Verification of Token-Scaling Models using an Under-Approximation

Torsten Liebke and Karsten Wolf
Universität Rostock, Germany
Verification of Petri Nets

Verification

Explicit / State Space
- Reachability Graph
- Coverability Graph
- Sweep-Line
- Random Walk

Symbolic
- BDD
- SAT
- Automata

Structural
- State Equation
- Siphon/Trap

→ Portfolio approaches
Portfolio approach

- Run several methods in parallel
- Fastest method determines run-time

→ Room for incomplete methods
Example

Robot manipulation

2n+1 tokens on p_i1
2n tokens on r_stopped
2n tokens on access

n = 1 .. 10000
up to $2.8 \times 10^{31}$ markings

Property:
EF(p_rel > p_m AND p_m > p_rdy)

So far for n = 5000, partial order red.:
$|\text{witness}| = 195006$

With new underapproximation:
$|\text{witness}| = 112$
$|\text{state space}| = 159$
Reduction Idea

Threshold

Proportional
Atomic Propositions

\[ 2p + q \geq 7 \]

Monotonous

only for positive, \( \geq \)
FIREABLE(t)

Shift

for all comparisons

\[ 2p + q \geq 1 \]
Underapproximation

For every marking reachable in transformed net there exists reachable marking in original net

→ Simulation relation
→ Every ACTL* property of original net holds in transformed net
→ Every ECTL* property of transformed net holds in original net
ACTL / ECTL

Atomic propositions
(= > < ≤ ≥ ≠)
∧ ∨
X (nextstep)
F (eventually)
G (globally)
U (until)
R (release)

A (forall paths)  E (exists path)

ACTL*  ECTL*
Usage in MCC

- Sufficient for reachability
- Necessary for LTL formulas
- Sufficient for ECTL formulas
- Necessary for ACTL formula
Heuristics (work in progress)

• Obtain reasonable threshold based on
  • largest constant used in formula
  • largest arc weights used in net
Experiments

• Benchmark: MCC 2019
  • 21 P/T nets scale with number of tokens → 214 net instances
  • 16 formulas ReachabilityCardinality + 16 formulas ReachabilityFireability per instance
    → 6848 formulas

• Environment
  • 32 physical cores, 2.7 GHz, 1TB RAM, CentOS Linux

• Portfolio
  • new method (with partial order reduction)
  • regular state space (with partial order reduction)
  • state equation + CEGAR
Results (threshold: 5)

- 6848 formulas
- 5152 "reachable"
- 1574 "unreachable" or "trivial" (new method cannot yield result)
- 122 "whole portfolio fails"
- 436 "new method"
- 4716 "other method"

8.5 %
Results (proportional: 33%)

- 6848 formulas
- 5152 "reachable"
- 1574 "unreachable" or "trivial" (new method cannot yield result)
- 122 "whole portfolio fails"
- 436 "new method"
- 4716 "other method"

- 114
- 659

- 8.5%  12.8%
Conclusion

• Nice and lightweight addendum to existing portfolio

• Applicable to nets with large bounds

• Complements overapproximation approaches
  • state equation
  • skeleton
Conclusion

• nice

• simple

• incomplete

• helpful

→ should look for more inexpensive incomplete methods