On Combining State Space Reductions with Global Fairness Assumptions

Shaojie Zhang[1] Jun Sun[2] Jun Pang[3] Yang Liu[1] Jin Song Dong[1]

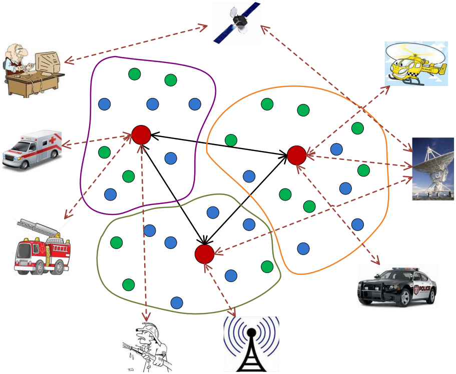
[1]National University of Singapore
[2]Singapore University of Technology and Design
[3]University of Luxembourg

17th International Symposium on Formal Methods

Table of Contents

Population Protocol Model

- Population protocol model is an elegant computation paradigm for describing mobile ad hoc networks [1].



Population Protocol Defining Features

- Anonymous, finite-state agents.
  - Each agent is a finite-state machine.
  - Agents do not have unique IDs.
- Computation by direct interaction.
  - Agents interact only in pairs.
  - Each interaction rule is of the form: $(a, b) \mapsto (c, d)$, in which a, b, c, and d are states.
- Distributed inputs and outputs.

- Convergence rather than termination.
  - A distributed system is said to be self-stabilizing if it satisfies the following two properties:
    - *convergence*: starting from an arbitrary configuration, the system is guaranteed to reach a stable configuration;
    - *closure*: once the system reaches a stable configuration, it cannot become unstable any more.
  - LTL Formulation
    - $\Diamond\Box$*property*
- Unpredictable interaction patterns.
  - A global fairness condition is imposed to ensure the protocol makes progress.

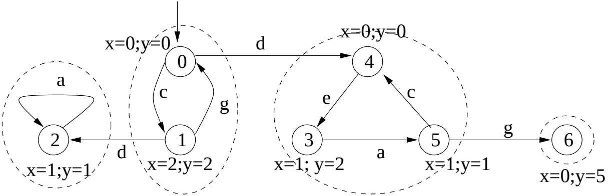
Our Contribution

- We investigate the problem of model checking with
  - Global fairness and *symmetry reduction*
    - prove that symmetry reduction and global fairness can be integrated without extra effort
    - present the combined reduction algorithm based on Tarjan's strongly connected component algorithm
  - Global fairness and *partial order reduction*
    - not property preserving

Table of Contents

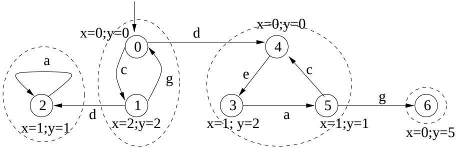
Model & Logic

- Labeled Kripke structure : Kripke structure + labeled transition system
- State/event linear temporal logic
  - $\Box(d \Rightarrow \Diamond(x > 1))$

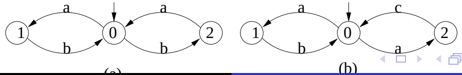


Fairness Constraints

- Weak fairness: if an event becomes enabled *forever* after some steps, then it must be engaged infinitely often.
- Strong fairness: if an event is *infinitely often* enabled, it must infinitely often occur.



- Global fairness: if a *transition* (from s to s' by engaging in event e) can be taken infinitely often, then it must actually be taken infinitely often.



Fairness Model Checking Algorithm

- On-the-fly model checking based on Tarjan's algorithm for identifying SCC
  - Tarjan's algorithm to search for SCCs.
  - Check different fairness inside the found SCCs.
  - model checking with global fairness can be reduced to the problem of searching for a terminal SCC which fails the given property [2].
    - An SCC fails a liveness property $\phi \Leftrightarrow$ a run which reaches any state in the SCC and infinitely often traverses through all states and transitions of the SCC fails.

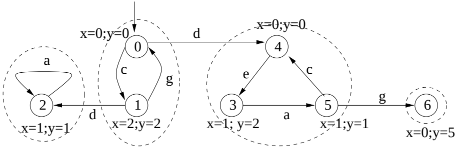


Table of Contents

- We have:
  - $\mathcal{L} \vDash_{gf} \phi$ if and only if there does not exist a terminal SCC S in $\mathcal{L}$ such that S fails ϕ.
- There exists a run $p = \langle s_0, a_0, s_1, a_1, \cdots \rangle$ in $\mathcal{L}$ if and only if there exists a run $q = \langle r_0, a_0, r_1, a_1, \cdots \rangle$ in $\mathcal{L}_G$ such that $r_i = rep(s_i)$ for all i [3].
- There exists an accepting loop in the product of $\mathcal{L}$ and $\mathcal{B}$ which satisfies global fairness if and only if there also exists an accepting loop in the product of $\mathcal{L}_G$ and $\mathcal{B}$ which satisfies global fairness.
- In the product of $\mathcal{L}$ (resp. $\mathcal{L}_G$) and $\mathcal{B}$, there exists an accepting loop which satisfies global fairness if and only if there exists an accepting SCC which is also a terminal SCC in $\mathcal{L}$ (resp.$\mathcal{L}_G$).
- We need to prove:
  - $\mathcal{L} \vDash_{gf} \phi$ if and only if $\mathcal{L}_G \vDash_{gf} \phi$.

- We have:
  - $\mathcal{L} \vDash_{gf} \phi$ if and only if there does not exist a terminal SCC S in $\mathcal{L}$ such that S fails ϕ.
- There exists a run $p = \langle s_0, a_0, s_1, a_1, \cdots \rangle$ in $\mathcal{L}$ if and only if there exists a run $q = \langle r_0, a_0, r_1, a_1, \cdots \rangle$ in $\mathcal{L}_G$ such that $r_i = rep(s_i)$ for all i [3].
- There exists an accepting loop in the product of $\mathcal{L}$ and $\mathcal{B}$ which satisfies global fairness if and only if there also exists an accepting loop in the product of $\mathcal{L}_G$ and $\mathcal{B}$ which satisfies global fairness.
- In the product of $\mathcal{L}$ (resp. $\mathcal{L}_G$) and $\mathcal{B}$, there exists an accepting loop which satisfies global fairness if and only if there exists an accepting SCC which is also a terminal SCC in $\mathcal{L}$ (resp.$\mathcal{L}_G$).
- We need to prove:
  - $\mathcal{L} \vDash_{gf} \phi$ if and only if $\mathcal{L}_G \vDash_{gf} \phi$.

- We have:
  - $\mathcal{L} \vDash_{gf} \phi$ if and only if there does not exist a terminal SCC S in $\mathcal{L}$ such that S fails ϕ.
- There exists a run $p = \langle s_0, a_0, s_1, a_1, \cdots \rangle$ in $\mathcal{L}$ if and only if there exists a run $q = \langle r_0, a_0, r_1, a_1, \cdots \rangle$ in $\mathcal{L}_G$ such that $r_i = rep(s_i)$ for all i [3].
- There exists an accepting loop in the product of $\mathcal{L}$ and $\mathcal{B}$ which satisfies global fairness if and only if there also exists an accepting loop in the product of $\mathcal{L}_G$ and $\mathcal{B}$ which satisfies global fairness.
- In the product of $\mathcal{L}$ (resp. $\mathcal{L}_G$) and $\mathcal{B}$, there exists an accepting loop which satisfies global fairness if and only if there exists an accepting SCC which is also a terminal SCC in $\mathcal{L}$ (resp.$\mathcal{L}_G$).
- We need to prove:
  - $\mathcal{L} \vDash_{gf} \phi$ if and only if $\mathcal{L}_G \vDash_{gf} \phi$.

- We have:
  - $\mathcal{L} \vDash_{gf} \phi$ if and only if there does not exist a terminal SCC S in $\mathcal{L}$ such that S fails ϕ.
- There exists a run $p = \langle s_0, a_0, s_1, a_1, \cdots \rangle$ in $\mathcal{L}$ if and only if there exists a run $q = \langle r_0, a_0, r_1, a_1, \cdots \rangle$ in $\mathcal{L}_G$ such that $r_i = rep(s_i)$ for all i [3].
- There exists an accepting loop in the product of $\mathcal{L}$ and $\mathcal{B}$ which satisfies global fairness if and only if there also exists an accepting loop in the product of $\mathcal{L}_G$ and $\mathcal{B}$ which satisfies global fairness.
- In the product of $\mathcal{L}$ (resp. $\mathcal{L}_G$) and $\mathcal{B}$, there exists an accepting loop which satisfies global fairness if and only if there exists an accepting SCC which is also a terminal SCC in $\mathcal{L}$ (resp.$\mathcal{L}_G$).
- We need to prove:
  - $\mathcal{L} \vDash_{gf} \phi$ if and only if $\mathcal{L}_G \vDash_{gf} \phi$.

```
int counter := 0;
stack path := an empty stack;
hashtable index := an empty hash table;
hashtable lowlink := an empty hash table;
TarjanModelChecking((init_s, init_b));

procedure TarjanModelChecking(v)
    index[rep(v)] := counter;
    lowlink[rep(v)] := counter;
    counter := counter + 1;
    push rep(v) into path
    forall v → v' do
        if (rep(v') is not in index)
            TarjanModelChecking(v')
            lowlink[rep(v)] = min(lowlink[rep(v)], lowlink[rep(v')]);
        else if (rep(v') is in path)
            lowlink[rep(v)] = min(lowlink[rep(v)], index[rep(v')]);
        endif
    endfor
    if (lowlink[rep(v)] = index[rep(v)])
        set scc := an empty set;
        repeat
            pop an element v' from path and add it into scc;
        until (v' = v)
        if (scc forms a terminal SCC in ℒ and scc is accepting)
            generate a counterexample and return false;
        endif
    endif
endprocedure
```

Experimental Result

Model	Network Size	Without Reduction		With Reduction		
		States	Time (Sec)	States	Time (Sec)	Gain
two-hop coloring	3	122856	36.7	42182	16.7	54.5%
orienting rings (prop 1)	3	19190	2.27	6398	0.53	76.7%
orienting rings (prop 2)	3	19445	2.23	6503	0.97	56.5%
orienting rings (prop 1)	4	1255754	267.2	313940	70.5	73.6%
orienting rings (prop 2)	4	1206821	267.1	302071	63.6	79.6%
orienting rings (prop 1)	5	11007542	9628.1	2201510	1067.4	88.9%
orienting rings (prop 2)	5	10225849	8322.6	2045935	954.5	88.5%
leader election (complete)	3	6946	0.87	2419	0.51	41.4%
leader election (complete)	4	65468	11.6	16758	5.00	56.9%
leader election (complete)	5	598969	176.1	120021	45.9	73.9%
leader election (odd)	3	55100	6.27	18561	2.56	59.2%
leader election (odd)	5	—	—	6444097	5803.96	×
token circulation	3	728	0.12	244	0.09	25.0%
token circulation	4	4466	0.35	1118	0.19	45.7%
token circulation	5	24847	1.86	4971	0.77	58.6%
token circulation	6	129344	10.7	21559	3.03	71.7%
token circulation	7	643666	77.2	91954	16.2	79.0%
token circulation	8	3104594	740.8	388076	97.1	86.9%

Table of Contents

- Partial order reduction is an effective state reduction technique for concurrent systems with *independent* actions.
- Partial order reduction + global fairness?

Definition

An independence relation $I \subseteq \rightarrow \times \rightarrow$ is a symmetric, antireflexive relation, satisfying the following two conditions for each state $s \in S$ and for each $(\alpha, \beta) \in I$:
(1) If $\alpha, \beta \in \mathit{enabled}(s)$, then $\alpha \in \mathit{enabled}(\beta(s))$.
(2) If $\alpha, \beta \in \mathit{enabled}(s)$, then $\alpha(\beta(s)) = \beta(\alpha(s))$.

Definition

Let $L : S \rightarrow 2^{AP}$ be the function that labels each state with a set of atomic propositions. A transition $\alpha \in T$ is invisible with respect to a set of propositions $AP' \subseteq AP$ if for each pair of states $s, s' \in S$ such that $s' = \alpha(s)$, $L(s) \cap AP' = L(s') \cap AP'$.

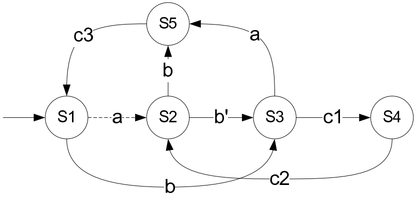
- C0 $\mathit{ample}(s) = \varnothing$ iff $\mathit{enabled}(s) = \varnothing$.
- C1 Along every path in the full state space starting from s, a transition that is dependent on a transition in $\mathit{ample}(s)$ cannot occur without one in $\mathit{ample}(s)$ occurring first.
- C2 If $\mathit{enabled}(s) \neq \mathit{ample}(s)$, then every $\alpha \in \mathit{ample}(s)$ is invisible.
- C3 A cycle is not allowed if it contains a state in which some transition α is enabled, but is never included in $\mathit{ample}(s)$ for any state s on the cycle.

Theorem

The original state space and reduced state space are stuttering equivalent.

Suppose the transitions labeled with a and b be independent and all other transitions be mutually dependent; let b, b' be invisible and a, c_1, c_2, c_3 visible

- Consider a globally fair path $\lambda = (abc_3bc_1c_2b'ac_3)^\omega$



Summary

- Unlike weak/strong fairness, global fairness can be combined with symmetry reduction.
- Present a practical fairness model checking algorithm with symmetry reduction.
- Classic partial order reduction can not guarantee to preserve properties with global fairness.

- Future work
  - Symmetry detection
  - Identify sufficient condition that allows the combination of fairness and abstraction

References I

- D. Angluin, J. Aspnes, M. J. Fischer and H. Jiang.
  Self-stabilizing Population Protocols.
  OPODIS, pp 103-117, 2005.
- J. Sun, Y. Liu, J. S. Dong and J. Pang,
  PAT: Towards Flexible Verification under Fairness,
  CAV, pp 709-714, 2009.
- E. A. Emerson and A. P. Sistla,
  Symmetry and Model Checking,
  Formal Methods in System Design, 9(1-2), pp 105-131, 1996.

Discussion

- Compare with related work
  - $O(|\overline{M}| \times n^3 \times |g| \times a)$