Well-structured extensions of pushdown systems

Mizuhito Ogawa (JAIST)

2012.9.18@RP12

Joint work with Cai Xiaojuan (SJTU)

This talk

- Models of (boolean-valued) multi-thread programs.
  - ✓Context-sensitive synchronization is *undecidable*.
    - –2-stacks PDA is Turing complete.
  - ✓Lots of models with restrictions for decidability.
    - –Context-bounded, atomicity, locking protocols, no synchronization.
  - ✓**Typical techniques**. Reduction to 1-stack PDS with infinite stack alphabet.

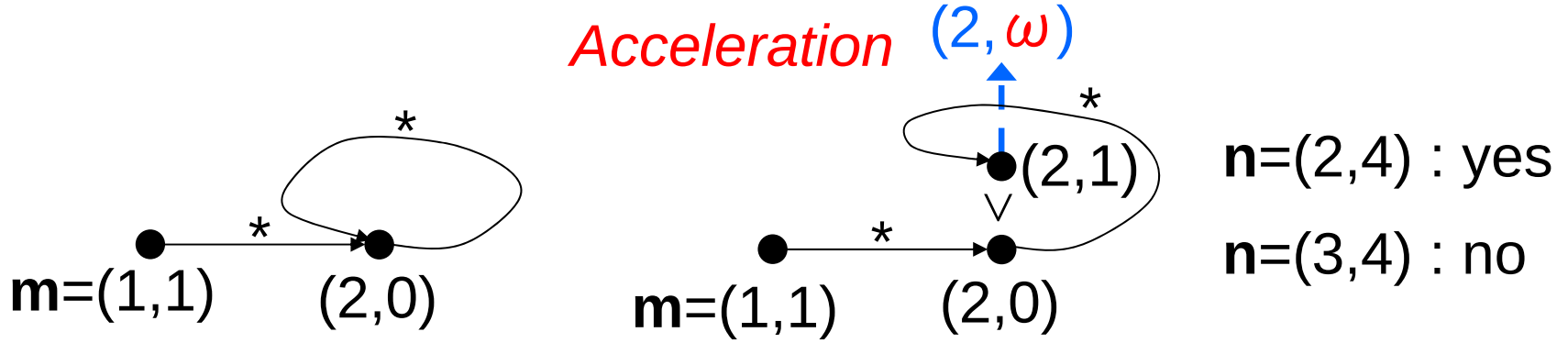
- **Aim**. Extend WSTS framework to (1-stack) PDS with WQO stack alphabet (e.g., $\mathbb{N}^k$) to show coverability.
  - ✓**Example**. Coverability of RVASS (POPL12), Multi-set PDS (CONCUR09) are decidable.

Classical coverability example. VAS (Perti net)

- VAS is a transition system on vectors $\mathbb{N}^k$ with transition rules $\mathbf{m} \rightarrow \mathbf{n}$ if $\mathbf{m} \geqq \mathbf{n}_1$ and $\mathbf{n} = \mathbf{m} - \mathbf{n}_1 + \mathbf{n}_2$.

- **Th**. Coverability of VAS (Perti net) is decidable.
  - ✓Given **m**, **n**, whether $\exists\, \mathbf{n}'.\ \mathbf{m} \rightarrow^* \mathbf{n}'$ and $\mathbf{n}' \geqq \mathbf{n}$.

- Two methodology
  - ✓*Post*: Acceleration (classical Karp-Miller tree)



  - ✓*Pre:* Monotonic WSTS

Well-quasi-ordering (WQO)

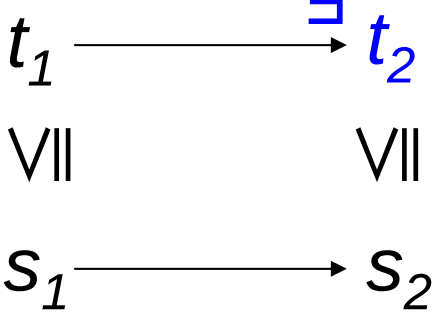
- **Def.** A QO $(A, \leqq)$ is WQO (well-quasi-ordering) if, for each infinite sequence $a_1, a_2, a_3, \ldots$ in A, there exist i, j such that $i < j$ and $a_i \leqq a_j$.

- **Example.**
  - ✓$(\mathbb{N}, \leqq)$ where $\leqq$ is *less-than-equal*
  - ✓$(A, =)$ where A is a finite set.
  - ✓$(\mathbb{N}^k, \leqq)$ where $\leqq$ is element-wise *less-than-equal*

- **Lemma**. Assume $(A, \leqq)$, $(A_1, \leqq_1)$, $(A_2, \leqq_2)$ are WQO.
  - ✓Dickson's lemma $(A_1 \times A_2, \leqq_1 \times \leqq_2)$ is a WQO.
  - ✓Higman's lemma (A*, embedding) is a WQO.

Well structured transition system (WSTS)

- **Def.** WSTS M = $((P, \leqq), s_0, \Delta)$ consists of
  - ✓$(P, \leqq)$ WQO
  - ✓$s_0 \in P$ the *initial state*
  - ✓$\Delta \subseteq P \times P$ transition



- **Def.** A transition system $((P, \leqq), s_0, \Delta)$ is *monotonic* if $s_1 \to s_2 \wedge s_1 \leqq t_1$ imply $\exists t_2.\ t_1 \to t_2 \wedge s_2 \leqq t_2$

- **Def.** $pre(s) = \{t \mid t \to s\}$, $post(s) = \{t \mid s \to t\}$
  $pre^*(s) = \{t \mid t \to^* s\}$, $post^*(s) = \{t \mid s \to^* t\}$
  $pre^*(I) = \{t \mid t \to^* s \in I\}$, $post^*(I) = \{t \mid s \to^* t,\ s \in I\}$

Coverability of monotonic WSTS by ideals

- **Def.** Let $(A, \leqq)$ be a QO. $I \subseteq A$ is
  - ✓*upward-closed* (*ideal*), if $x \in I \wedge x \leqq y \Rightarrow y \in I$.
  - ✓*downward-closed,* if $x \in I \wedge y \leqq x \Rightarrow y \in I$.

  denoted $I^{\uparrow} = I$ and $I^{\downarrow} = I$, respectively.

- **Assumption**: For a WSTS (P, s_0, Δ), *min*(*pre*(*I*)) can be effectively computed for each ideal *I*.
  - ✓The set of minimal elements of an ideal is finite.

- **Th**. *Coverability (reachability to ideal I) is decidable.*

  Proof. Reduced to whether $s_0 \in pre^*(I)$. Since $\subseteq$ is a WFO on ideals, $pre^*(I) = \cup_i pre^i(I)$ converges.

Difficulties of extensions to PDS

- WSTS techniques cannot be applied directly to PDS.
  - ✓Tempting to apply word embedding on stack contents, which destroys monotonicity.
  - ✓$w \leqq w'$ as element-wise comparison (i.e., $|w|=|w'|$), which will be neither WQO nor WFO.

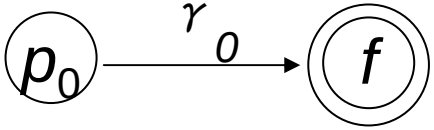
- **Our idea**. Combine classical P-automata techniques to acceleration / WSTS.
  - ✓*Completeness.* P-automata techniques for PDS with infinite states/stack alphabet (ignoring termination).
  - ✓*Termination analysis*. e.g., RVASS, Multi-set PDS

Remark

- Most of multi-thread models has non-standard pop rules (i.e., $\langle p, \gamma_1 \gamma_s \rangle \rightarrow \langle q, \gamma \rangle$)
  - ✓If stack alphabet is finite, possible to reduce standard pop rules.
  - ✓With infinite stack alphabet, such conversion introduces infinite states.

- Revisit P-automata construction for infinite states / stack alphabet with *non-standard pop* rules.
  - ✓We ignore termination (but observe convergence).

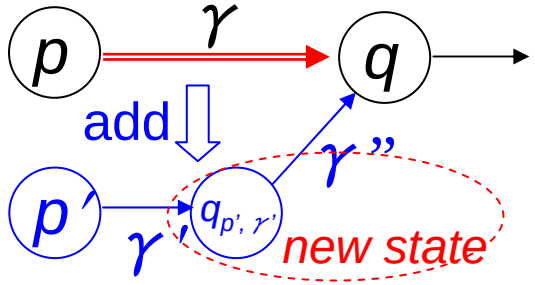
Step 1. P-Automaton (*post**)

- *Post** automaton accepts reachable configurations.
  - ✓Starting an initial automata, e.g., 

  - ✓Apply saturation rules until convergence.

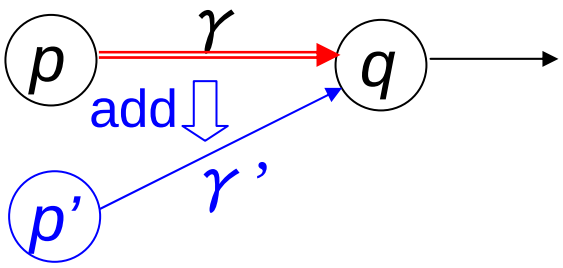
push

$(p, \gamma) \rightarrow (p', \gamma' \gamma'') \in \Delta$



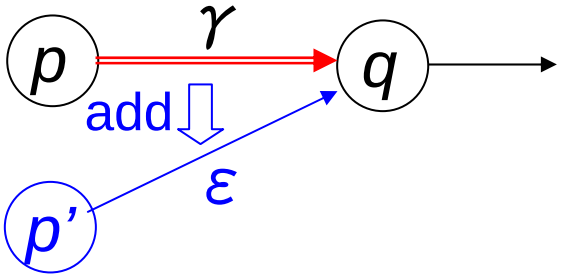
internal

$(p, \gamma) \rightarrow (p', \gamma') \in \Delta$



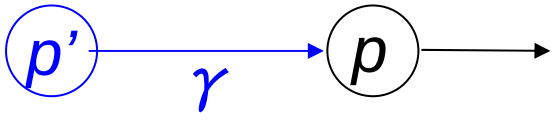
pop

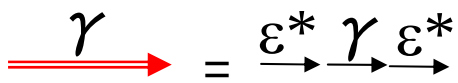
$(p, \gamma) \rightarrow (p', \varepsilon) \in \Delta$



simple-push

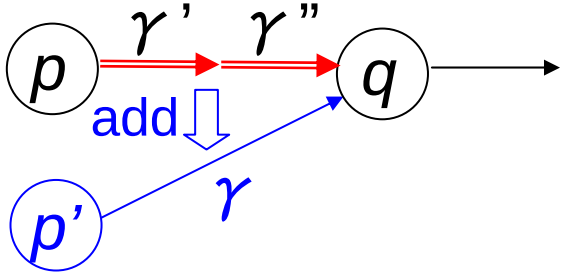
$(p, \varepsilon) \rightarrow (p', \gamma) \in \Delta$





non-standard pop

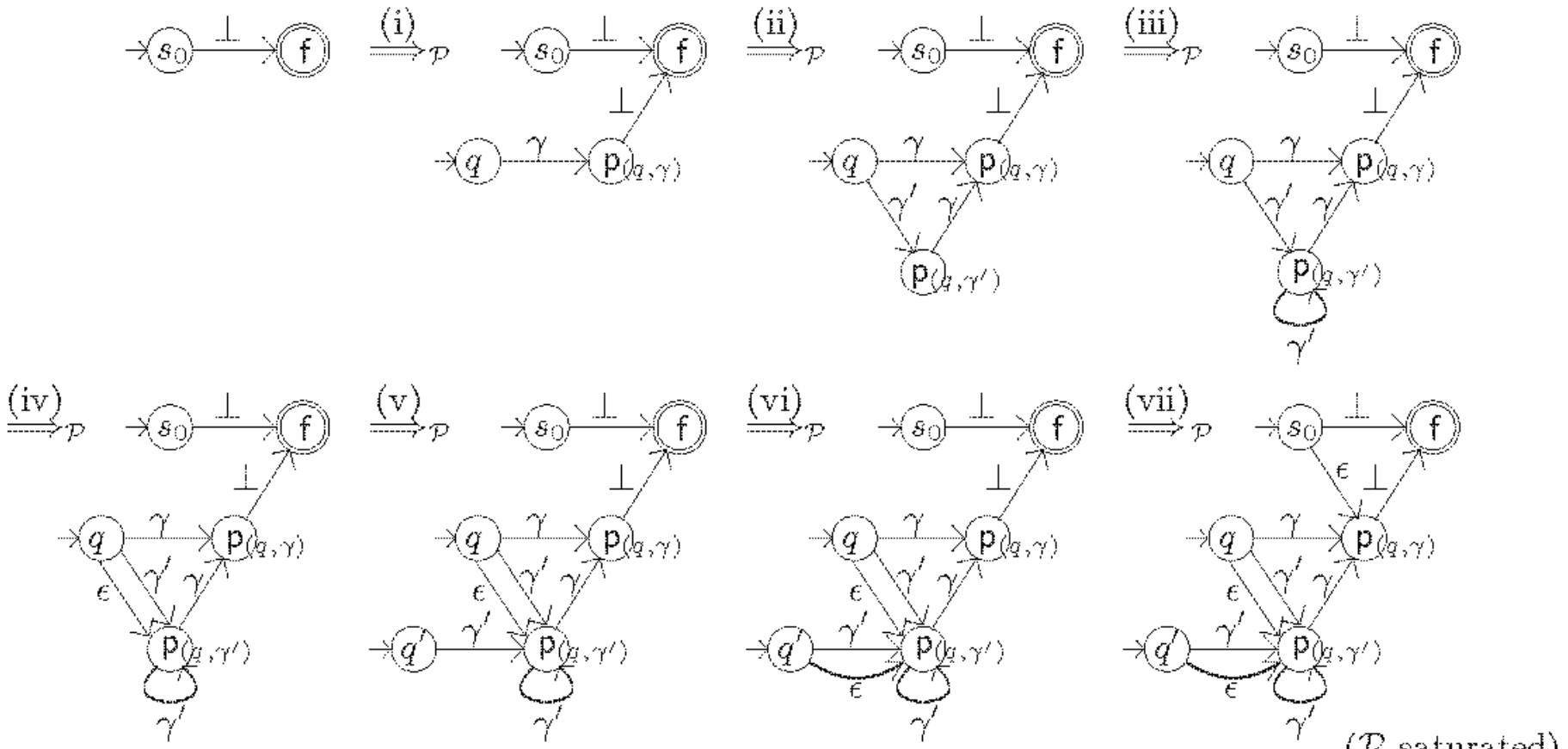
$(p, \gamma' \gamma'') \rightarrow (p', \gamma) \in \Delta$



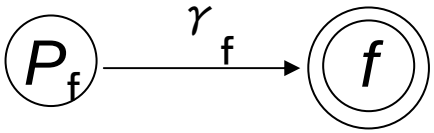
P-automaton example (post*)

Let a PDS $\mathcal{P} = (\{s_0, q, q'\}, \Delta, \{\gamma, \gamma'\}, \{s_0\})$ be with

$$\Delta = \left\{ \begin{array}{ll} \text{(i)}. \ (s_0, \bot) \longrightarrow (q, \gamma\bot) & \text{(v)}. \ (q, \gamma') \longrightarrow (q', \gamma') \\ \text{(ii)}. \ (q, \gamma) \longrightarrow (q, \gamma'\gamma) & \text{(vi)}. \ (q', \gamma') \longrightarrow (q', \epsilon) \\ \text{(iii)}. \ (q, \gamma') \longrightarrow (q, \gamma'\gamma') & \text{(vii)}. \ (q, \gamma) \longrightarrow (s_0, \epsilon) \\ \text{(iv)}. \ (q, \gamma') \longrightarrow (q, \epsilon) & \text{(viii)}. \ (q', \gamma) \longrightarrow (s_0, \epsilon) \end{array} \right\}$$



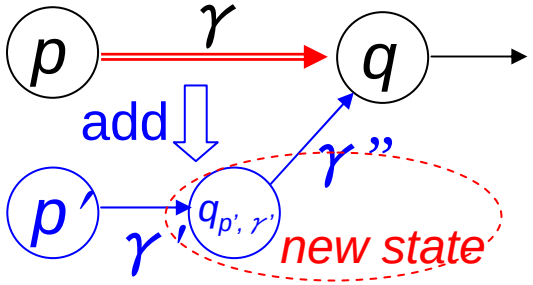
Step 1'. P-Automaton (*pre**)

- *Pre** automaton accepts predecessor configurations.
  - ✓Starting an initial automata, e.g., 

  - ✓Apply saturation rules until convergence.

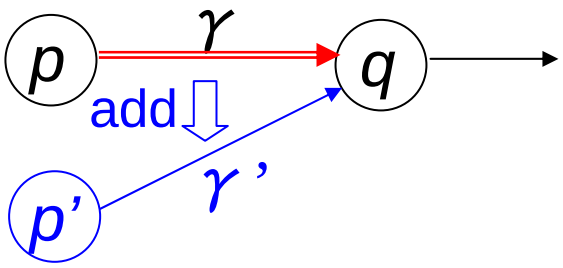
non-standard pop

$(p', \gamma' \gamma'') \rightarrow (p, \gamma) \in \Delta$



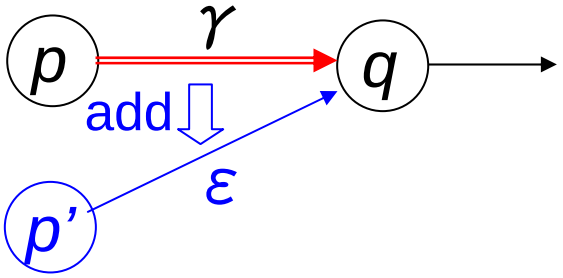
internal

$(p', \gamma') \rightarrow (p, \gamma) \in \Delta$



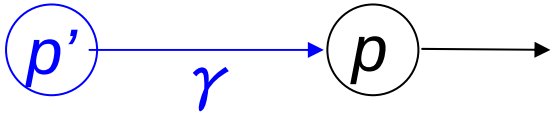
simple-push

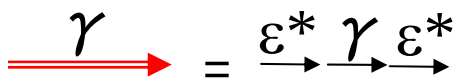
$(p', \varepsilon) \rightarrow (p, \gamma) \in \Delta$



pop

$(p', \gamma) \rightarrow (p, \varepsilon) \in \Delta$

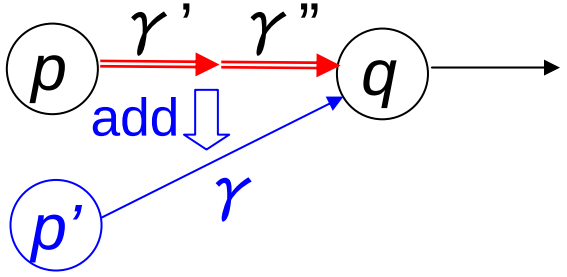




*Pre** is obtained by reversing transitions

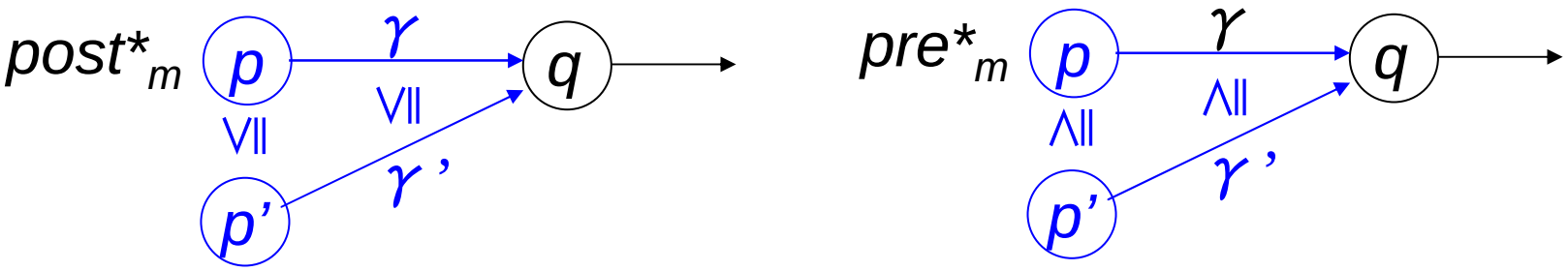
push

$(p', \gamma) \rightarrow (p, \gamma' \gamma'') \in \Delta$



Step 2. Coverability and P-automata minimization

- Minimization rules for coverability of *monotonic* PDS.

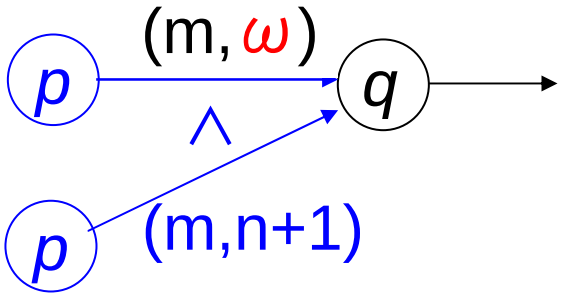


- **Th**. Coverability from (p,w) to (q,v) $\in P \times \Gamma^*$
  $\Leftrightarrow (q.v) \in post^*_m(\{(p,w)\})^{\downarrow}$, $(p.w) \in pre^*_m(\{(q,v)\}^{\uparrow})$

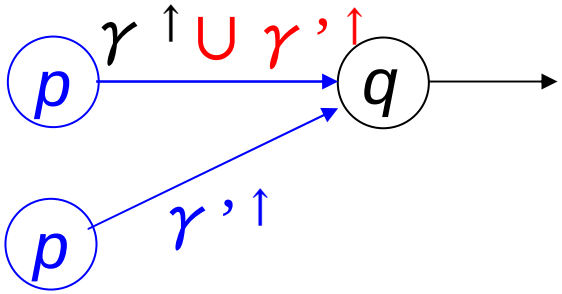
- At this level, we still do not require termination.
  - ✓*Post** : take *downward closure* of reachables.
  - ✓*Pre** : take *upward closure* of targets.

Step 3. Analysis on terminating cases

- Termination techniques for monotonic PDS
  - ✓*Post**: Acceleration (for $\mathbb{N}^k$)



  - ✓*Pre** : Ideal representation to compact



WQO over D implies
WFO ⊃ over { $X^{\uparrow}$ | $X \subseteq D$ }

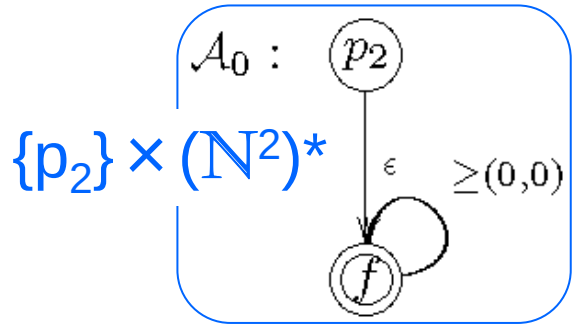
- Examples. finite states & WQO stack alphabet, Multi-set PDS, RVASS (finite states & N^k stack alphabet).

Ex1. PDS with finite states, WQO-stack alphabet

- PDS $(P, (\Gamma, \leqq), \Delta)$ has
  - ✓finite states, WQO stack alphabet
  - ✓without *non-standard pop* rules.

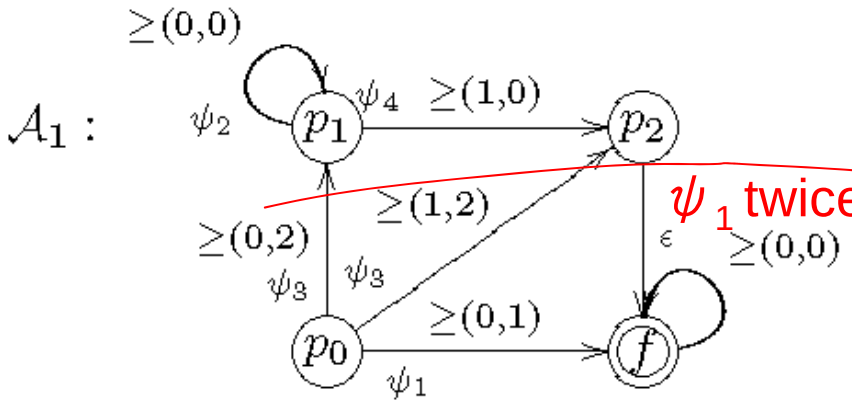
*Pre** is applied

- **Example**. $(\{p_0,p_1,p_2\}, \mathbb{N}^2, \Delta)$, reaching to $\langle p_0, \geqq(0,0)^* \rangle$

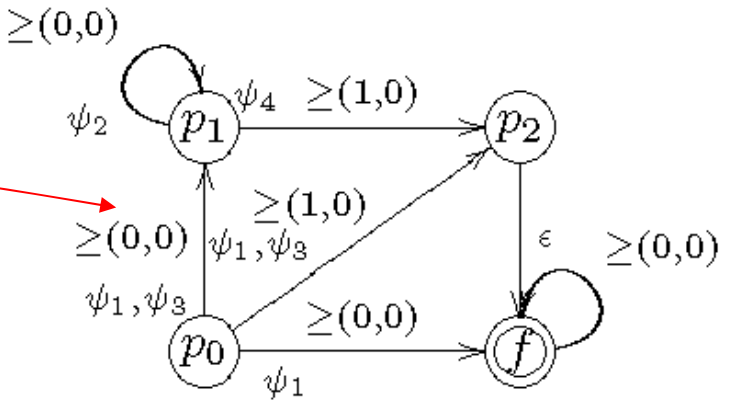


$\{p_2\} \times (\mathbb{N}^2)^*$

$$
\begin{array}{ll}
\psi_1 : \langle p_0, v \rangle \to \langle p_0, (v + (1,1))v \rangle & \\
\psi_2 : \langle p_1, v \rangle \to \langle p_1, \epsilon \rangle & \\
\psi_3 : \langle p_0, v \rangle \to \langle p_1, v - (0,2) \rangle & \text{if } v \geq (0,2) \\
\psi_4 : \langle p_1, v \rangle \to \langle p_2, \epsilon \rangle & \text{if } v \geq (1,0)
\end{array}
$$



ψ_1 twice



Def. PDS with WQO-stack alphabet

- **Def**. PDS with WQO-stack alphabet $(P, (\Gamma, \leqq), \Delta)$ is
  - ✓P : a finite set (of control states)
  - ✓$(\Gamma, \leqq)$: WQO (stack alphabet)
  - ✓ $\Delta \subseteq P \times P \times \mathit{Pfun}(\Gamma, \Gamma^{\leqq 2})$: a finite set of transitions, denoted $\langle p, \gamma \rangle \rightarrow \langle q, \psi(\gamma) \rangle$

  where *Pfun*(A,B) is the set of partial functions (A to B).

- **Assumptions**. We assume
  - ✓ψ is monotonic.
  - ✓For each ideal I in $\Gamma^{\leqq 2}$, $\min(\psi^{-1}(I))$ is computable.

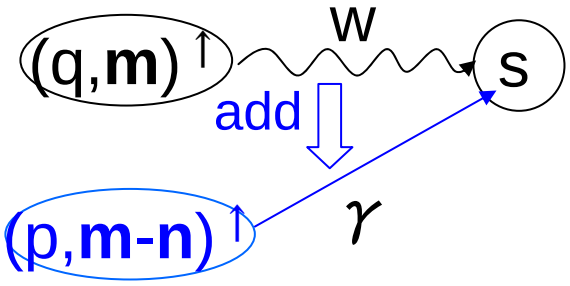
Ex 2. MPDS (WQO states, finite stack alphabet)

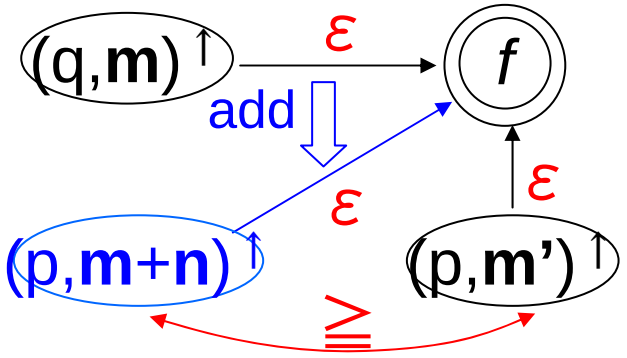
- Multi-set PDS $((P, \leqq), \Gamma, \Delta)$ has
  - ✓WQO states = finite control states × vectors ($\mathbb{N}^k$)
  - ✓finite stack alphabet
  - ✓without *non-standard pop* rules.

*Pre** is applied

$$\frac{(p, \gamma, q, w, \boldsymbol{n}) \in \delta_1}{\langle (p, \boldsymbol{m}), \gamma w' \rangle \hookrightarrow \langle (q, \boldsymbol{n} + \boldsymbol{m}), w w' \rangle} \qquad \frac{(p, q, \boldsymbol{n}) \in \delta_2, \boldsymbol{m} - \boldsymbol{n} \in \mathbb{N}^k}{\langle (p, \boldsymbol{m}), \epsilon \rangle \hookrightarrow \langle (q, \boldsymbol{m} - \boldsymbol{n}), \epsilon \rangle}$$

- Saturation and minimization rules in *pre**



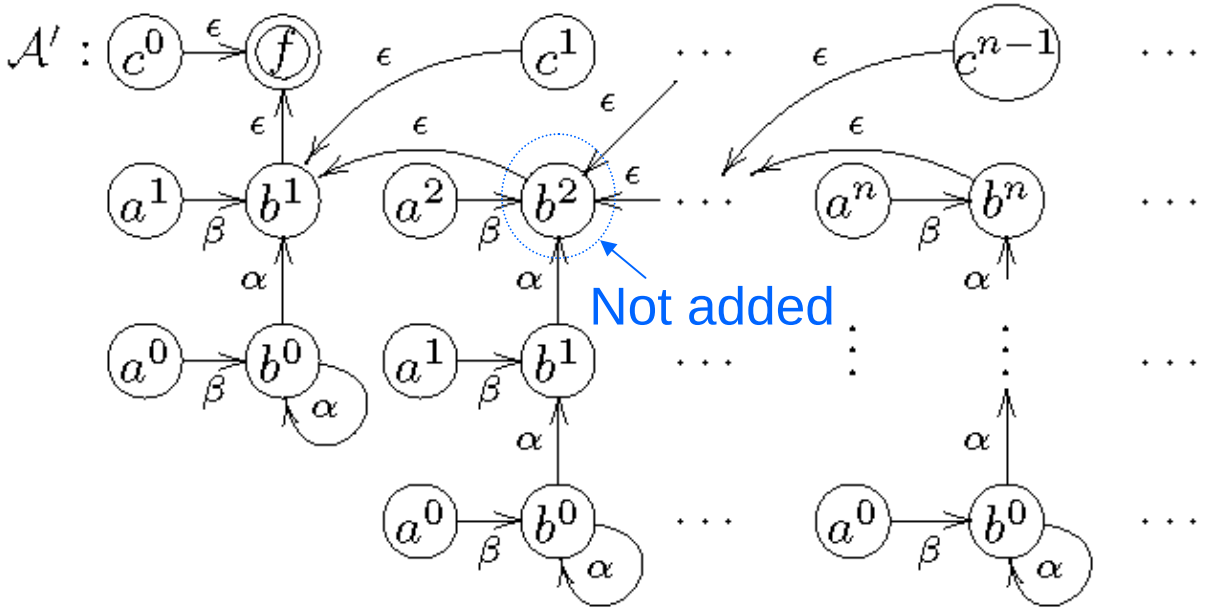


Only with the empty stack

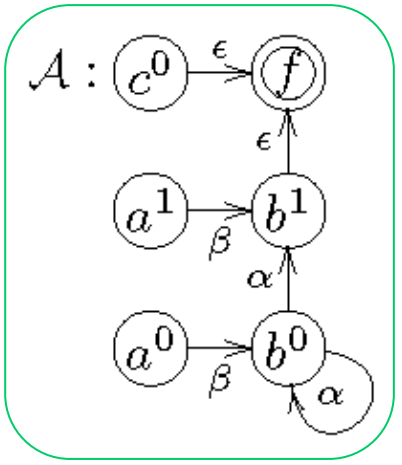
Multi-set PDS example (pre*)

- P = {a,b,c} $\times \mathbb{N}$, $\Gamma = \{\alpha, \beta\}$

$$\delta_1 = \{\psi_1 : (b^n, \alpha \to a^{n+1}, \beta), \psi_2 : (a^n, \beta \to b^n, \epsilon), \psi_3 : (c^n, \epsilon \to a^n, \beta)\}.$$
$$\delta_2 = \{\psi_0 : (b^n, \epsilon \to c^{n-1}, \epsilon)\}.$$



With state compaction



- $< \alpha^0, \varepsilon >$ will not cover $<c^0, \varepsilon >$

$$\langle a^0, \beta\alpha\alpha\rangle \overset{(\psi_2)}{\hookrightarrow} \langle b^0, \alpha\alpha\rangle \overset{(\psi_1)}{\hookrightarrow} \langle a^1, \beta\alpha\rangle \overset{(\psi_2)}{\hookrightarrow} \langle b^1, \alpha\rangle \overset{(\psi_1)}{\hookrightarrow} \langle a^2, \beta\rangle \overset{(\psi_2)}{\hookrightarrow} \langle b^2, \epsilon\rangle \overset{(\psi_0)}{\hookrightarrow} \langle c^1, \epsilon\rangle$$

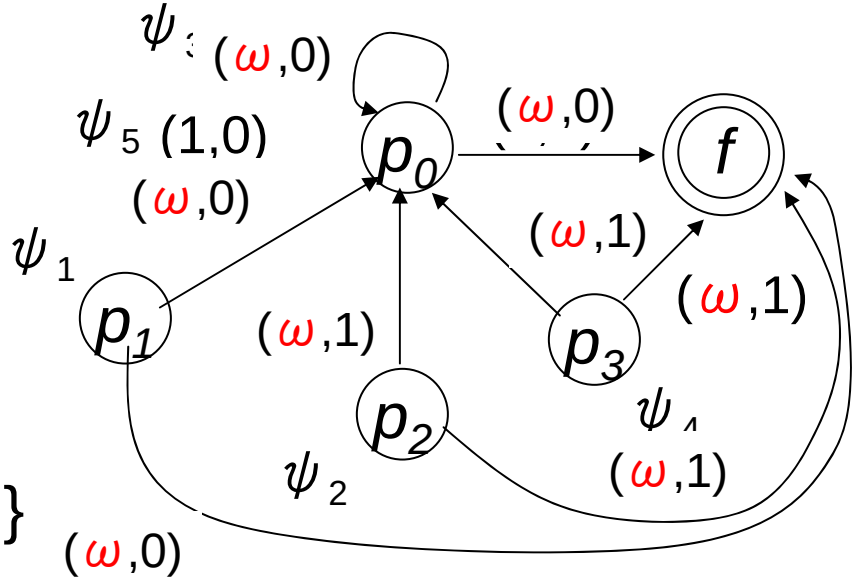
Ex 3. RVASS (finite states, WQO stack alphabet)

- RVASS (P, $(\mathbb{N}^k, \leqq)$, Δ) has
  - ✓finite states, stack alphabet = finite states × $\mathbb{N}^k$
  - ✓with *simple-push* and *non-standard* pop rules.

*Post** is applied

$$\frac{q \xrightarrow{z} q' \;\; \boldsymbol{n}+\boldsymbol{z} \in \mathbb{N}^k}{\langle q, \boldsymbol{n}\rangle c \hookrightarrow \langle q', \boldsymbol{n}+\boldsymbol{z}\rangle c} \qquad \frac{q \xrightarrow{q_1 q_2} q'}{\langle q, \boldsymbol{n}\rangle c \hookrightarrow \langle q_1, \boldsymbol{0}\rangle \langle q, \boldsymbol{n}\rangle c} \qquad \frac{q \xrightarrow{q_1 q_2} q'}{\langle q_2, \boldsymbol{n}'\rangle \langle q, \boldsymbol{n}\rangle c \hookrightarrow \langle q', \boldsymbol{n}+\boldsymbol{n}'\rangle c}$$

$$\begin{array}{l}
\psi_1 : \langle p_0, \epsilon\rangle \to \langle p_1, (0,0)\rangle \\
\psi_2 : \langle p_1, \boldsymbol{n}\rangle \to \langle p_2, \boldsymbol{n}+(1,1)\rangle \\
\psi_3 : \langle p_2, \boldsymbol{n}\rangle \to \langle p_0, \boldsymbol{n}-(0,1)\rangle \\
\psi_4 : \langle p_2, \boldsymbol{n}_1\boldsymbol{n}_2\rangle \to \langle p_3, \boldsymbol{n}_1+\boldsymbol{n}_2\rangle \\
\psi_5 : \langle p_3, \boldsymbol{n}\rangle \to \langle p_1, \boldsymbol{n}-(1,1)\rangle
\end{array}$$



Initial configuration = { <p_0. (0,0)> }

$$\langle p_0,(0,0)\rangle \hookrightarrow \langle p_1,(\underline{0},0)(0,0)\rangle \hookrightarrow \langle p_2,(1,1)(0,0)\rangle \hookrightarrow \langle p_0,(1,0)(0,0)\rangle$$
$$\hookrightarrow \langle p_1,(0,0)(0,0)(0,0)\rangle \hookrightarrow \langle p_2,(1,1)(0,0)(0,0)\rangle \hookrightarrow \langle p_3,(2,1)(0,0)\rangle \hookrightarrow \langle p_1,(\underline{1},0)(0,0)\rangle \hookrightarrow \cdots$$

Conclusion

- We showed
  - ✓P-automata construction works even for PDS with infinite states/stack alphabet.
  - ✓Minimization rules for coverability
  - ✓Acceleration for *post**, Ideal compaction for *pre** (when finite states & WQO stack alphabet)
    - –State reachability of RVASS is extended to coverability, Multi-set PDS coverability

- **Future work**. More examples to establish a general proof framework for coverability.
  - ✓Dense Timed Pushdown Automata (DTPDA, LICS12) with certain extensions.