On Proving Confluence of Concurrent Programs by All-Path Reachability of LCTRSs

Misaki Kojima Naoki Nishida

Nagoya University

IWC 2024, 9th July, 2024

Contents of This Talk

Background

Concurrent program → transformation → concurrent LCTRS → APR analysis → result

- LCTRSs model concurrent programs
  - All-path reachability (APR) analysis for runtime-error verification
- Most concurrent LCTRSs are
  - non-terminating
  - overlapping (with non-trivial CPs)
- Some LCTRSs are confluent w.r.t. an initial ground term
  - Despite not satisfy the well-known criteria for confluence
- Well-known criteria for confluence are
  - termination + joinability of CPs
  - (weak) orthogonality = left-linear + non-overlapping (triviality of CPs)

Purpose and Results

Purpose

Develop a method to prove confluence w.r.t. initial term s_0 of concurrent LCTRSs

$$\begin{tikzcd} & s_0 \arrow[dl, "*"'] \arrow[dr, "*"] & \\ t_1 \arrow[dr, dotted, "*"] & & t_2 \arrow[dl, dotted, "*"'] \\ & \cdot & \end{tikzcd}$$

Result

Show how to prove joinability of two reachable terms of s_0 by APR proofs

Approach

- A sufficient condition is that all reachable terms can be reduced back to s_0
- Solve APR problem $\{\text{reachable terms}\} \Rightarrow \{s_0\}$

Contents of This Talk

Logically Constrained Term Rewrite System (LCTRS)

[Kop and Nishida, 2013]

- Computation models for functional and imperative languages
- Represent asynchronous integer transitions systems

Example

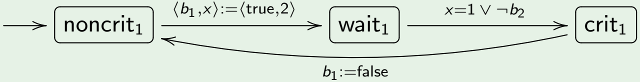
$$\mathcal{R}_2 = \left\{ \begin{array}{ll} \mathsf{fact}(x) \to \mathsf{subfact}(x, 1) & \\ \mathsf{subfact}(x, y) \to y & [\, x \leq 0 \,] \\ \mathsf{subfact}(x, y) \to \mathsf{subfact}(x - 1, x \times y) & [\, x > 0 \,] \end{array} \right\}$$

$$\begin{aligned} \mathsf{fact}(3) &\to_{\mathcal{R}_2} \mathsf{subfact}(3, 1) \\ &\to_{\mathcal{R}_2} \mathsf{subfact}(3 - 1, 3 \times 1) \to^2_{\mathcal{R}_2} \mathsf{subfact}(2, 3) \\ &\to_{\mathcal{R}_2} \mathsf{subfact}(2 - 1, 2 \times 3) \to^2_{\mathcal{R}_2} \mathsf{subfact}(1, 6) \\ &\to_{\mathcal{R}_2} \mathsf{subfact}(1 - 1, 1 \times 6) \to^2_{\mathcal{R}_2} \mathsf{subfact}(0, 6) \\ &\to_{\mathcal{R}_2} 6 \end{aligned}$$

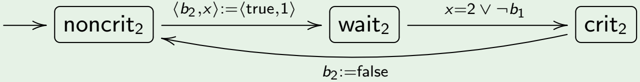
LCTRSs for Asynchronous ITSs [Kojima and Nishida, 2023]

Example (Peterson's mutual exclusion [Baier and Katoen, 2008])

Process 1:



Process 2:



- b_i indicates that Process i wants to enter the critical section
- x indicates that Process x has priority for the critical section
- Asynchronous ITS for Processes 1 & 2 is represented by

$$\left\{\begin{array}{llll}
\mathsf{cnfg}(\mathsf{noncrit}_1, p_2, b_1, b_2, x) & \to \mathsf{cnfg}(\mathsf{wait}_1, p_2, b_1', b_2, x') & [\, b_1' = \mathsf{true} \wedge x' = 2 \,] \\
\mathsf{cnfg}(\mathsf{wait}_1, p_2, b_1, b_2, x) & \to \mathsf{cnfg}(\mathsf{crit}_1, p_2, b_1, b_2, x) & [\, x = 1 \vee \neg b_2 \,] \\
\mathsf{cnfg}(\mathsf{crit}_1, p_2, b_1, b_2, x) & \to \mathsf{cnfg}(\mathsf{noncrit}_1, p_2, b_1', b_2, x) & [\, b_1' = \mathsf{false} \,] \\
\mathsf{cnfg}(p_1, \mathsf{noncrit}_2, b_1, b_2, x) & \to \mathsf{cnfg}(p_1, \mathsf{wait}_2, b_1, b_2', x') & [\, b_2' = \mathsf{true} \wedge x' = 1 \,] \\
\mathsf{cnfg}(p_1, \mathsf{wait}_2, b_1, b_2, x) & \to \mathsf{cnfg}(p_1, \mathsf{crit}_2, b_1, b_2, x) & [\, x = 2 \vee \neg b_1 \,] \\
\mathsf{cnfg}(p_1, \mathsf{crit}_2, b_1, b_2, x) & \to \mathsf{cnfg}(p_1, \mathsf{noncrit}_2, b_1, b_2', x) & [\, b_1' = \mathsf{false} \,]
\end{array}\right\}$$

All-Path Reachability Problems of LCTRSs

[Ciobâcă and Lucanu, 2018]

- Constrained term $\langle t \mid \phi \rangle$
  - t is a term and ϕ is a constraint
  - $\langle t \mid \phi \rangle$ represents the set of ground instance $t\theta$ such that θ satisfies ϕ

Example

Constrained term representing the initial state of the previous example

$$\langle \mathsf{cnfg}(\mathsf{noncrit}_1, \mathsf{noncrit}_2, \mathsf{false}, \mathsf{false}, x) \mid x = 1 \vee x = 2 \rangle$$

- APR Problem $\langle s \mid \phi \rangle \Rightarrow \langle t \mid \psi \rangle$
- Execution path = finite and ends with an irreducible state or infinite

Demonical validity of $\langle s \mid \phi \rangle \Rightarrow \langle t \mid \psi \rangle$

Every finite execution path from a state in $\langle s \mid \phi \rangle$ includes a state in $\langle t \mid \psi \rangle$

- Constant-directed APR Problem $\langle s \mid \phi \rangle \Rightarrow \langle c \mid \mathsf{true} \rangle$ where c is a constant nf
  - Abbreviate to $\langle s \mid \phi \rangle \Rightarrow c$
- Proof systems for constant-directed APR problems have been proposed

[Kojima and Nishida, 2023]

Contents of This Talk

How to Prove Confluence w.r.t. Initial Terms

- Prove that all reachable terms of s_0 can be reduced back to s_0

$$\begin{tikzcd} & s_0 \arrow[dl, "*"'] \arrow[dr, "*"] & \\ t_1 \arrow[ur, dotted, "*"'] & & t_2 \arrow[ul, dotted, "*"] \end{tikzcd}$$

- This may be reduced to APR problem $\{\text{reachable terms}\} \Rightarrow \{s_0\}$

Difficulties

- $\{$reachable terms$\}$ cannot be represented by a single constrained term
- Infinite reductions from t_1 and t_2 are not considered for APR-validity

Approach to difficulties

- Take $\langle s_0 \mid \mathsf{true} \rangle$ for $\{\text{reachable terms}\}$
  - s_0 itself is a reachable term
  - APR problem $\langle s_0 \mid \mathsf{true} \rangle \Rightarrow \langle s_0 \mid \mathsf{true} \rangle$ is meaningless
- Solve APR problem $\langle s_0 \mid \mathsf{true} \rangle \Rightarrow \mathsf{init}$ of $\mathcal{R} \cup \{s_0 \to \mathsf{init}\}$
  - init is a fresh constant
- Strong connectedness of APR proofs under certain conditions

c-DCC: Proof System for APR Problems

[Kojima and Nishida, 2023]

- c-DCC$(\mathcal{R}, \mathcal{G})$: Proof system based on $\mathcal{R}$ and the set of APR problems $\mathcal{G}$

axiom/c-subs

$$\frac{}{\langle s \mid \phi \rangle \Rightarrow c} \text{ if } \phi \text{ is unsatisfiable or } s = c$$

c-der

$$\frac{\langle s_1 \mid \phi_1 \rangle \Rightarrow c \quad \ldots \quad \langle s_n \mid \phi_n \rangle \Rightarrow c}{\langle s \mid \phi \rangle \Rightarrow c} \text{ if } \langle s \mid \phi \rangle \cap NF_{\mathcal{R}} = \emptyset$$

where $\langle s_i \mid \phi_i \rangle$ are constrained terms that are reachable in one step from $\langle s \mid \phi \rangle$

weak circ

$$\frac{}{\langle s \mid \phi \rangle \Rightarrow c} \text{ if } \exists (\langle s' \mid \phi' \rangle \Rightarrow c) \in \mathcal{G}.\ \langle s \mid \phi \rangle = \langle s' \mid \phi' \rangle$$

Example (Peterson's mutual exclusion [Baier and Katoen, 2008])

$$
\left\{
\begin{array}{llllll}
\mathsf{cnfg}(\mathsf{noncrit}_1, p_2, & b_1, b_2, x) & \to \mathsf{cnfg}(\mathsf{wait}_1, & p_2, & b_1', b_2, x') & [\, b_1' = \mathsf{true} \wedge x' = 2 \,] \\
\mathsf{cnfg}(\mathsf{wait}_1, p_2, & b_1, b_2, x) & \to \mathsf{cnfg}(\mathsf{crit}_1, & p_2, & b_1, b_2, x\ ) & [\, x = 1 \vee \neg b_2 \,] \\
\mathsf{cnfg}(\mathsf{crit}_1, p_2, & b_1, b_2, x) & \to \mathsf{cnfg}(\mathsf{noncrit}_1, & p_2, & b_1', b_2, x\ ) & [\, b_1' = \mathsf{false} \,] \\[1ex]
\mathsf{cnfg}(p_1, \mathsf{noncrit}_2, & b_1, b_2, x) & \to \mathsf{cnfg}(p_1, & \mathsf{wait}_2, & b_1, b_2', x') & [\, b_2' = \mathsf{true} \wedge x' = 1 \,] \\
\mathsf{cnfg}(p_1, \mathsf{wait}_2, & b_1, b_2, x) & \to \mathsf{cnfg}(p_1, & \mathsf{crit}_2, & b_1, b_2, x\ ) & [\, x = 2 \vee \neg b_1 \,] \\
\mathsf{cnfg}(p_1, \mathsf{crit}_2, & b_1, b_2, x) & \to \mathsf{cnfg}(p_1, & \mathsf{noncrit}_2, & b_1, b_2', x\ ) & [\, b_1' = \mathsf{false} \,] \\[1ex]
\multicolumn{6}{l}{\mathsf{cnfg}(\mathsf{noncrit}_1, \mathsf{noncrit}_2, \mathsf{false}, \mathsf{false}, x) \to \mathsf{init}}
\end{array}
\right\}
$$

$$
\dfrac{
\dfrac{
\dfrac{\dfrac{}{(2)} \quad \dfrac{}{(3)}}{(9)\ \mathsf{cnfg}(\mathsf{n}_1, \mathsf{n}_2, \mathsf{f}, \mathsf{f}, 2)}
\quad
\dfrac{\dfrac{}{(3)}}{(10)\ \mathsf{cnfg}(\mathsf{c}_1, \mathsf{w}_2, \mathsf{t}, \mathsf{t}, 1)}
}{(5)\ \mathsf{cnfg}(\mathsf{c}_1, \mathsf{n}_2, \mathsf{t}, \mathsf{f}, 2)}
\quad
\dfrac{\dfrac{}{(10)}}{(6)\ \mathsf{cnfg}(\mathsf{w}_1, \mathsf{w}_2, \mathsf{t}, \mathsf{t}, 1)}
}{(2)\ \mathsf{cnfg}(\mathsf{w}_1, \mathsf{n}_2, \mathsf{t}, \mathsf{f}, 2)}
\quad
\dfrac{
\dfrac{\dfrac{\dfrac{}{(2)}}{(11)\ \mathsf{cnfg}(\mathsf{w}_1, \mathsf{c}_2, \mathsf{t}, \mathsf{t}, 2)}}{(7)\ \mathsf{cnfg}(\mathsf{w}_1, \mathsf{w}_2, \mathsf{t}, \mathsf{t}, 2)}
\quad
\dfrac{\dfrac{}{(11)} \quad \dfrac{}{(1)}}{(8)\ \mathsf{cnfg}(\mathsf{n}_1, \mathsf{c}_2, \mathsf{f}, \mathsf{t}, 1)}
}{(3)\ \mathsf{cnfg}(\mathsf{n}_1, \mathsf{w}_2, \mathsf{f}, \mathsf{t}, 1)}
\quad
\dfrac{}{(4)\ \mathsf{init}}
}{(1)\ \mathsf{cnfg}(\mathsf{n}_1, \mathsf{n}_2, \mathsf{f}, \mathsf{f}, 1)}
$$

- Note that $\langle s \mid \mathsf{true} \rangle \Rightarrow \mathsf{init}$ abbreviated to s in the above tree
- APR problem $\langle s_0 \mid \mathsf{true} \rangle \Rightarrow \mathsf{init}$ of $\mathcal{R} \cup \{ s_0 \to \mathsf{init} \}$ is solved
- All terms are reduced to (1)?
  - Yes, and thus confluent
  - (4) don't have to be considered

- Does validity of APR problem imply joinability of all reachable terms?
  - No

Necessity of Strong Connectedness

Example

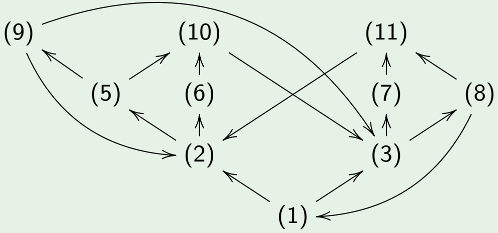
$$\mathcal{R} = \left\{ \begin{array}{l} \mathsf{a} \to \mathsf{b} \\ \mathsf{a} \to \mathsf{c} \\ \mathsf{b} \to \mathsf{b} \\ \mathsf{c} \to \mathsf{c} \\ \mathsf{a} \to \mathsf{init} \end{array} \right\} \qquad \dfrac{\dfrac{\overline{(2)}}{(2)\ \langle \mathsf{b} \mid \mathsf{true} \rangle \Rightarrow \mathsf{init}} \quad \dfrac{\overline{(3)}}{(3)\ \langle \mathsf{c} \mid \mathsf{true} \rangle \Rightarrow \mathsf{init}} \quad \dfrac{}{(4)\ \langle \mathsf{init} \mid \mathsf{true} \rangle \Rightarrow \mathsf{init}}}{(1)\ \langle \mathsf{a} \mid \mathsf{true} \rangle \Rightarrow \mathsf{init}}$$

- $\langle \mathsf{a} \mid \mathsf{true} \rangle \Rightarrow \mathsf{init}$ is valid but $\mathcal{R}$ is not confluent

- Any infinite path not reaching initial term is not considered for APR-validity
- To consider them, we need strong connectedness
  - Ignore (4) $\langle \mathsf{init} \mid \mathsf{true} \rangle \Rightarrow \mathsf{init}$

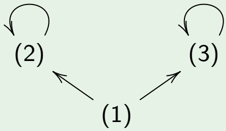
Example

$$
\left\{
\begin{array}{llll}
\mathsf{cnfg}(\mathsf{noncrit}_1, p_2, b_1, b_2, x) & \rightarrow \mathsf{cnfg}(\mathsf{wait}_1, & p_2, b_1', b_2, x') & [\, b_1' = \mathsf{true} \wedge x' = 2 \,] \\
\mathsf{cnfg}(\mathsf{wait}_1, \quad p_2, b_1, b_2, x) & \rightarrow \mathsf{cnfg}(\mathsf{crit}_1, & p_2, b_1, b_2, x\ ) & [\, x = 1 \vee \neg b_2 \,] \\
\mathsf{cnfg}(\mathsf{crit}_1, \quad p_2, b_1, b_2, x) & \rightarrow \mathsf{cnfg}(\mathsf{noncrit}_1, & p_2, b_1', b_2, x\ ) & [\, b_1' = \mathsf{false} \,] \\
\quad \vdots & & &
\end{array}
\right\}
$$



Example

$$
\mathcal{R} = \left\{
\begin{array}{l}
\mathsf{a} \rightarrow \mathsf{b} \\
\mathsf{a} \rightarrow \mathsf{c} \\
\mathsf{b} \rightarrow \mathsf{b} \\
\mathsf{c} \rightarrow \mathsf{c} \\
\mathsf{a} \rightarrow \mathsf{init}
\end{array}
\right\}
$$

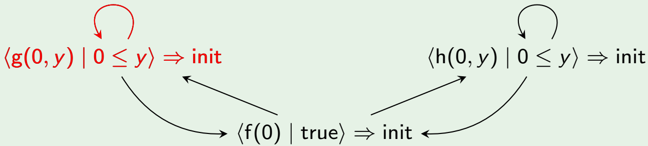


Strong Connectedness is NOT Sufficient

- Strong connectedness does not imply joinability of all reachable terms

Example

$$\mathcal{R}_2 = \left\{ \begin{array}{lll} \mathsf{f}(x) \to \mathsf{g}(x,y) \ [\, y \geq x \,] & & \mathsf{f}(x) \to \mathsf{h}(x,y) \ [\, y \geq x \,] \\ \mathsf{g}(x,y) \to \mathsf{f}(x) \ [\, y \leq x \,] & & \mathsf{g}(x,y) \to \mathsf{g}(x,y') \ [\, y > x \wedge y' = y+1 \,] \\ \mathsf{h}(x,y) \to \mathsf{f}(x) \ [\, y \leq x \,] & & \mathsf{h}(x,y) \to \mathsf{h}(x,y') \ [\, y > x \wedge y' = y+1 \,] \end{array} \right\}$$



- The proof tree is strongly connected
- But $\mathcal{R}_2$ is not confluent w.r.t. $\mathsf{f}(0)$
- There exists a cyclic path such that
  1. $\langle \mathsf{g}(x,y) \mid x \leq y \rangle \Rightarrow \mathsf{init}$ contains two or more terms, and
  2. s_0 is not contained

Our Confluence Criterion

- All reachable terms can be reduced to s_0 if
  1. all constrained terms are singleton sets, or
  2. there is no cycle not including s_0

Theorem (main result)

Let G be a proof tree for APR problem $\langle s_0 \mid \mathsf{true} \rangle \Rightarrow \mathsf{init}$ of $\mathcal{R} \cup \{s_0 \to \mathsf{init}\}$. Suppose that G is strongly connected and one of the following holds:

1. *for every node of G, $\langle s \mid \phi \rangle$ of the attached $\langle s \mid \phi \rangle \Rightarrow \mathsf{init}$ is singleton, or*
2. *$G \setminus \{\text{root node}\}$ is acyclic.*

Then, $\mathcal{R}$ is confluent w.r.t. s_0.

Remarks

- We have not adapted our APR prover Crisys2cdcc to our confluence criterion
- The example (Peterson's mutual exclusion) in this talk is linear and all its CPs are strongly closed and thus strongly confluent [Schöpf and Middeldorp, 2023]
  - crest[1] [Schöpf and Middeldorp, 2024] succeeds in proving its confluence
  - crest failed to prove confluence of the LCTRS obtained from it by adding some redundant rules ($\ell \to \ell$)

[1] `http://cl-informatik.uibk.ac.at/software/crest/`

Contents of This Talk

1. Background
2. All-path Reachability Problems of LCTRSs
3. Confluence w.r.t. Initial Terms
4. Conclusion

Conclusion

Summary

Show how to prove joinability of two reachable terms of s_0 by APR proofs

Future Work

- Implementation
- Relax our sufficient condition
  - Each CP can be reduced to its critical peak

$$
\begin{tikzcd}
 & t_0 \arrow[dl] \arrow[dr] & & \\
t_1 \arrow[ur, dotted, bend left, "*"] & & t_2 \arrow[ul, dotted, bend right, "*"'] \arrow[dl] \arrow[dr] & \\
 & t_3 \arrow[ur, dotted, bend left, "*"] & & t_4 \arrow[ul, dotted, bend right, "*"']
\end{tikzcd}
$$

References

Baier, C. and Katoen, J. (2008).
Principles of model checking.
MIT Press.

Ciobâcă, Ș. and Lucanu, D. (2018).
A coinductive approach to proving reachability properties in logically constrained term rewriting systems.
In Galmiche, D., Schulz, S., and Sebastiani, R., editors, *Proceedings of the 9th International Joint Conference on Automated Reasoning*, volume 10900 of *Lecture Notes in Computer Science*, pages 295–311. Springer.

Kojima, M. and Nishida, N. (2023).
Reducing non-occurrence of specified runtime errors to all-path reachability problems of constrained rewriting.
Journal of Logical and Algebraic Methods in Programming, 135:1–19.

Kop, C. and Nishida, N. (2013).
Term rewriting with logical constraints.
In Fontaine, P., Ringeissen, C., and Schmidt, R. A., editors, *Proceedings of the 9th International Symposium on Frontiers of Combining Systems*, volume 8152 of *Lecture Notes in Artificial Intelligence*, pages 343–358.

References (cont.)

Schöpf, J. and Middeldorp, A. (2023).
Confluence criteria for logically constrained rewrite systems.
In Pientka, B. and Tinelli, C., editors, *Proceedings of the 29th International Conference on Automated Deduction*, volume 14132 of *Lecture Notes in Computer Science*, pages 474–490. Springer.

Schöpf, J. and Middeldorp, A. (2024).
crest 0.8.
In Chenavier, C. and Nishida, N., editors, *Proceedings of the 13th International Workshop on Confluence*, pages 66–66.