# Polynomially Bounded Matrix Interpretations

Johannes Waldmann, HTWK Leipzig

# Derivational Complexity...

- (derivation) relation $\to$ on domain $D$,
- size measure $|\cdot| : D \to \mathbb{N}$,

derivation height of $s$ w.r.t. $\to$:

$$\mathrm{dh}_{\to}(s) := \sup\{k \mid \exists t : s \to^k t\}$$

derivational complexity of $\to$:

$$\mathrm{dc}_{\to} := n \mapsto \sup\{\mathrm{dh}_{\to}(s) \mid n \geq |s|\}$$

# …of (String) Rewriting

- $\{0 \to 1\}$ is linear

  $$0^k \to^k 1^k$$

- $\{01 \to 10\}$ is quadratic

  $$01^k \to^k 1^k0,\ 0^i1^k \to^{i \cdot k} 1^k0^i$$

- $\{01 \to 110\}$ is exponential

  $$01^k \to^k 1^{2k}0,\ 0^i1 \to^* 1^{2^i}0^i$$

- etc.

# Matrix Interpretations

mapping $[\cdot] : \Sigma \to \mathbb{N}^{d\times d}$, extended to $\Sigma^* \to \mathbb{N}^{d\times d}$,

- compatibility: $\forall (l \to r) \in R$ :
  $[l] - [r] \in \mathbb{N}^{d\times d}, ([l] - [r])_{\text{top,right}} > 0$
- monotonicity w.r.t. left and right multiplication (contexts and substitutions)
  $\forall c \in \Sigma : [c]_{\text{top,left}} \geq 1, [c]_{\text{bottom,right}} \geq 1$

Example, w.r.t. $R = \{ab \to ba\}$

$[a]=\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, [b]=\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}; \qquad [ab]=\begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix}, [ba]=\begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}$

# Interpretations & Complexity

existence of compatible monotone maxtrix interpretation

- proves termination,
- bounds derivational complexity.
  - in general, by an exponential function,
  - for certain matrices, by a polynomial.

# String $\to$ Term Rewriting

- same question: bound derivational complexity,
- use path-separated weighted tree automata, where interpretation of $k$-ary function symbol is $(\vec{x_1}, \ldots, \vec{x_k}) \mapsto M_1\vec{x_1} + \ldots + M_k\vec{x_k} + \vec{a}$
- interpretation of term (tree) $t$ is sum of interpretations of paths (strings)
- compute bound for corresponding word matrix interpretation (use all the $M_i$, ignore $\vec{a}$)
- add one to the resulting degree

# Upper triangular form

interpretation is upper triangular if

$$\forall c, i, j : ((i > j) \Rightarrow [c]_{i,j} = 0) \wedge ((i = j) \Rightarrow [c]_{i,j} \leq 1)$$

$$\begin{array}{cccc} a & b & ab & ba \\ \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \end{array}$$

Upper triangular interpretation gives polynomial bound on derivational complexity.

degree $\leq$ dimension - 1.

# Other Matrix Forms

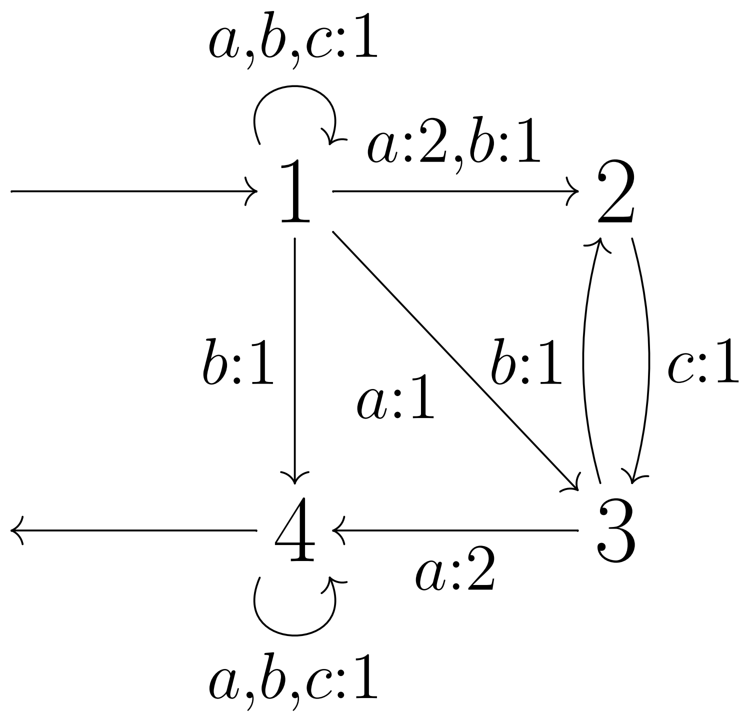
there are matrix interpretations with polynomial growth but not of upper triangular form. Example:

$$a \mapsto \begin{pmatrix} 1 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$b \mapsto \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$c \mapsto \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

as weighted automaton:




and these are needed, see example in paper.

# Non-Triangularity is Needed

rewriting system:

$$Ra^2 \to a^2R, RX \to LX, a^2L \to La^2, XL \to XRa$$

typical derivation:

$$XRa^{2k}X \to^* Xa^{2k}RX \to Xa^{2k}LX \to^*$$
$$XLa^{2k}X \to XRa^{2k+1}X \to^* Xa^{2k}RaX$$

termination depends on counting mod 2

system does not admit a compatible upper triangular interpretation (counting would need a loop).

# Deciding Polynomial Growth

Algorithm:

1. compute strongly connected components $A_1, \ldots, A_k$ of underlying graph.
2. if there is any arrow with weight $> 1$ inside one component, then growth is exponential.
3. consider each $A_i$ as classical automaton. if any $A_i$ contains a diamond ($=$ distinct paths with identical start, label, end), then $A$ grows exponentially. — Otherwise, polynomially.

Notes: degree is $<$ maximal number of SCCs on a chain of SCCs, this bound is not sharp.

# Diamonds

Diamond $=$ pair of distinct paths with identical start, label, end.

$$\begin{tikzcd} p \arrow[r, bend left, "w"] \arrow[r, bend right, "w"'] & q \end{tikzcd}$$

no diamond $=$ strong form of non-ambiguity

Thm: $A$ contains no diamond iff

- the reduced form (all states reachable and productive)
- of $A \times A$ (cartesian product construction)
- consists of the main diagonal only.

(cf. Sakarovitch: Theorie des Automates)

# Related (and much Earlier)

- Ambiguity of finite automata
  Ibarra and Ravikumar, Weber and Seidl
- DT0L growth
  Rosenberg, Salomaa
- $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$-rational series
  Berstel, Reutenauer

so . . . what's new?

# Implementation

in the context of termination provers:
given a rewrite system $R$, numbers $d, g$:
construct a constraint system for an unknown matrix interpretation $[\cdot]$ of dimension $d$:

- $[\cdot]$ is monotonic and compatible with $R$ (non-linear arithmetic constraint)
- $[\cdot]$ is polynomially bounded with degree $\leq g$. (finite domain constraint)

Then feed the complete system to a constraint solver. (Matchbox uses bit-blasting to Minisat.)

# Constraints for SCCs

$Q =$ indices of matrices $=$ states of automaton

- relation $C \subseteq Q^2$ "reachable":
  - $p \xrightarrow{c:w}_A q \wedge w > 0 \Rightarrow C(p, q)$,
  - $C$ is transitive: $C \circ C \subseteq C$
- relation $S \subseteq Q^2$ "strongly connected":
  - $S = C \cap C^-$,
  - $p \xrightarrow{c:w}_A q \wedge w > 1 \Rightarrow \neg S(p, q)$,
- $T(p, q) := S(p, p) \wedge (C \setminus C^-)(p, q) \wedge S(q, q)$, height of $T \leq b$ (use unary encoding)

# Constraints for Diamonds

- define $M \subseteq Q^4$: move relation of $A \times A$:
  $$M = \{((p_1, p_2), (q_1, q_2)) \mid S(p_1, q_1), S(p_2, q_2), \\ \exists c \in \Sigma : p_1 \rightarrow_c q_1 \wedge p_2 \rightarrow_c q_2)\}$$
- set $R \subseteq Q^2$:
  states in $A \times A$ reachable from diagonal
  $$\text{diag} \subseteq R \wedge M(R) \subseteq R$$
- set $P \subseteq Q^2$:
  states in $A \times A$ reaching the diagonal
  $$\text{diag} \subseteq P \wedge M^-(P) \subseteq P$$
- reduced automaton consists of diagonal only:
  $$R \cap P \subseteq \text{diag}$$

# Over-Approximation

- The given construction over-approximates strong connectivity.
  (Necessarily so. No easy way to encode “the smallest transitive $C$ such that $\ldots$”)
- This is actually good: it might unify adjacent SCCs (if their union is still diamond-free),
- and thus reduce the height of the chains (the degree of the bound).

see example in the paper.

# Degree Reduction by Approx.

SCCs:
$\{1\}, \{2, 4\}, \{3, 5\}$

merge $\{1\}$
with $\{2, 4\}$

result $\{1, 2, 4\}$ is
still diamond-free

# Summary, Discussion

summary:

- define non-triangular polynomially bounded interpretations
- decide polynomial growth of $\mathbb{N}$-matrix interpretations, encode as constraint system

open, ongoing, related:

- (non-)completeness
- polynomially bounded interpretation for $\{a^2 \to bc, b^2 \to ac, c^2 \to ab\}$
- polynomially bounded $\mathbb{Q}$-matrix interpretations (Friedrich Neurauter)