Symbolic Unfoldings of High-level Petri Nets

Lukas Panneke

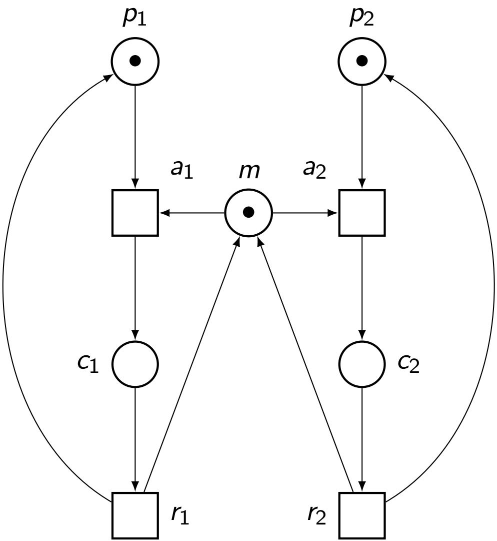
German Aerospace Center (DLR)

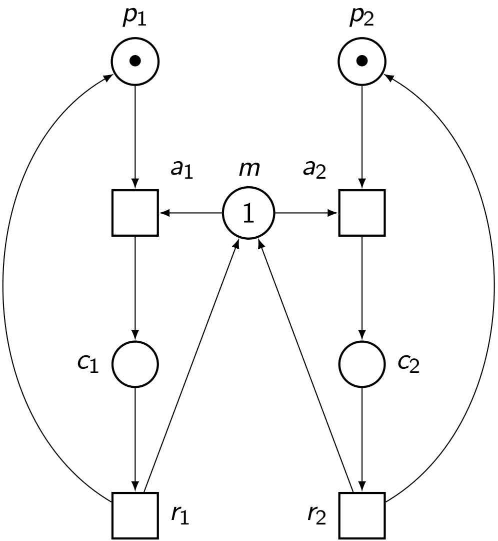
D-CON 2024, February 29

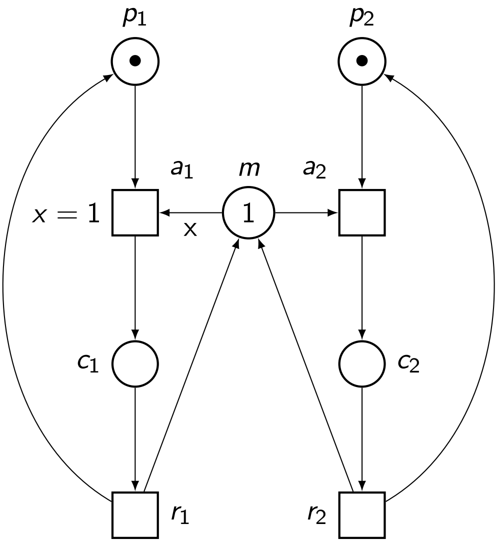
lukas.panneke@dlr.de
github.com/Selebrator

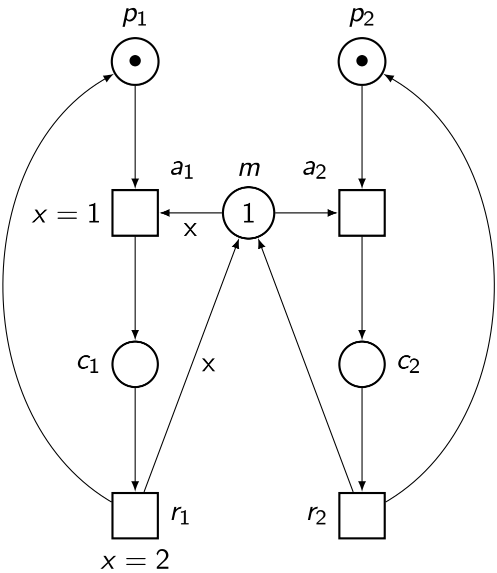
A Motivating Use-Case — Reachability Analysis

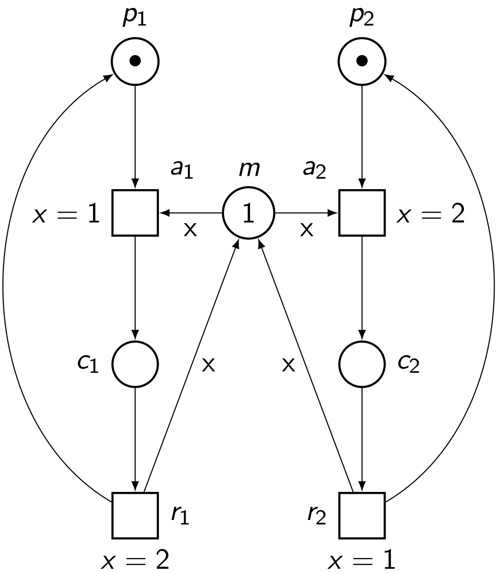
- Petri nets
  - a graphical and mathematical modeling formalism
  - good for modeling concurrent, distributed, and nondeterministic systems
- The reachability problem
  - given a net and a desired state, ask is there is a sequence of transitions from the initial to the desired state – if the state is reachable
  - is known to be computationally hard (non-primitive recursive)
  - **There are high-level Petri nets where no existing tool can decide reachability queries**
- Unfoldings
  - Make any Petri net acyclic while preserving behavior
  - Easier to analyse than Petri nets; smaller than state space

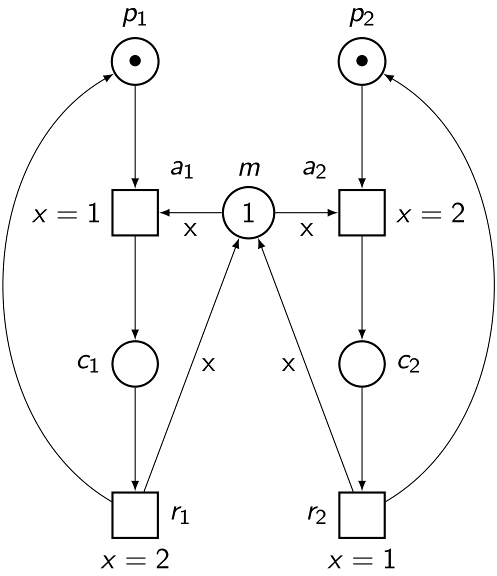

p_1
p_2
a_1
m
a_2
c_1
c_2
r_1
r_2

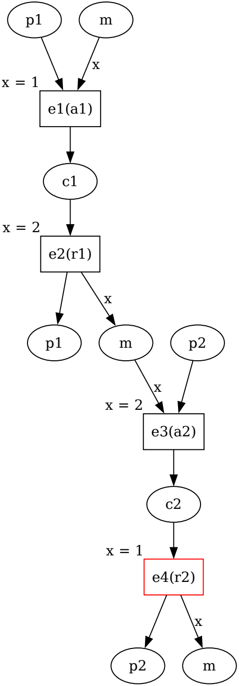

p_1
p_2
a_1
m
a_2
1
c_1
c_2
r_1
r_2


p_1
p_2
a_1
m
a_2
$x = 1$
1
x
c_1
c_2
r_1
r_2


p_1
p_2
a_1
m
a_2
$x = 1$
1
x
c_1
x
c_2
r_1
r_2
$x = 2$


p_1
p_2
a_1
m
a_2
$x = 1$
1
$x = 2$
x
x
c_1
x
x
c_2
r_1
r_2
$x = 2$
$x = 1$


p_1
p_2
a_1
m
a_2
$x = 1$
1
$x = 2$
x
x
c_1
x
x
c_2
r_1
r_2
$x = 2$
$x = 1$


p1
m
x
x = 1
e1(a1)
c1
x = 2
e2(r1)
x
p1
m
p2
x
x = 2
e3(a2)
c2
x = 1
e4(r2)
x
p2
m

Symbolic Unfoldings for Deciding Reachability

- Encode marking reachability as transition firability
  - Goal marking reachable iff goal transition in unfolding (not dead)
- Use symbolic bounded model checking
  - Completeness of prefix grantees that bound is sufficiently high

High-level Petri Net Unfoldings — Your Options

$$\begin{tikzcd}
N \arrow[r, "\text{expand}", "\mathbf{(0,2)}"'] \arrow[d, "\begin{array}{c}\text{unfold}\\ \text{[WCH23]}\\ \mathbf{(1,2,3\cancel{b}a)}\end{array}"'] \arrow[dr, "\text{unfold with jit-expand [KK03]}", "\mathbf{(2,3a)}"'] & Exp(N) \arrow[d, "\begin{array}{c}\text{unfold}\\ \text{[ERV02]}\\ \mathbf{(3a)}\end{array}"] \\
\begin{array}{c}\text{FCP of}\\ Sym\text{-}Unf(N)\\ \text{[CJ04]}\end{array} & \begin{array}{c}\text{FCP of}\\ LL\text{-}Unf(N)\\ \text{[NPW81]}\end{array}
\end{tikzcd}$$

- **(0)** Finite color class
- **(1)** 1-bounded net
- **(2)** Decidable logic
- **(3a)** Finitely many reachable markings
- **(3b)** Every reachable marking is reachable in a bounded number of steps

Contribution: Mode Determinism

Definition (Mode Determinism)

A high-level Petri net is *mode deterministic* iff every transition is enabled in at most 1 firing mode in *every reachable marking*.

Sufficient a priori condition: every transitions output variables are deterministically determined by its input variables.

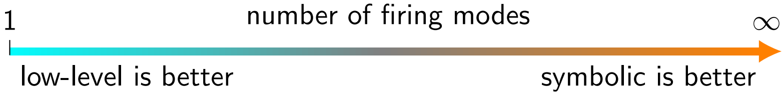


Figure: Heuristic for predicting which approach is better.

Benchmark

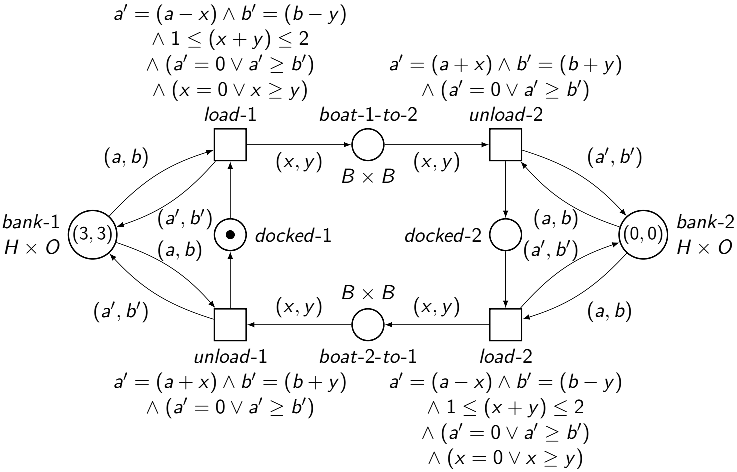
Symbolic approach
Calculate FCP or reachability deciding prefix
of symbolic unfolding of net

vs.

Low-level approach
Calculate FCP or reachability deciding prefix
of low-level unfolding of expansion of net
using jit-expand

Faster is better since symbolic is smaller

Benchmark: Hobbits & Orcs — Net

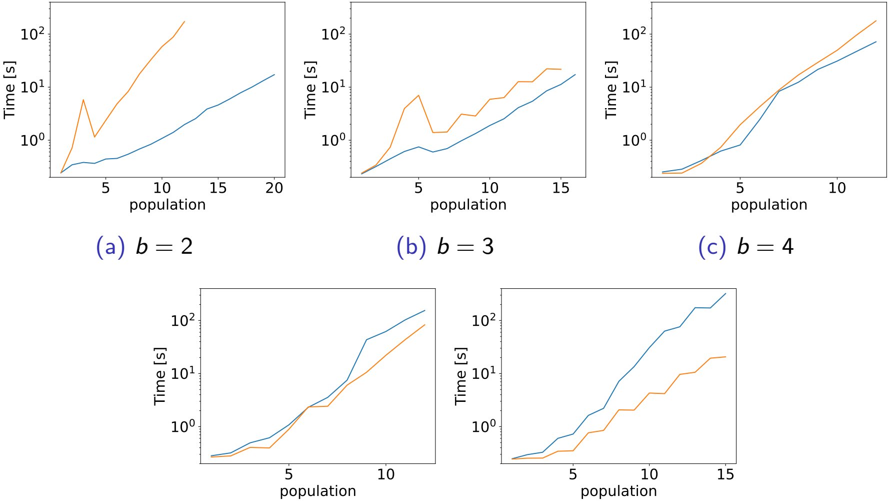


$a' = (a - x) \wedge b' = (b - y)$
$\wedge\ 1 \leq (x + y) \leq 2$
$\wedge\ (a' = 0 \vee a' \geq b')$
$\wedge\ (x = 0 \vee x \geq y)$
$a' = (a + x) \wedge b' = (b + y)$
$\wedge\ (a' = 0 \vee a' \geq b')$
load-1
boat-1-*to*-2
unload-2
(a, b)
(x, y)
$B \times B$
(x, y)
(a', b')
bank-1
$H \times O$
$(3, 3)$
(a', b')
(a, b)
docked-1
docked-2
(a, b)
(a', b')
$(0, 0)$
bank-2
$H \times O$
(a', b')
(x, y)
$B \times B$
(x, y)
(a, b)
unload-1
boat-2-*to*-1
load-2
$a' = (a + x) \wedge b' = (b + y)$
$\wedge\ (a' = 0 \vee a' \geq b')$
$a' = (a - x) \wedge b' = (b - y)$
$\wedge\ 1 \leq (x + y) \leq 2$
$\wedge\ (a' = 0 \vee a' \geq b')$
$\wedge\ (x = 0 \vee x \geq y)$

Parameters: number of hobbits H, number of orcs O, size of boat b, number of rivers r
Modes of load: $M(1) = 2$; $M(b) = M(b-1) + \lfloor b/2 \rfloor + 2$

Benchmark: Hobbits & Orcs — Result

Symbolic vs. Low-level



(a) $b = 2$

(b) $b = 3$

(c) $b = 4$

(d) $b = 5$

(e) $b = 6$

Conclusion

- First tool to use symbolic unfoldings
- First tool to decide reachability for infinetly many reachable markings
- New benchmark families
- Neither approach is generally best: mode determinism

Future work

- Submit benchmark families to MCC
- Implement more general cut-off criterion
- Apply symbolic unfolding to more problems
  - Deadlock detection
  - High-level Petri game strategies
- Generalize to *k*-bounded nets
- Compare to other approaches for analyzing high-level nets