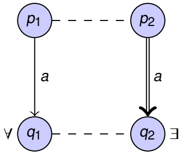
Model-checking bisimulation-based information flow properties for infinite-state systems

Raghavendra K. R.
Joint work with Deepak D'Souza
Dept. of CSA, IISc.

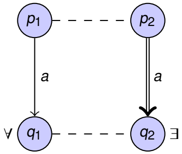
System model

- Set of events (Σ) partitioned into Low L and High H, Input I and Output O
- Every event has its complement
- Trace: a sequence of events
- System: Labeled Transition Systems (LTS) $M = (Q, \Sigma, \rightarrow, s)$
- Low user observes only the low events
- Information flow properties restrict the flow of information about high events to the low user

Weak bisimulation

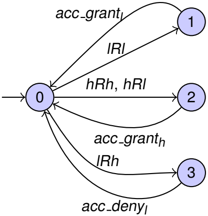


Weak bisimulation



- Bisimulation game
- M_1 and M_2 are weakly bisimilar if there exists a weak bisimulation containing (s_1, s_2)

No Read Up Policy

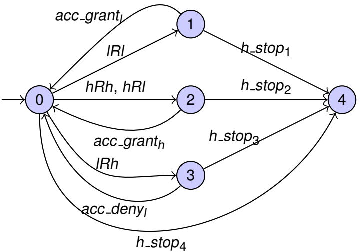


Trace-based Strong Non-deterministic Non-interference (SNNI)

M satisfies SNNI iff $L(M \setminus \mathrm{H}) = L(M/\mathrm{H})$.

Satisfies SNNI and secure.

No Read Up Policy

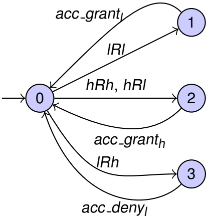


Trace-based Strong Non-deterministic Non-interference (SNNI)

M satisfies SNNI iff $L(M \setminus \mathrm{H}) = L(M/\mathrm{H})$.

Satisfies SNNI Not secure.

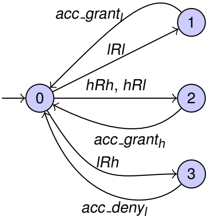
No Read Up Policy



Bisimulation-based SNNI (BSNNI)

M satisfies BSNNI iff $M \setminus \mathrm{H} \approx_B M/\mathrm{H}$.

No Read Up Policy

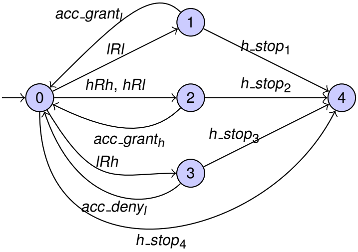


Bisimulation-based SNNI (BSNNI)

M satisfies BSNNI iff $M \setminus \mathrm{H} \approx_B M/\mathrm{H}$.

Satisfies BSNNI. Also secure

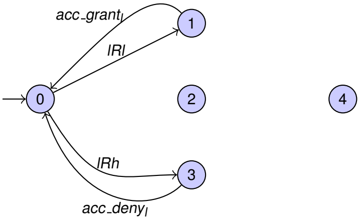
No Read Up Policy

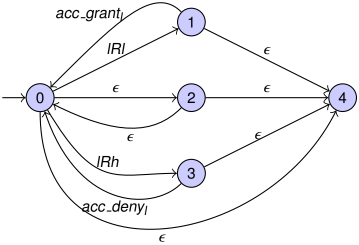


Bisimulation-based SNNI (BSNNI)

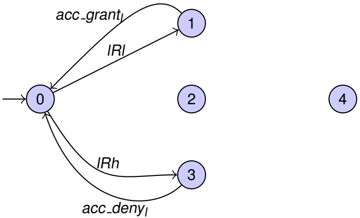
M satisfies BSNNI iff $M \setminus \mathrm{H} \approx_B M/\mathrm{H}$.

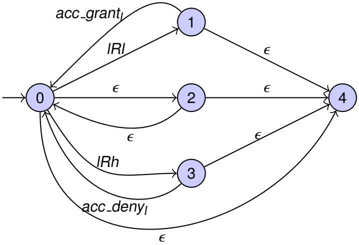
No Read Up - Bisimulation





No Read Up - Bisimulation





Does not satisfy BSNNI

Bisimulation-based properties - Focardi & Gorrieri '94

1. Bisimulation-based Non-deterministic Non-interference (BNNI) - $M/\mathrm{H} \approx (M \setminus (\mathrm{I} \cap \mathrm{H}))/\mathrm{H}$
2. Bisimulation-based Strong Non-deterministic Non-interference (BSNNI) - $M \setminus \mathrm{H} \approx M/\mathrm{H}$
3. Let M' be any system with only high events. Bisimulation-based Non-Deducibility on Compositions (BNDC) - $M/\mathrm{H} \approx (M|M') \setminus \mathrm{H}$
4. Strong BNNI (SBNNI) For all reachable states q, M_q satisfies BNNI
5. Strong BSNNI (SBSNNI) For all reachable states q, M_q satisfies BSNNI
6. Strong BNDC (SBNDC) For all $q \xrightarrow{h} r$ in M, $M_q \setminus \mathrm{H} \approx M_r \setminus \mathrm{H}$

Bisimulation-based properties - Focardi & Gorrieri '94

1. Bisimulation-based Non-deterministic Non-interference (BNNI) - $M/\mathrm{H} \approx (M \setminus (\mathrm{I} \cap \mathrm{H}))/\mathrm{H}$
2. Bisimulation-based Strong Non-deterministic Non-interference (BSNNI) - $M \setminus \mathrm{H} \approx M/\mathrm{H}$
3. Let M' be any system with only high events. Bisimulation-based Non-Deducibility on Compositions (BNDC) - $M/\mathrm{H} \approx (M|M') \setminus \mathrm{H}$
4. Strong BNNI (SBNNI) For all reachable states q, M_q satisfies BNNI
5. Strong BSNNI (SBSNNI) For all reachable states q, M_q satisfies BSNNI
6. Strong BNDC (SBNDC) For all $q \xrightarrow{h} r$ in M, $M_q \setminus \mathrm{H} \approx M_r \setminus \mathrm{H}$

Shown decidability for finite-state systems.

Pushdown systems

Example

$p \xrightarrow{(} p \text{ push } A;$

$p \xrightarrow{)} p \text{ pop } A;$

Pushdown systems

Example

$p \xrightarrow{(} p$ push A;

$p \xrightarrow{)} p$ pop A;

- Induces a possibly infinite transition system
- Bisimilarity on the induced transitions systems

Checking weak bisimilarity for PDS

- Srba '02: undecidable - reducing the halting problem of 2 counter machines.
- Given a 2 counter machine R, construct P_R and two states $p_1\alpha$ and $p_2\beta$ such that R halts iff $p_1\alpha \not\approx p_2\beta$.
- Doesn't imply undecidability for bisimulation-based properties directly.

Checking weak bisimilarity for PDS

- Srba '02: undecidable - reducing the halting problem of 2 counter machines.
- Given a 2 counter machine R, construct P_R and two states $p_1\alpha$ and $p_2\beta$ such that R halts iff $p_1\alpha \not\approx p_2\beta$.
- Doesn't imply undecidability for bisimulation-based properties directly.

Observations

- $p_1\alpha$ has no ϵ-transitions
- if there is a winning strategy for the attacker from $(p_1\alpha, p_2\beta)$ then there is one starting with $p_1\alpha$

Checking weak bisimilarity for PDS

- Srba '02: undecidable - reducing the halting problem of 2 counter machines.
- Given a 2 counter machine R, construct P_R and two states $p_1\alpha$ and $p_2\beta$ such that R halts iff $p_1\alpha \not\approx p_2\beta$.
- Doesn't imply undecidability for bisimulation-based properties directly.

Observations

- $p_1\alpha$ has no ϵ-transitions
- if there is a winning strategy for the attacker from $(p_1\alpha, p_2\beta)$ then there is one starting with $p_1\alpha$

Corollary

The restricted PDS bisimulation problem is undecidable

Checking BSNNI for PDS

- Reducing the restricted PDS bisimulation problem
- Construct P' from P such that $p_1\alpha \approx p_2\beta$ in M_P iff $M_{P'}$ satisfies BSNNI.

Checking BSNNI for PDS

- Reducing the restricted PDS bisimulation problem
- Construct P' from P such that $p_1\alpha \approx p_2\beta$ in M_P iff $M_{P'}$ satisfies BSNNI.
- $\Sigma' = \Sigma \cup \{k, \bar{k}\}$, $\mathrm{H} = \mathrm{I} = \{k, \bar{k}\}$

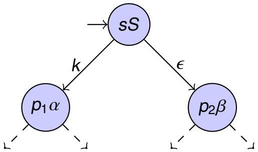


Figure: $M_{P'}$

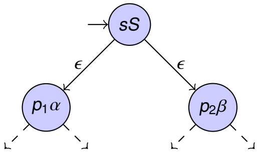


Figure: $M_{P'}/\mathrm{H}$

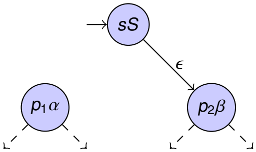


Figure: $M_{P'} \setminus \mathrm{H}$

Checking properties for PDS

- Checking BSNNI is undecidable
- BNNI is same as BSNNI for $M_{P'}$, Checking BNNI is also undecidable

Checking properties for PDS

- Checking BSNNI is undecidable
- BNNI is same as BSNNI for $M_{P'}$, Checking BNNI is also undecidable
- LTS M with only k, $\bar{k}$ events

Checking properties for PDS

- Checking BSNNI is undecidable
- BNNI is same as BSNNI for $M_{P'}$, Checking BNNI is also undecidable
- LTS M with only k, $\bar{k}$ events
- Consider $(M_{P'}|M) \setminus$ H

Checking properties for PDS

- Checking BSNNI is undecidable
- BNNI is same as BSNNI for $M_{P'}$, Checking BNNI is also undecidable
- LTS M with only k, $\bar{k}$ events
- Consider $(M_{P'}|M) \setminus$ H
- $(q\gamma, m) \equiv (q'\gamma', m')$ iff $q\gamma = q'\gamma'$

Checking properties for PDS

- Checking BSNNI is undecidable
- BNNI is same as BSNNI for $M_{P'}$, Checking BNNI is also undecidable
- LTS M with only k, $\bar{k}$ events
- Consider $(M_{P'}|M) \setminus \mathrm{H}$
- $(q\gamma, m) \equiv (q'\gamma', m')$ iff $q\gamma = q'\gamma'$
- Let $N = (M_{P'}|M) \setminus \mathrm{H}/\equiv$

Checking properties for PDS

- Checking BSNNI is undecidable
- BNNI is same as BSNNI for $M_{P'}$, Checking BNNI is also undecidable
- LTS M with only k, $\bar{k}$ events
- Consider $(M_{P'}|M) \setminus \mathrm{H}$
- $(q\gamma, m) \equiv (q'\gamma', m')$ iff $q\gamma = q'\gamma'$
- Let $N = (M_{P'}|M) \setminus \mathrm{H}/\equiv$
- $N \approx (M_{P'}|M) \setminus \mathrm{H}$

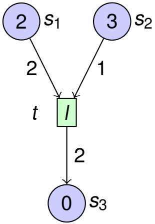
Checking properties for PDS

- Checking BSNNI is undecidable
- BNNI is same as BSNNI for $M_{P'}$, Checking BNNI is also undecidable
- LTS M with only k, $\bar{k}$ events
- Consider $(M_{P'}|M) \setminus \mathrm{H}$
- $(q\gamma, m) \equiv (q'\gamma', m')$ iff $q\gamma = q'\gamma'$
- Let $N = (M_{P'}|M) \setminus \mathrm{H}/\equiv$
- $N \approx (M_{P'}|M) \setminus \mathrm{H}$
- $p_1\alpha \approx p_2\beta$ in M_P iff $M_{P'}/\mathrm{H} \approx N$.
- Checking BNDC is undecidable

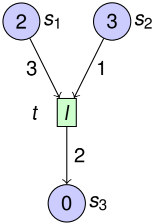
Theorem

Checking each of the properties for PDS is undecidable.

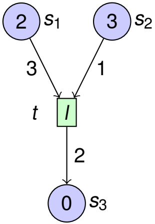
Petri nets



Petri nets



Petri nets



Induces a possibly infinite transition system on markings

Checking weak bisimilarity for Petri nets

- Jancar '94: undecidable - reduction from halting problem of 2 counter machines to the strong bisimilarity problem.
- Weak bisimilarity problem is also undecidable.
- Given a 2 counter machine R, construct N_1 and N_2 with initial markings M_1 and M_2 respectively such that R halts iff $M_1 \not\approx M_2$.
- Doesn't imply undecidability for bisimulation-based properties directly.

Checking weak bisimilarity for Petri nets

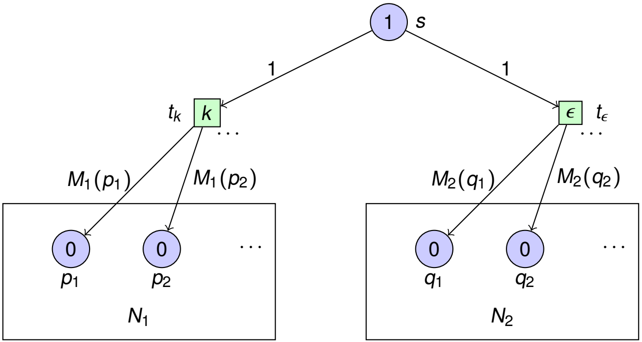
- Jancar '94: undecidable - reduction from halting problem of 2 counter machines to the strong bisimilarity problem.
- Weak bisimilarity problem is also undecidable.
- Given a 2 counter machine R, construct N_1 and N_2 with initial markings M_1 and M_2 respectively such that R halts iff $M_1 \not\approx M_2$.
- Doesn't imply undecidability for bisimulation-based properties directly.

Similar Observations

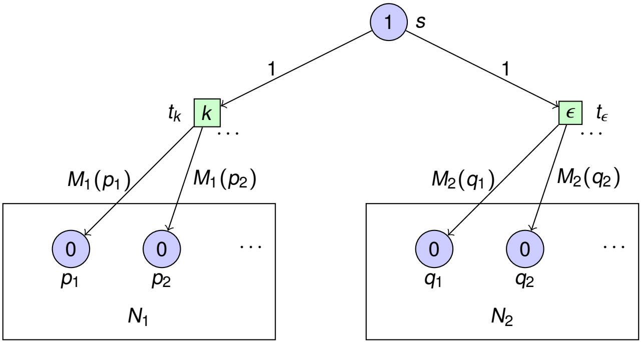
Corollary

The restricted PN bisimulation problem is undecidable

Checking BSNNI for Petri nets



Checking BSNNI for Petri nets



Theorem

Checking each of the properties for Petri nets is undecidable

Summary

Model checking each of the bisimulation-based information flow properties for

- pushdown systems
- Petri nets
- process algebras

is undecidable.

Research lines

- Semantic characterization of different properties.
- Deterministic PDS - weak bisimilarity is decidable
- Totally normed BPA, totally normed BPP