Preorder-constrained simulation for program refinement with effects

Koko Muroya (RIMS, Kyoto University), Takahiro Sanada (RIMS, Kyoto University), Natsuki Urabe (NII)

Goal: coinductive, non-syntactical technique for proving program refinement

Program refinement $t \sqsubseteq u$:
"observation of evaluating t is also observable in evaluating u"

coinductive:
"stepwise" reasoning
non-syntactical:
cf. applicative bisimilarity [Abramsky '90]

in the presence of **effects**
✓ mutable state, errors
✓ nondeterministic choice
✓ I/O
× probabilistic choice

Example: reduction semantics as NA

nondeterministic automaton

$$\mathscr{A}_\Omega = (\mathbf{T}_\Omega \cup \{\checkmark\},\ \{\tau\} \cup \overline{\Omega} \cup \mathbb{N},\ \rightarrow,\ \{\checkmark\})$$

for λ-calculus w/ algebraic effects Ω :

- terms $\mathbf{T}_\Omega$ as states
  - ✓ as a final state
- algebraic operations $\overline{\Omega}$ & ground results $\mathbb{N}$ as labels
  where $\overline{\Omega} = \{f_i \mid f \in \Omega, 0 \le i \le \mathrm{arity}(f) - 1\}$
- reduction as transition

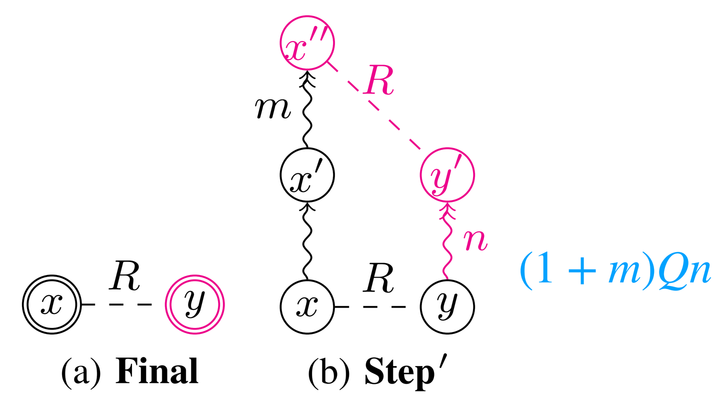
$$\frac{}{E[(\lambda x.t)\,v] \xrightarrow{\tau} E[t[v/x]]} \qquad \frac{f \in \Omega}{E[f(t_0, \ldots, t_{\mathrm{arity}(f)-1})] \xrightarrow{f_i} E[t_i]} \qquad \frac{}{\underline{n} \xrightarrow{n} \checkmark}$$

Program refinement as "trace inclusion"

- error $t \sqsubseteq^{Q}_{\{\mathtt{err}:0\}} u \iff$
  $t \overset{w}{\twoheadrightarrow} \checkmark \implies u \overset{w'}{\twoheadrightarrow} \checkmark \wedge |w|\,Q\,|w|$
- nondeterministic choice $t \sqsubseteq_{\{\mathtt{or}:2\}} u \iff$
  $t \overset{w}{\twoheadrightarrow} \checkmark \implies u \overset{w'}{\twoheadrightarrow} \checkmark \wedge w =_{\mathrm{remove}(\tau,\mathtt{or}_0,\mathtt{or}_1)} w'$
- I/O $t \sqsubseteq_{\{\mathtt{in}:2,\mathtt{out}_0:1,\mathtt{out}_1:1\}} u \iff$
  $t \overset{w}{\twoheadrightarrow} \checkmark \implies u \overset{w'}{\twoheadrightarrow} \checkmark \wedge w =_{\mathrm{remove}(\tau)} w'$

Starting point: counting simulation [M. '20]

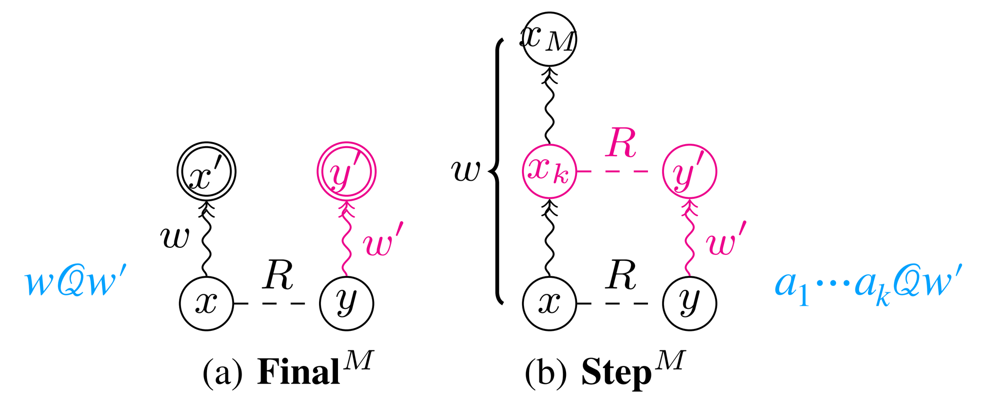
Def. Let Q be a preorder on $\mathbb{N}$.



Prop. For $\mathscr{A}_{\{\mathtt{err}\}}$, $\exists R\colon Q\text{-sim. } tRu \implies t \sqsubseteq^{Q}_{\{\mathtt{err}\}} u.$

Proposal: Preorder-constrained simulation

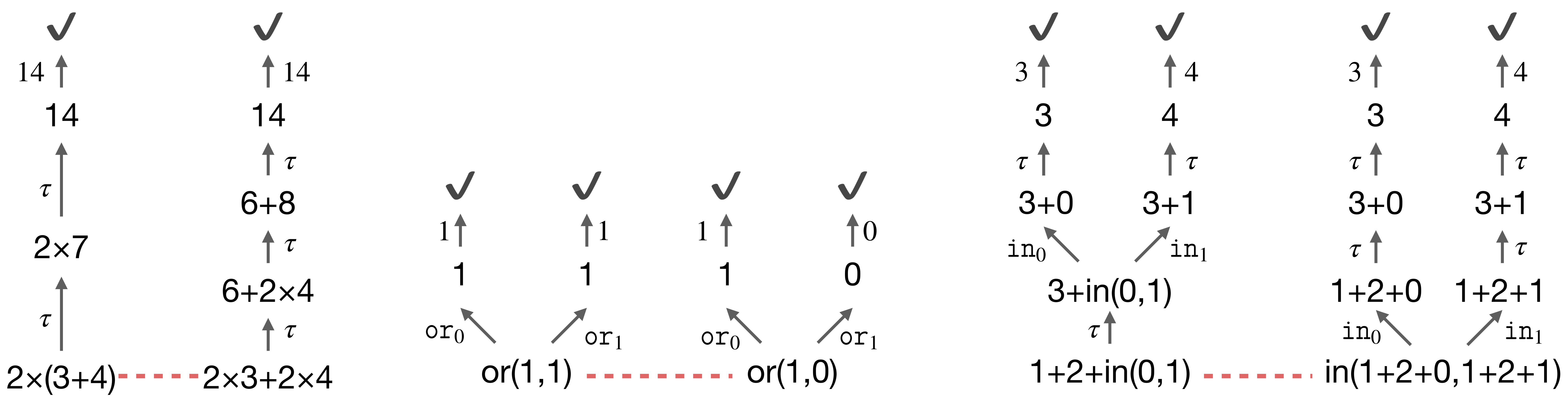
Def. Let $M \in \mathbb{N}$, and let $\mathcal{Q}$ be a preorder on Σ^*.



Thm.

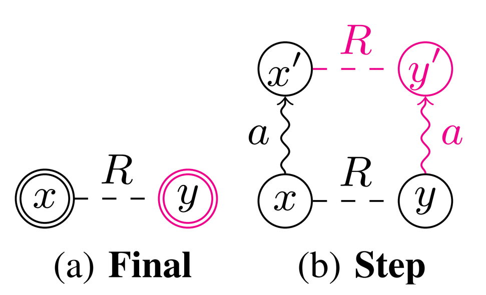
- For $\mathscr{A}_{\{\mathtt{err}\}}$, $\exists R\colon (M, \tilde{Q})\text{-sim. } tRu \implies t \sqsubseteq^{Q}_{\{\mathtt{err}\}} u$
- For $\mathscr{A}_{\{\mathtt{or}\}}$,
  $\exists R\colon (M, =_{\mathrm{remove}(\tau,\mathtt{or}_0,\mathtt{or}_1)})\text{-sim. } tRu \implies t \sqsubseteq_{\{\mathtt{or}\}} u$
- For $\mathscr{A}_{\{\mathtt{in},\mathtt{out}_0,\mathtt{out}_1\}}$,
  $\exists R\colon (M, =_{\mathrm{remove}(\tau)})\text{-sim. } tRu \implies t \sqsubseteq_{\{\mathtt{in},\mathtt{out}_0,\mathtt{out}_1\}} u$

Example pairs of NAs



Two challenges

1. Standard stepwise comparison is **not satisfactory**.



2. Observation **varies** between effects.

Advanced topics

- generalised notion of trace inclusion
- complete variant of preorder-constrained simulation
- two-player reachability game
- up-to technique in terms of preorders