Automatic Certification of Polynomial Derivation Lengths in String Rewriting

Johannes Waldmann, HTWK Leipzig

String Rewriting

- string rewriting system R is set of rules
- rule $=$ pair of strings
- apply a rule (l, r) to a string u:
  split $u = x \cdot l \cdot y$, obtain $x \cdot r \cdot y = v$
- one-step rewrite relation $u \to_R v$

example: $R = \{ab \to ba\}$,
$a\underline{ab}b \to_R ab\underline{ab} \to_R \underline{ab}ba \to_R b\underline{ab}a \to_R bbaa$
(cf. bubble sort)

Derivational Complexity

For a terminating rewrite system R, how long can $\longrightarrow_R$-derivations be, as a function of the length of the start word?

$$\mathrm{dc}_{\to}(s) = \max\{k \mid |u| \leq s, \exists v : u \longrightarrow_R^k v\}$$

Examples:

- linear: $a \to b$
- quadratic: $ab \to ba$ (bubblesort)

Transformations

definition of $\mathrm{dc}_{\to}$ works for any relation $\to$ on a domain D with a size function $|\cdot| : D \to \mathbb{N}$.

- order-preserving mapping
  $f : (D, >_D) \to (E, >_E)$
  $x >_D y \Rightarrow f(x) >_E f(y)$
- then $\forall s : \mathrm{dc}_D(s) \leq \mathrm{dc}_E(f^{\|}(s))$
  where $f^{\|}(s) = \max\{|f(x)|_E \mid |x|_D \leq s\}$

Example: $D = \Sigma^*, >_D = \to_R, E = \mathbb{N}, >_E = >$
for $\Sigma = \{a, b\}, R = \{a \to b\}$,
take $f(w) = |w|_a$, then $f^{\|}(s) = s$.

Algebras

- transformation $f : \Sigma^* \longrightarrow E$ given by actions of letters $\Sigma \longrightarrow (E \longrightarrow E)$
- interpretation $[\cdot]$ maps empty word ϵ to $[\epsilon] \in E$ and each letter $a \in \Sigma$ to function $[a] : E \longrightarrow E$,
- then $[a_1 a_2 \ldots a_n] = [a_1][a_2] \ldots [a_n][\epsilon]$

e. g. $|w|_a$ (number of letters) given by
$[\epsilon] = 0, [a] = x \mapsto x + 1, [b] = x \mapsto x$

these are linear mappings. . . represent as matrices

Matrix Interpretations

$E = \{v \mid v \in \mathbb{N}^d, v_d \geq 1\}$ (as column vectors)
$x >_E y \iff x_1 > y_1 \land x_2 \geq y_2 \land \ldots \land x_n \geq y_n$
interpret letter a by matrix $[a] \in \mathbb{N}^{d \times d}$ with
$[a]_{1,1} \geq 1 \land [a]_{d,d} \geq 1$
empty word by $(0, \ldots, 0, 1)^T$
interpretation is compatible with R if

$$\forall (l \to r) \in R : ([l]_{1,d} > [r]_{1,d} \land \forall i, j : [l]_{i,j} \geq [r]_{i,j})$$

Then $[\cdot]$ is order-preserving from $\to_R$ to $>_E$.
Thus $\mathrm{dc}_R(s) \leq \sup\{[w]_{1,d} : |w| \leq [s]^{\|}\}$

Example

$$R = \{ab \to ba\},\ a \mapsto \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, b \mapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

$$[a] \begin{pmatrix} x \\ 1 \end{pmatrix} = \begin{pmatrix} 2x \\ 1 \end{pmatrix}, [b] \begin{pmatrix} x \\ 1 \end{pmatrix} = \begin{pmatrix} x+1 \\ 1 \end{pmatrix}.$$

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

$$[aa\underline{ab}] = \begin{pmatrix} 8 & 8 \\ 0 & 1 \end{pmatrix}, [aa\underline{ba}] = \begin{pmatrix} 8 & 4 \\ 0 & 1 \end{pmatrix}$$

Tight bounds

For $R = \{ab \to ba\}$, previous interpretation $[\cdot]$ is compatible, but not tight:

$$[a^k b] = \begin{pmatrix} 2^k & 2^k \\ 0 & 1 \end{pmatrix} \text{ but } \mathrm{dc}_{\to_R}(a^k b) = k$$

"better" interpretation:

$$[a](x, y, 1) = (x + y, y, 1), [b](x, y, 1) = (x, y + 1, 1)$$

$$[ab](x, y, 1) = (x + y + 1, y + 1, 1),$$

$$[ba](x, y, 1) = (x + y \qquad , y + 1, 1).$$

this interpretation is quadratically bounded,

$$[w]_{1,2} \leq [a^{|w|}]_{1,2} = \sum \{k \mid 1 \leq k \leq |w|\} = \Theta(|w|^2)$$

Upper triangular form

$m \in \mathbb{N}^{d \times d}$ is upper triangular if

$\forall i, j : (i > j \Rightarrow m_{i,j} = 0) \wedge (i = j \Rightarrow m_{i,j} \in \{0, 1\})$

Example (previous slide):

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

Let $[\cdot] : \Sigma \to U$. Then

$(n \mapsto \max\{[w]_{i,j} \mid w \in \Sigma^n\}) \in O(n^{j \dot{-} j})$.

upper triangular interpretation gives polynomial bound on derivational complexity

Polynomial Derivations

R_d over $\Sigma = \{1, 2, \ldots, d\}$ with rules

$$\{ki \to jk \mid i < k \wedge j < k\}$$

E.g. $R_2 = \{21 \to 12\}$, $R_3 = \{21 \to 12, 31 \to 13, 31 \to 21, 32 \to 13, 32 \to 23\}$

Derivation with $\approx n^d$ steps:

$$w = d^n (d-1)^n \ldots 1^n \to^* \{1, 2, \ldots, d\}^{n^2}$$

Bound for derivation lengths: letter k at position p (counting from right end) gets weight $\binom{p}{k-1}$.

Total weight is $\leq |w|^d$.

Upper Triangular Form: Example

Interpretation for $R_d = \{ki \to jk \mid i < k \wedge j < k\}$:

$$i \mapsto \begin{pmatrix} 1 & 0 & 0 & \boxed{1} & \ldots & 0 \\ 0 & 1 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & 1 & & \\ \ldots & & & & & \\ 0 & 0 & 0 & \ldots & 1 & 1 \\ 0 & 0 & 0 & \ldots & 0 & 1 \end{pmatrix}$$

in first row, entry 1 at positions 1 and $d + 1 - i$.

Other Matrix Forms

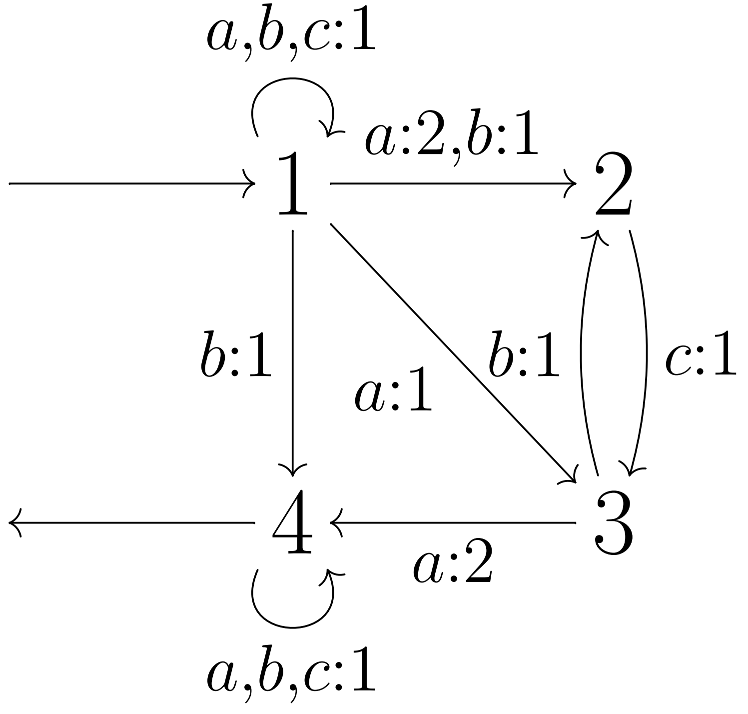
there are matrix interpretations with polynomial growth but not of upper triangular form. Example:

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

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

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

as weighted automaton:



Is $\mathbb{N}$-Automaton polynomial?

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. from each component A_i, construct a (classical) automaton (incoming arrow $\Rightarrow$ initial state, outgoing arrow $\Rightarrow$ final state)
4. if any A_i is ambiguous, then A is exponential.
5. Otherwise, A has polynomial growth.
6. degree is $<$ maximal number of nontrivial SCCs on a chain of SCCs.

Symbolic Computation

- find compatible matrix interpretation by constructing a constraint system (inequalities for matrix entries)
- ensure polynomial growth by additional symbolic constraints
- solve by further translation to SAT

Symbolic Computation (II)

for interpretation $[\cdot]$, introduce growth vector
with entries g_k denoting polynomials,
for each letter $a \in \Sigma$, check that

$$g_i(n+1) \leq \sum [a]_{i,j} g_j(n).$$

(finite constraint system if max. degree is given)

optimization: instead of full polynomial, consider only degree and leading coefficient.

Summary, Discussion

- upper triangular form ensures polynomial growth, but does not cover all cases
- weighted automata method can decide polynomial growth of matrix interpretation
- symbolic constraint system helps find matrix interpretation with polynomial growth

open problem:

- is $\{a^2 \to bc, b^2 \to ac, c^2 \to ab\}$ polynomial?
- it is at least quadratic: $\underline{cc}\,\underline{aa} \to^2 a\underline{bb}c \to aacc$
- our 5×5 matrix interpretation is exponential