Petri Nets: Modelling, Properties and Analysis

Jiri Srba

Department of Computer Science
Aalborg University, Denmark

Lecture 3

State Space Reduction Techniques

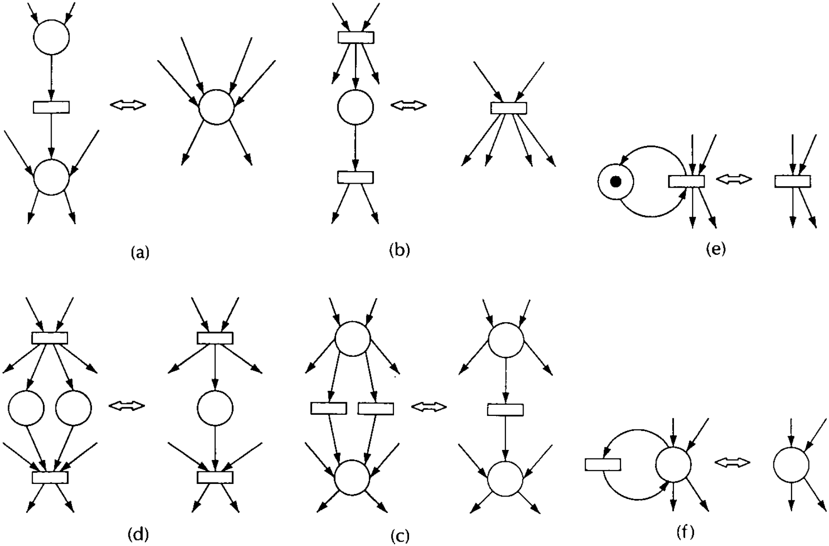
Even for bounded nets, the size of the state space is the main obstacle for verification (using e.g. coverability tree/graph).

Idea

Reduce syntactically the size of the reachable state space while preserving the answer to given verification question.

- Symmetry reduction techniques.
- Partial order reductions (reduce interleaving of parallel events):
  - stubborn sets
  - ample sets
  - persistent sets
- Structural net reductions.

Structural Net Reduction Rules



Properties of Structural Reductions

Let (N, M_0) be a marked Petri net and let (N', M_0) be a marked Petri net after using the reductions rules arbitrarily many times but making sure that no places that contain tokens in the initial marking M_0 are removed.

Theorem

The net (N, M_0) is bounded if and only if (N', M_0) is bounded.

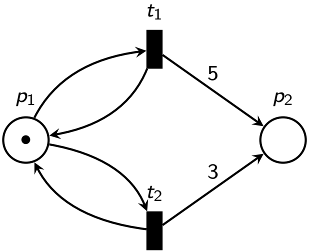
Theorem

The net (N, M_0) is safe (1-bounded) if and only if (N', M_0) is safe.

Theorem

The net (N, M_0) is live if and only if (N', M_0) is live.

State Equations of Petri Nets—Motivation



- Can the marking $(1, 7)$ be reached?
- Can the marking $(1, 11)$ be reached?

General Construction of State Equations

Let $N = (P, T, F, W)$ be a Petri net with an initial marking M_0 and a final marking M. W.l.o.g. assume that $T = \{t_1, t_2, \ldots, t_n\}$. We construct a system of linear inequalities over the variables $x_1, x_2, \ldots, x_n$:

- for each $p \in P$, add the equality

$$M(p) = M_0(p) + \sum_{i=1}^{n} x_i \cdot (W((t_i, p)) - W((p, t_i)))$$

- for each i, $1 \leq i \leq n$, add the inequality

$$x_i \geq 0$$

General Construction of State Equations

Let $N = (P, T, F, W)$ be a Petri net with an initial marking M_0 and a final marking M. W.l.o.g. assume that $T = \{t_1, t_2, \ldots, t_n\}$. We construct a system of linear inequalities over the variables $x_1, x_2, \ldots, x_n$:

- for each $p \in P$, add the equality

$$M(p) = M_0(p) + \sum_{i=1}^{n} x_i \cdot (W((t_i, p)) - W((p, t_i)))$$

- for each i, $1 \leq i \leq n$, add the inequality

$$x_i \geq 0$$

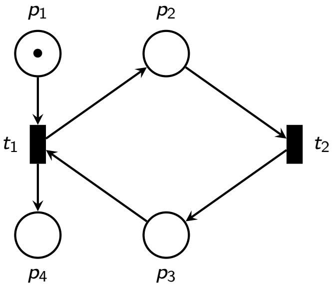
Theorem

If the marking M is reachable from M_0 then the system of inequalities has an integer solution.

Fact: checking whether the integer linear program above has a solution is an NP-complete problem.

General Construction of State Equations

Note that even if the linear program has an integer solution, we cannot guarantee that the marking M is reachable from M_0.



Clearly, the marking $(0, 0, 0, 1)$ cannot be reached but the state equations have an integer solution.

Undecidability of Bisimulation

Theorem

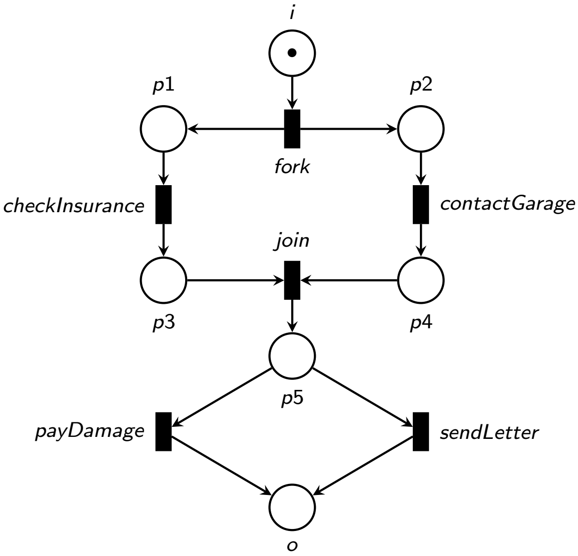
Given two marked nets, the problem whether their initial markings are strongly bisimilar is undecidable.

Proof: by reduction from two counter Minsky machine.

Workflow Nets

- Workflow nets by Wil van der Aalst [ICATPN'97] are widely used for modelling of business workflow processes.
- Based on the Petri nets formalism.
- Abstraction from data, focus on execution flow.
- Early detection of design errors like deadlocks, livelocks and other abnormal behaviour.
- Classical soundness for workflow nets:
  - option to complete,
  - proper termination, and
  - absence of redundant tasks.

Workflow of Processing a Car Damage Claim



Workflow Net Definition

Definition [Workflow Net]

A Petri net $N = (P, T, F, W)$ is a workflow net if

- there is a unique input place $i \in P$ with no incoming arcs and a unique output place $o \in P$ with no outgoing arcs, and
- every place and every transition in N is on a directed path from i to o.

Let M_i be a marking with exactly one token in the place i.
Let M_o be a marking with exactly one token in the place o.

Workflow Net Definition

Definition [Workflow Net]

A Petri net $N = (P, T, F, W)$ is a workflow net if

- there is a unique input place $i \in P$ with no incoming arcs and a unique output place $o \in P$ with no outgoing arcs, and
- every place and every transition in N is on a directed path from i to o.

Let M_i be a marking with exactly one token in the place i.
Let M_o be a marking with exactly one token in the place o.

Definition [Soundness]

A workflow net N is sound if

1. whenever $M_i \longrightarrow^* M$ for some M then $M \longrightarrow^* M_o$,
2. if $M_i \longrightarrow^* M$ and $M(o) \geq 1$ then $M = M_o$, and
3. for every $t \in T$ there is $M_i \longrightarrow^* M$ such that M enables t.

Decidability of Soundness

1. Construct the coverability graph starting from M_i.
2. If the graph contains ω then the net is not sound. (Why?)
3. Otherwise, check whether
   (i) from every node in the graph you can reach M_o,
   (ii) check that there is no marking M such that $M(o) \geq 1$ and at the same time M has more than one token, and
   (iii) check that every transition appears in the reachability graph.

Decidability of Soundness

1. Construct the coverability graph starting from M_i.
2. If the graph contains ω then the net is not sound. (Why?)
3. Otherwise, check whether
   (i) from every node in the graph you can reach M_o,
   (ii) check that there is no marking M such that $M(o) \geq 1$ and at the same time M has more than one token, and
   (iii) check that every transition appears in the reachability graph.

However, the complexity of this decision algorithm is not optimal!

A Necessary and Sufficient Condition for Soundness

Let N be a workflow net and let $\overline{N}$ be the net N extended with a fresh transition t^* and two new arcs $(o, t^*) \in F$ and $(t^*, i) \in F$.

Theorem

A workflow net N is sound if and only if $(\overline{N}, M_i)$ is live and bounded.

A Necessary and Sufficient Condition for Soundness

Let N be a workflow net and let $\overline{N}$ be the net N extended with a fresh transition t^* and two new arcs $(o, t^*) \in F$ and $(t^*, i) \in F$.

Theorem

A workflow net N is sound if and only if $(\overline{N}, M_i)$ is live and bounded.

Theorem

The structural reduction rules applied to workflow nets preserve soundness.

Note that rule (e) is never applicable in workflow nets and that rule (f) is correct for soundness due to the assumption that any place in a workflow net is on some path from i to o.