T}(u)$  is regular

There is a unique minimal folding  $\mathcal{A}(u)$  which is finite.

Two  $\omega$ -terms are equal over  $\mathbf{R}$  iff they have the same folding.



One can also get a characterization of the automata arising this way.

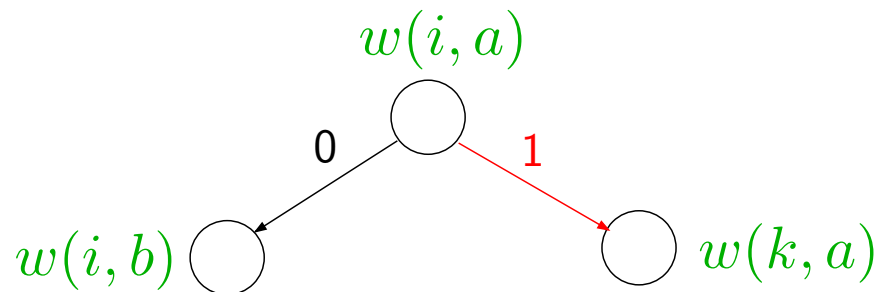
To solve the word problem for  $\omega$ -terms, it remains to compute this folding.





# Computing folded trees

**Lemma** The left basic factorization of  $w(i, a)$  is  $w(i, b) \cdot b \cdot w(k, a)$  where  $b$  is the last letter encountered in  $w(i, a)$ , at position  $k$ .



Example:  $w\# = z = \begin{matrix} & 0 & 1 & 2 & 3 & 4 & 5 & 6 & & 7 & 8 & 9 \\ ( & b & ( & a & b & )^\omega & c & )^\omega & \# \end{matrix}$

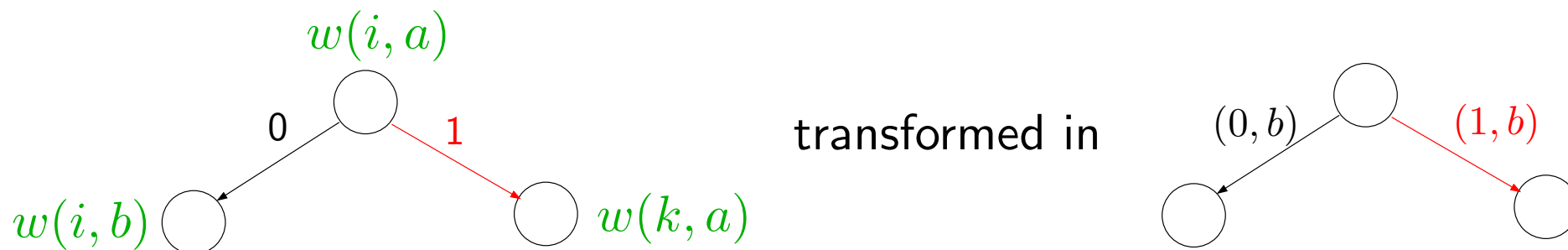
	$a$	$b$	$c$	$\#$
0	$b$	$\varepsilon$	$b(ab)^\omega$	$w$
...	...	...	...	...
7	$b$	$\varepsilon$	$b(ab)^\omega$	$w$

Left basic factorization of  $w = z(0, \#)$ :  $z(0, c) \cdot c \cdot z(7, \#) = b(ab)^\omega \cdot c \cdot w$ .



# An algorithm for solving the $\omega$ -wp on $\mathbb{R}$

One can transform the folding obtained so far to an automaton on  $\{0, 1\} \times A$ .



To test equality of  $u$  and  $v$ , build their associated automata, in time  $O(|A||uv|)$ , and minimize them.

The size of the automaton for  $u$  is  $O(|A||u|)$ .

Using Hopcroft minimization algorithm, we get

**Proposition** The word problem for  $\omega$  terms over  $\mathbb{R}$  can be solved in time  $O(|A|^2 n \log(|A|n))$ .

## Minimization in linear time

The automata we get by the previous algorithm have strong properties.

- At most two transitions,  $(0, a)$  and  $(1, a)$  from a given state.
- If a  $(0, a)$  transition is taken, no more  $(i, a)$  transitions can be seen.
- Cycles only involve  $(1, a)$  transitions: very few cycles.
- Cycles are **disjoint**.
- For cycle-free automata, the minimization is linear [Rev92].

Revuz's algorithm can be adapted here:

**Proposition** The word problem for  $\omega$  terms over  $\mathbf{R}$  can be solved in  $O(n|A|)$ -time.

# Minimization in linear time: ideas of the proof

For acyclic automata [Rev92]

- compute for each state the longest path from it (**height**).
- proceed bottom-up, identifying states at the same height only.

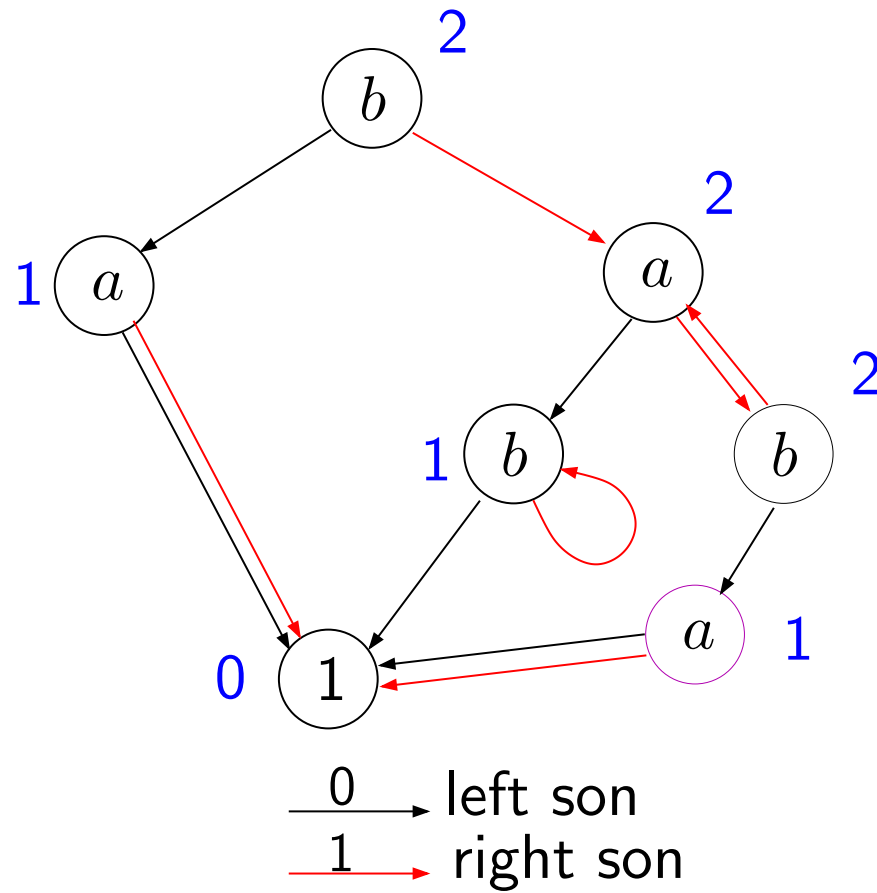
For  $\mathcal{R}$ -automata, let  $\zeta(q) = (a, q.0)$  where  $(0, a)$  labels the left transition.

- compute the height, assigning weight 0 to edges of cycles.
- then, from height 0 to the maximal height:
  - roll paths coming to a cycle around the cycle if possible.
  - for each cycle  $(q_1, \dots, q_k)$ , compute smallest conjugate of  $\zeta(q_1) \cdots \zeta(q_k)$  [Bl80] and merge states in the cycle accordingly.
  - identify equal cycles.
  - merge states not on a cycle (similar to [Rev92]).

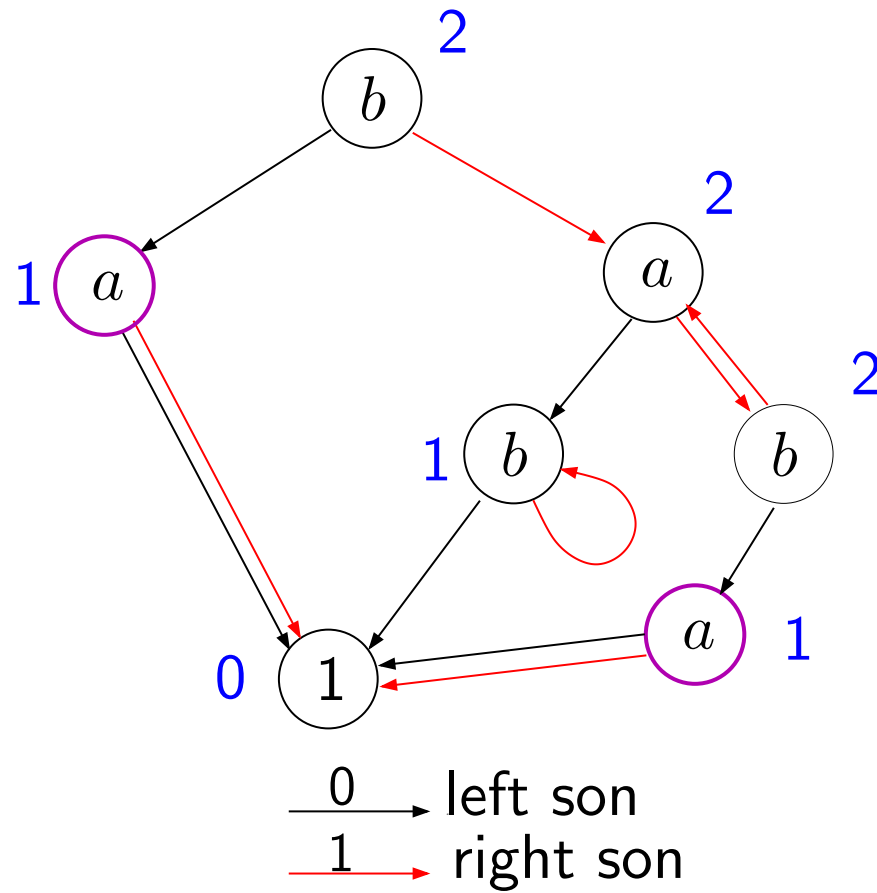
To identify equal cycles and merge cycles and states, bucket sort.

Heights of states above present level might become incorrect  $\Rightarrow$  height updates.

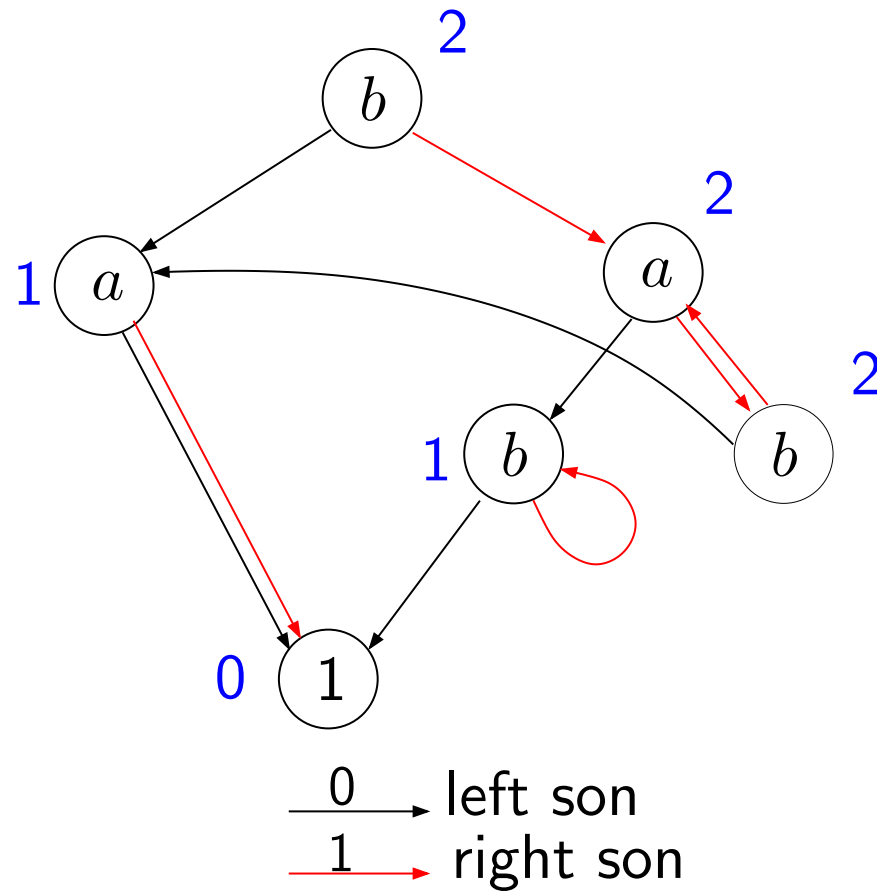
# Minimization: example



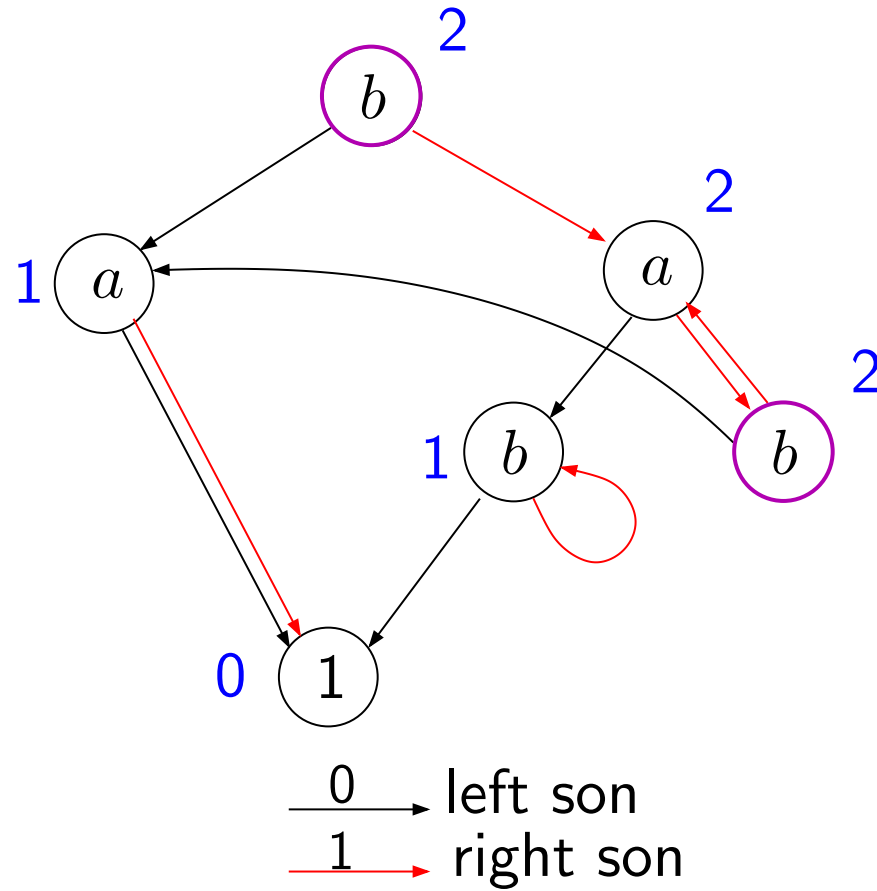
# Minimization: example



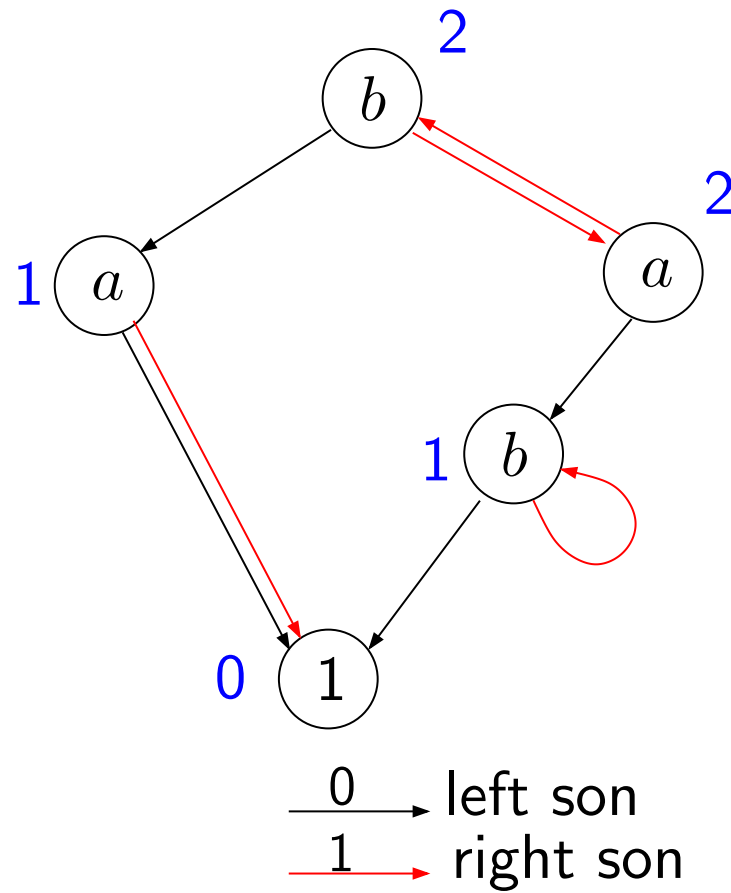
# Minimization: example



# Minimization: example



# Minimization: example



# Canonical form

Another approach: try to get a confluent Noetherian system of rewriting rules.

Natural approaches (reducing the length, start the period as soon as possible, using KB algorithm etc.) do not work well.

One associates to an  $\mathbf{R}$ -automaton  $\mathcal{A}$  a canonical form  $\text{cf}(u)$ .

- If  $\mathcal{A}$  is the trivial  $\mathbf{R}$ -automaton,  $\text{cf}(\mathcal{A}) = 1$ ;
- if the initial state  $r$ , labeled  $a$ , is not the end of an edge labeled 1, then  $\text{cf}(\mathcal{A}) = uav$  where  $u = \text{cf}(\mathcal{A} \cdot 0)$  and  $v = \text{cf}(\mathcal{A} \cdot 1)$ .
- otherwise  $\text{cf}(\mathcal{A}) = (uav)^\omega$  where  $u = \text{cf}(\mathcal{A} \cdot 0)$  and  $v = \text{cf}(\widetilde{\mathcal{A}} \cdot 1)$ .

Then define  $\text{cf}(u) = \text{cf}(\mathcal{A}(u))$  where  $\mathcal{A}(u)$  is the minimal  $\mathbf{R}$ -automaton of  $u$ .

The canonical form of  $u$  can be of exponentially longer (or shorter).

$$w_k = (\cdots ((a_1 a_1 b_1 b_1)^\omega a_2 a_2 b_2 b_2)^\omega \cdots a_k a_k b_k b_k)^\omega.$$

It is used to find a basis of the variety of  $\omega$ -monoids generated by  $\mathbf{R}$ .

# The variety $\mathbf{R}^\omega$

**Proposition** The identities  $\Sigma$

$$x(yx)^\omega = (xy)^\omega = (xy)^\omega x$$

$$(x^\omega)^\omega = x^\omega$$

$$(x^r)^\omega = x^\omega \quad (r \geq 2)$$

form a basis for the variety  $\mathbf{R}^\omega$  of  $\omega$ -semigroups generated by  $\mathbf{R}$ .

**Proof.** (technical) Show that  $\Sigma \vdash u = \text{cf}(u)$

Note:  $\mathbf{R}^\omega \subsetneq \mathcal{V}$ : for instance the ordinal  $\omega + 1$ , labeled with only one letter, is a counterexample to the identity  $x^\omega x = x^\omega$ .

Neither model for the solution of one of the word problems seems to be adequate to handle the other.

**Proposition**  $\mathbf{R}^\omega$  is not finitely based.

# Pseudowords

$\omega$ -terms over  $\mathbf{V}$  are special instances of pseudowords.

$u, v \in A^*$ ,  $d_{\mathbf{V}}(u, v) = 2^{-r(u, v)}$  where  $r(u, v) = \min |\{M \in \mathbf{V}, M \not\models u = v\}|$

$u$  and  $v$  are not distinguishable by monoids of  $\mathbf{V}$  ( $u \sim_{\mathbf{V}} v$ ) iff  $d_{\mathbf{V}}(u, v) = 0$ .

Then  $d_{\mathbf{V}}$  is a distance over  $A^*/\sim_{\mathbf{V}}$ .

$\bar{F}_A \mathbf{V}$ : topological completion of  $(A^*/\sim_{\mathbf{V}}, d_{\mathbf{V}})$  is the monoid of pseudowords.

# Pseudowords

$\omega$ -terms over  $\mathbf{V}$  are special instances of pseudowords.

$u, v \in A^*$ ,  $d_{\mathbf{V}}(u, v) = 2^{-r(u, v)}$  where  $r(u, v) = \min |\{M \in \mathbf{V}, M \not\models u = v\}|$

$u$  and  $v$  are not distinguishable by monoids of  $\mathbf{V}$  ( $u \sim_{\mathbf{V}} v$ ) iff  $d_{\mathbf{V}}(u, v) = 0$ .

Then  $d_{\mathbf{V}}$  is a distance over  $A^*/\sim_{\mathbf{V}}$ .

$\bar{F}_A \mathbf{V}$ : topological completion of  $(A^*/\sim_{\mathbf{V}}, d_{\mathbf{V}})$  is the monoid of pseudowords.

$\bar{F}_A \mathbf{V}$  contains the  $\omega$ -terms: for  $x \in A^+$  and for  $\varphi : A^* \rightarrow M \in \mathbf{V}$ ,

$$\varphi(x^{n!}) = \varphi(x)^\omega \text{ for } n \text{ large enough.}$$

Hence  $M \models x^{n!} = x^{(n+k)!}$  and the sequence  $(x^{n!})$  converges to  $x^\omega$ .

# Pseudowords

$\omega$ -terms over  $\mathbf{V}$  are special instances of pseudowords.

$u, v \in A^*$ ,  $d_{\mathbf{V}}(u, v) = 2^{-r(u, v)}$  where  $r(u, v) = \min |\{M \in \mathbf{V}, M \not\models u = v\}|$

$u$  and  $v$  are not distinguishable by monoids of  $\mathbf{V}$  ( $u \sim_{\mathbf{V}} v$ ) iff  $d_{\mathbf{V}}(u, v) = 0$ .

Then  $d_{\mathbf{V}}$  is a distance over  $A^*/\sim_{\mathbf{V}}$ .

$\overline{F}_A \mathbf{V}$ : topological completion of  $(A^*/\sim_{\mathbf{V}}, d_{\mathbf{V}})$  is the monoid of pseudowords.

$\overline{F}_A \mathbf{V}$  contains the  $\omega$ -terms: for  $x \in A^+$  and for  $\varphi : A^* \rightarrow M \in \mathbf{V}$ ,

$$\varphi(x^{n!}) = \varphi(x)^\omega \text{ for } n \text{ large enough.}$$

Hence  $M \models x^{n!} = x^{(n+k)!}$  and the sequence  $(x^{n!})$  converges to  $x^\omega$ .

**Theorem** (analogous to [BC'01])  $w \in \overline{F}_A \mathbf{R}$ . Following conditions are equivalent

- $w$  is an  $\omega$ -term.
- the set of tails of  $w$  is finite.
- $\mathcal{A}(w)$  is finite.
- the set of factors of  $w$  is finite.

# Reducibility problem

Defined in [AS98] in a more general form.

- Set  $X = \{x_1, \dots, x_k\}$  of variables,
- Morphism  $\varphi : A^* \rightarrow T$  and for each  $x_i \in X$ , an element  $t_i \in T$ .
- Equations  $y, z \in X^*$  having a word-solution in all  $A$ -generated  $A^* \xrightarrow{\eta} M \in \mathbf{V}$

$$\forall A^* \xrightarrow{\eta} M \in \mathbf{V}, \exists \delta = \delta_M : X^* \rightarrow A^* \text{ such that } \begin{cases} \eta \circ \delta(y) = \eta \circ \delta(z) \\ \forall x_i \in X, \varphi \circ \delta(x_i) = t_i \end{cases}$$

$\mathbf{V}$  is **reducible** if the system of equations  $\{y = z\}$  has a **uniform** solution

$$\delta' : X \rightarrow F_A^\omega$$

on  $\mathbf{V}$  in  **$\omega$ -terms** under the constraint  $\varphi$ :

$$\mathbf{V} \models \delta'(y) = \delta'(z)$$

$$\forall x_i \in X, \varphi \circ \delta'(x_i) = t_i$$

# Reducibility and $\omega$ -word problem

Sufficient condition for decidability, more robust under operations on ps-varieties.

For instance, if  $\mathbf{V}$  is recursively enumerable, reducible, and has a decidable  $\omega$ -WP, then  $\mathbf{V}$  is decidable. (In fact, much more [AS98])

**Proof** Semi-alg. to decide  $M \notin \mathbf{V}$ :

**Theorem** [Rei82] For any psv.  $\mathbf{V}$ , there exist  $u_i, v_i \in \bar{F}_A M$  such that  $\mathbf{V}$  is the class of monoids satisfying all  $u_i = v_i$ .

$$\mathbf{V} = \llbracket u_i = v_i, i \in I \rrbracket$$

Hence  $M \notin \mathbf{V}$  iff  $\exists i, M \not\models u_i = v_i$ .

# Reducibility and $\omega$ -word problem

Sufficient condition for decidability, more robust under operations on ps-varieties.

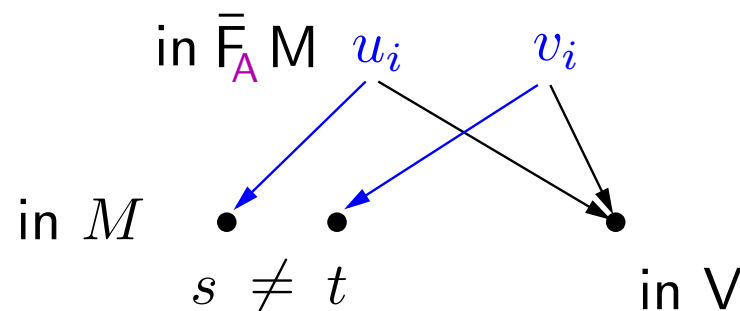
For instance, if  $V$  is recursively enumerable, reducible, and has a decidable  $\omega$ -WP, then  $V$  is decidable. (In fact, much more [AS98])

**Proof** Semi-alg. to decide  $M \notin V$ :

**Theorem** [Rei82] For any psv.  $V$ , there exist  $u_i, v_i \in \bar{F}_A M$  such that  $V$  is the class of monoids satisfying all  $u_i = v_i$ .

$$V = \llbracket u_i = v_i, i \in I \rrbracket$$

Hence  $M \notin V$  iff  $\exists i, M \not\models u_i = v_i$ .



# Reducibility and $\omega$ -word problem

Sufficient condition for decidability, more robust under operations on ps-varieties.

For instance, if  $\mathbf{V}$  is recursively enumerable, reducible, and has a decidable  $\omega$ -WP, then  $\mathbf{V}$  is decidable. (In fact, much more [AS98])

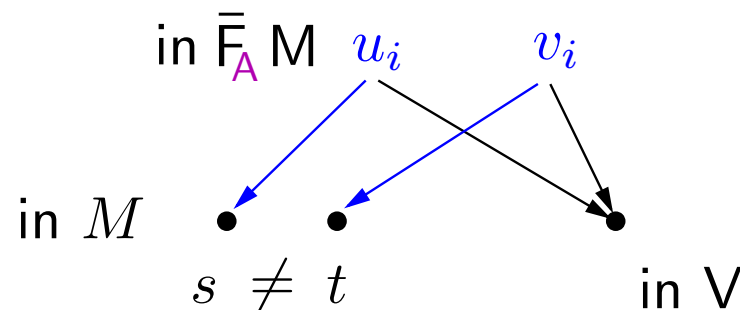
**Proof** Semi-alg. to decide  $M \notin \mathbf{V}$ :

**Theorem** [Rei82] For any psv.  $\mathbf{V}$ , there exist  $u_i, v_i \in \bar{F}_A M$  such that  $\mathbf{V}$  is the class of monoids satisfying all  $u_i = v_i$ .

$$\mathbf{V} = \llbracket u_i = v_i, i \in I \rrbracket$$

Hence  $M \notin \mathbf{V}$  iff  $\exists i, M \not\models u_i = v_i$ .

Use reducibility for equation  $x_1 = x_2$



# Reducibility and $\omega$ -word problem

Sufficient condition for decidability, more robust under operations on ps-varieties.

For instance, if  $\mathbf{V}$  is recursively enumerable, reducible, and has a decidable  $\omega$ -WP, then  $\mathbf{V}$  is decidable. (In fact, much more [AS98])

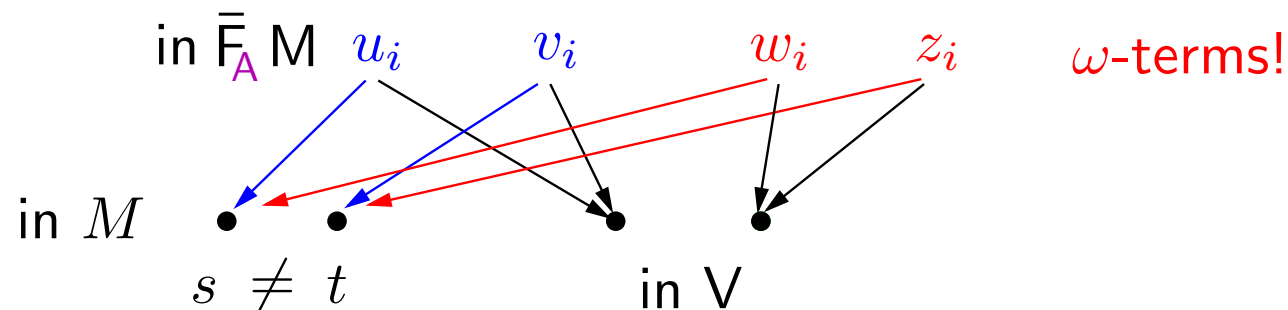
**Proof** Semi-alg. to decide  $M \notin \mathbf{V}$ :

**Theorem** [Rei82] For any psv.  $\mathbf{V}$ , there exist  $u_i, v_i \in \bar{F}_A M$  such that  $\mathbf{V}$  is the class of monoids satisfying all  $u_i = v_i$ .

$$\mathbf{V} = \llbracket u_i = v_i, i \in I \rrbracket$$

Hence  $M \notin \mathbf{V}$  iff  $\exists i, M \not\models u_i = v_i$ .

Use reducibility for equation  $x_1 = x_2$



Enumerate the  $(w, z, s, t) \in F_A^{\omega 2} \times M^2$  and test equality on  $\mathbf{V}$  ( $\omega$ -WP) and  $M$ .

# Reducibility of $\mathcal{R}$

**Proposition**  $\mathcal{R}$  is reducible for equation systems associated with a graph.

A variable is associated to each edge or vertex.

An edge  $x \xrightarrow{y} z$  produces an equation  $xy = z$ .

**Applications** (with JA and JC Costa)

The join  $\mathcal{V} \vee \mathcal{W}$  is the smallest psv. containing both  $\mathcal{V}$  and  $\mathcal{W}$ .

The join of “simple” decidable psvs. might not be decidable ( $\mathcal{V} \vee \text{Com}$  [ABR92]).

**Proposition** The joins  $\mathcal{R} \vee \mathcal{G}$ ,  $\mathcal{R} \vee \text{Ab}$ , ... are decidable.

Proofs rely also on reducibility for graph systems of  $\mathcal{G}$  [Ash91] and  $\text{Ab}$  [Del98].

## Further work

- Reducibility of  $\mathcal{R}$  for general equation systems. Very partial results for dual systems ( $yx = z$  instead of  $xy = z$ ).