Formal Verification of Real-time Systems

Tomohiro Yoneda

National Institute of Informatics

Tokyo Institute of Technology

Personal History

- Ph.D thesis
  - 1985, Tokyo Institute of Technology
  - Adviser: Prof. Tohma
- 3 Papers in FTCS
  - FTCS-15, 16, 19
- Current interests
  - Formal verification of real-time systems
  - Synthesis tools for Asynchronous circuits
  - Main Conferences: ASYNC, CAV

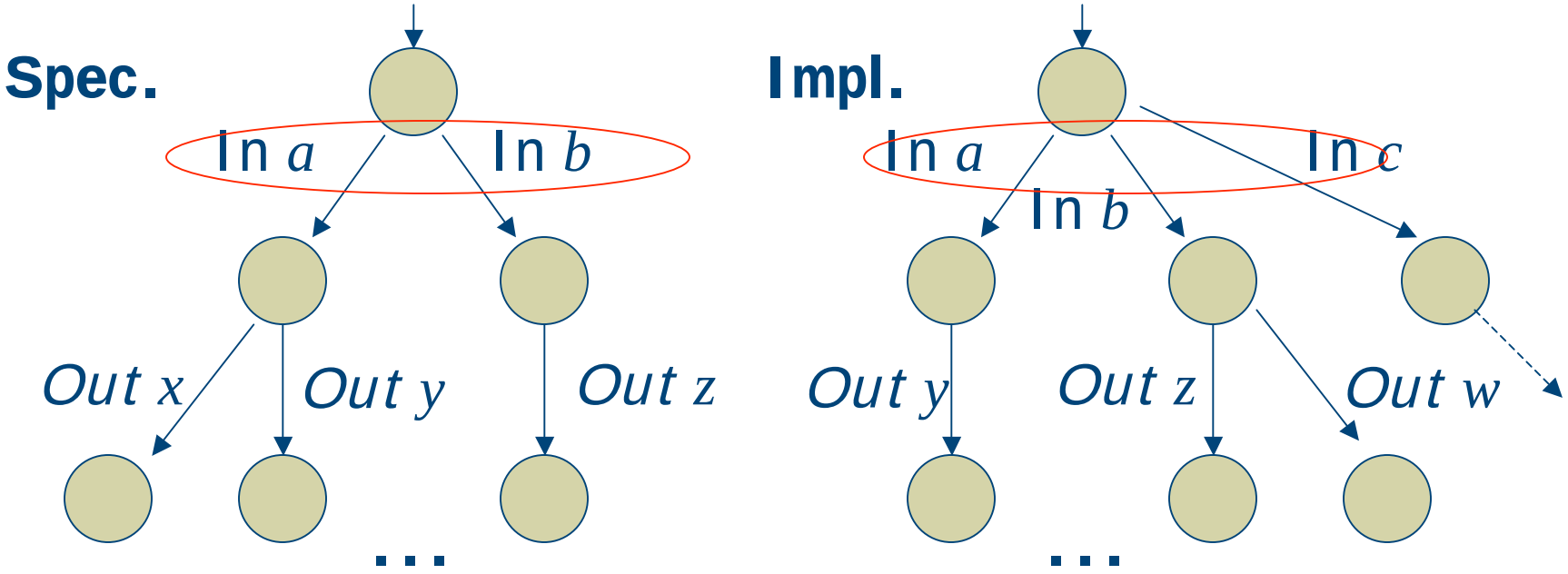
What are verified and how?

- What?
  - Time dependent systems
    - Circuits composed of gates with bounded delays
    - Protocols for real-time control
- How?
  - Conformance Checking
    - Impl. and Spec. are expressed by the same model
    - State space exploration checking correspondence
  - Contribution
    - Extension to real-time models, improvement in performance, development of a tool

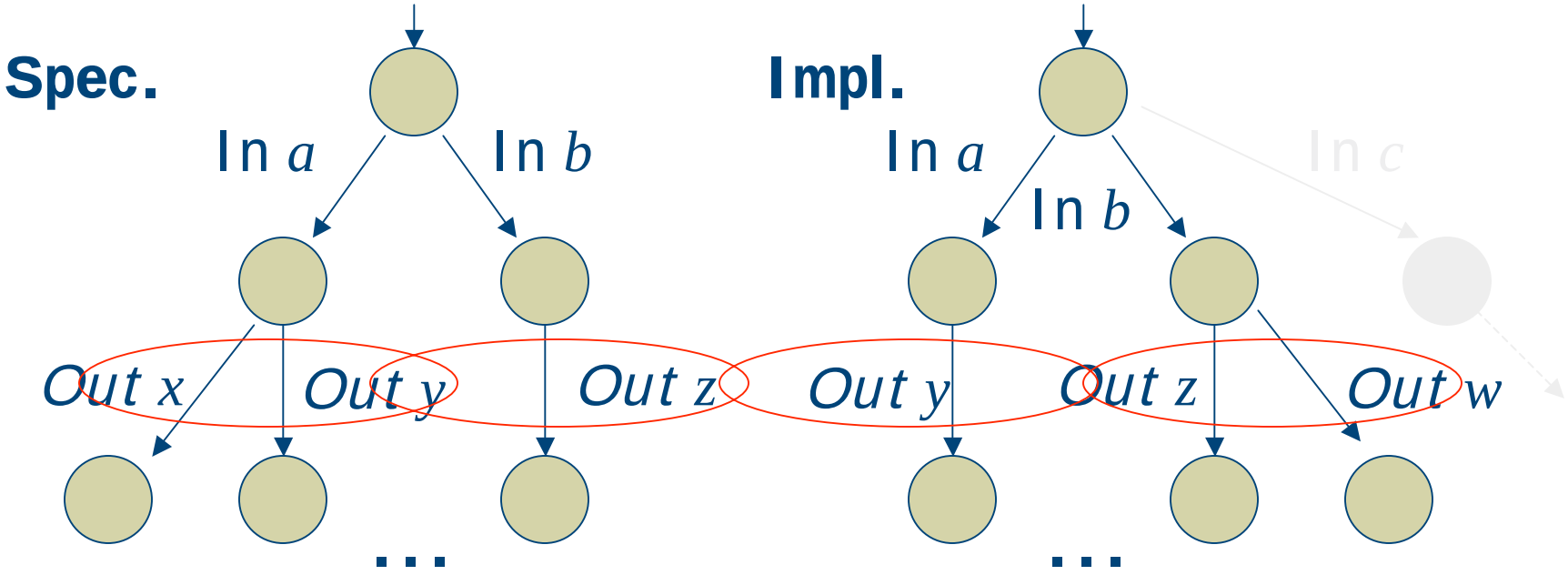
Approach

- Formal model used
  - Time Petri nets
- Improvement in performance
  - Partial order reduction technique
  - Hierarchical verification technique

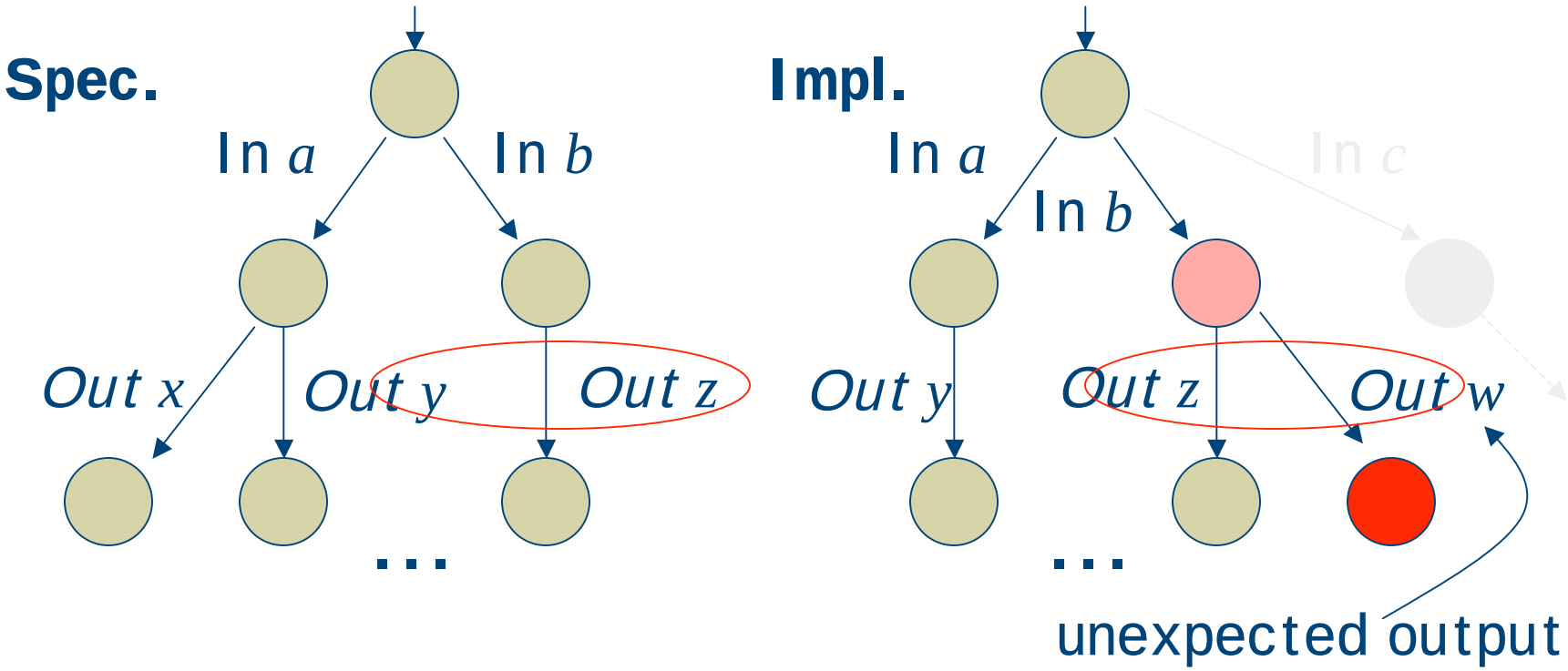
Verification method (1)



Verification method (1)

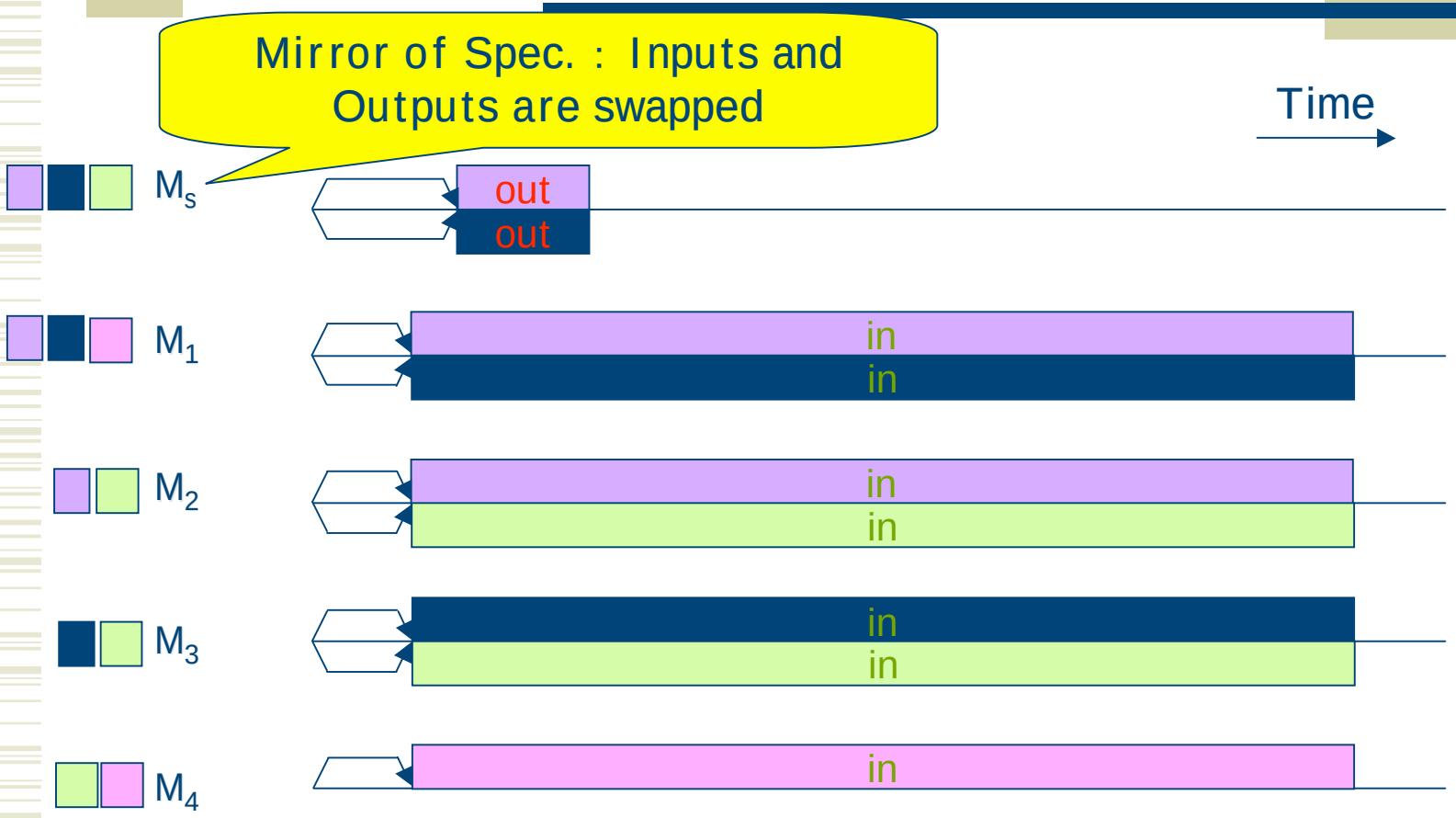


Verification method (1)

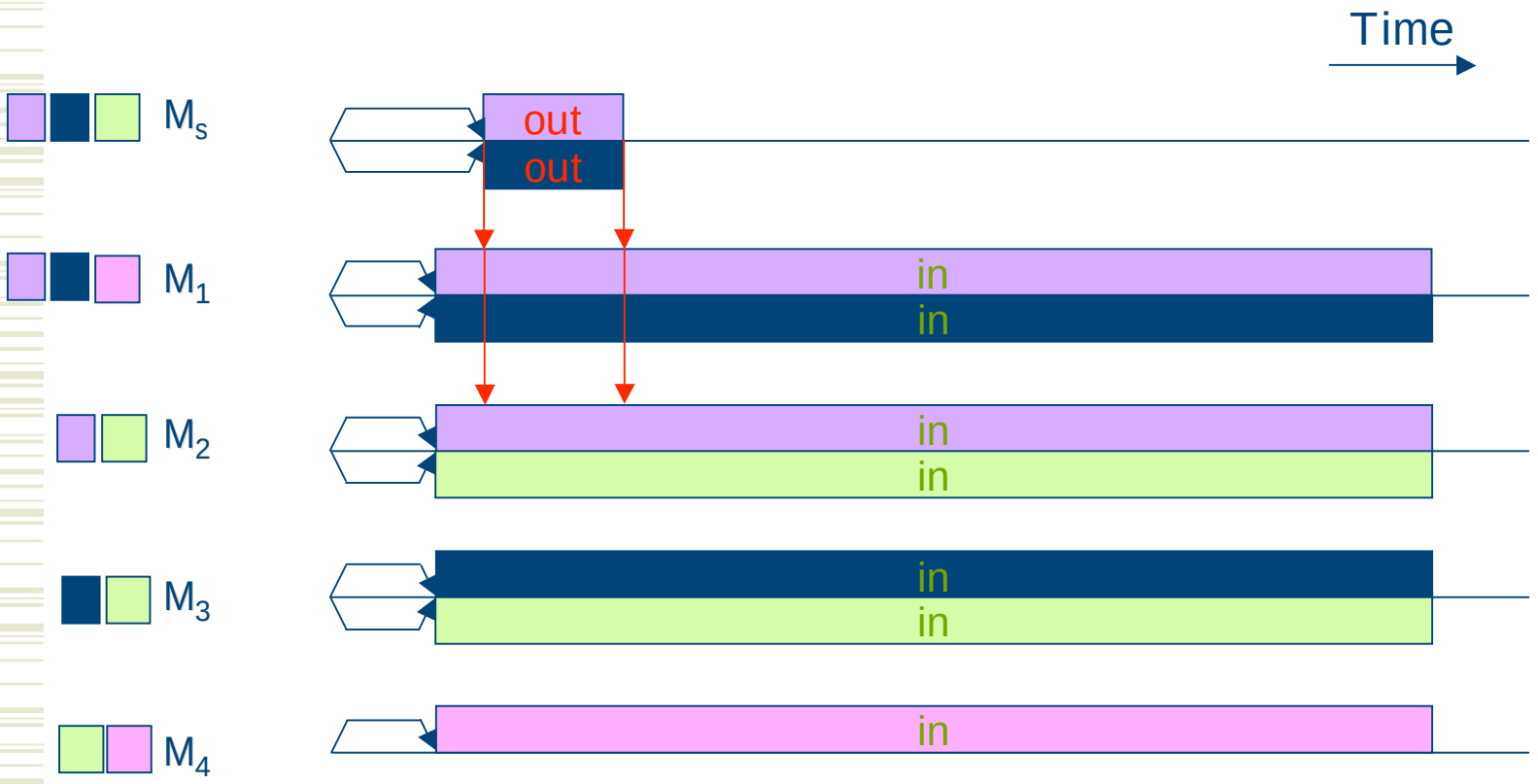


- Unexpected outputs must not be produced
- Expected outputs must be produced within given time frame

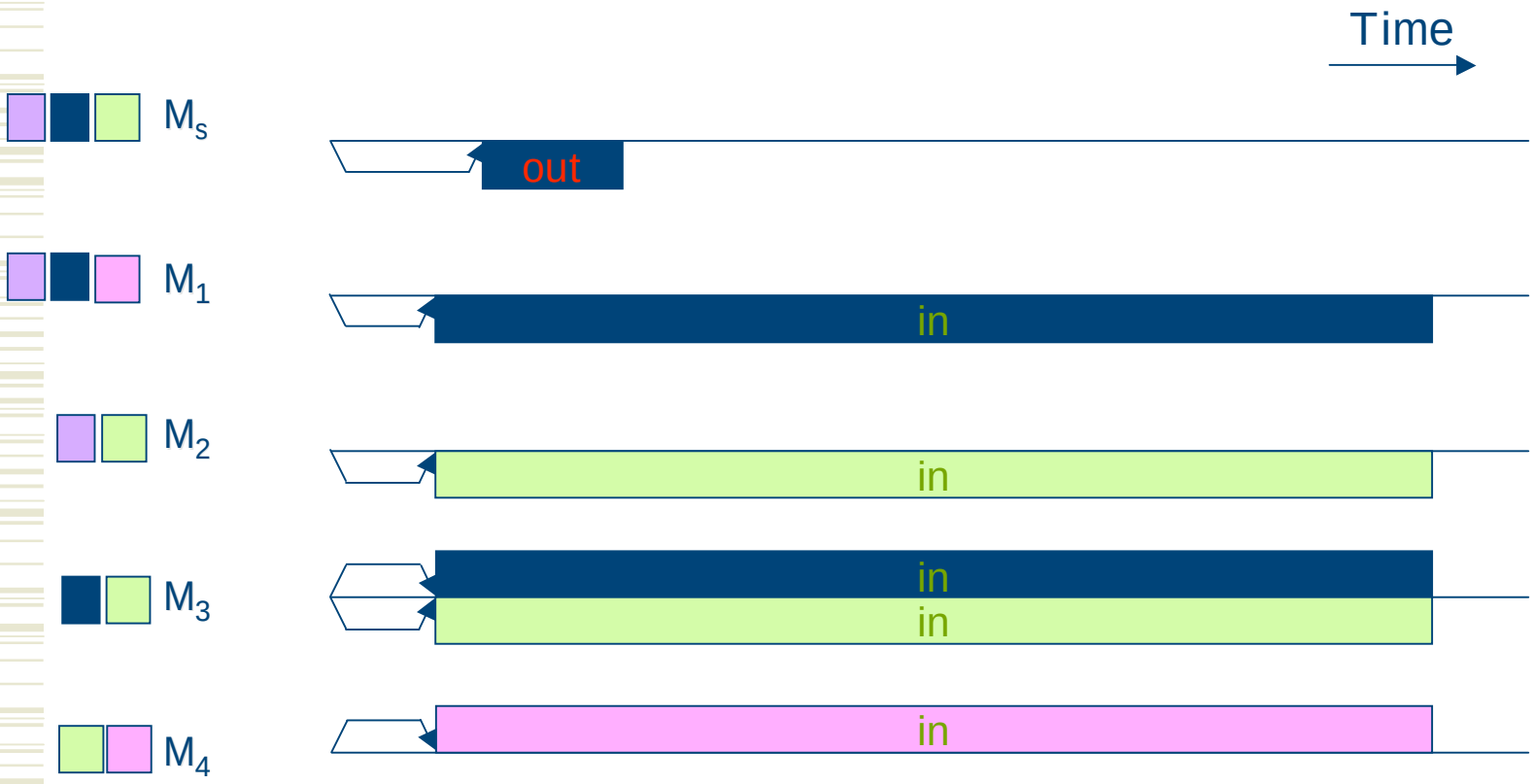
Verification method (2)



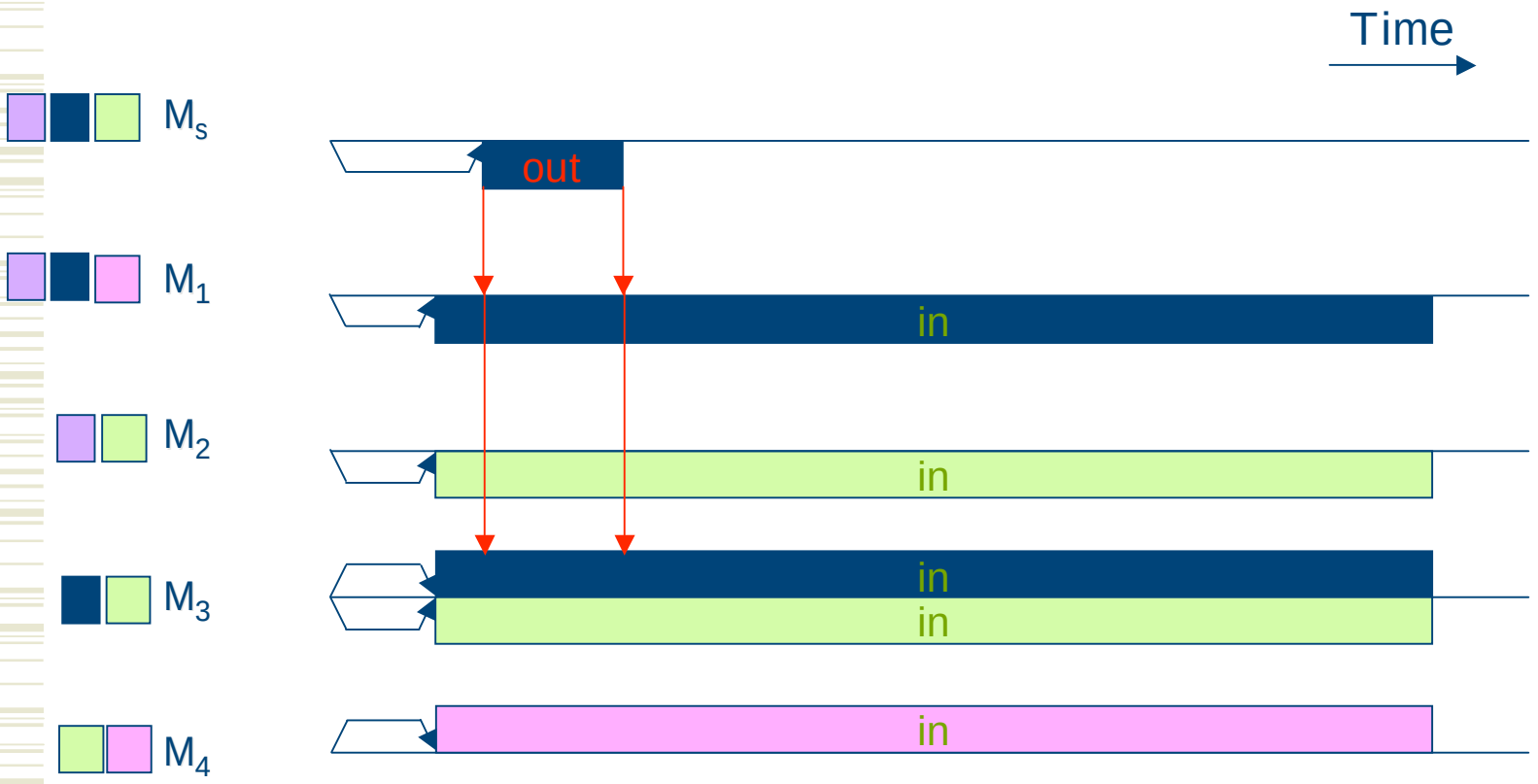
Verification method (2)



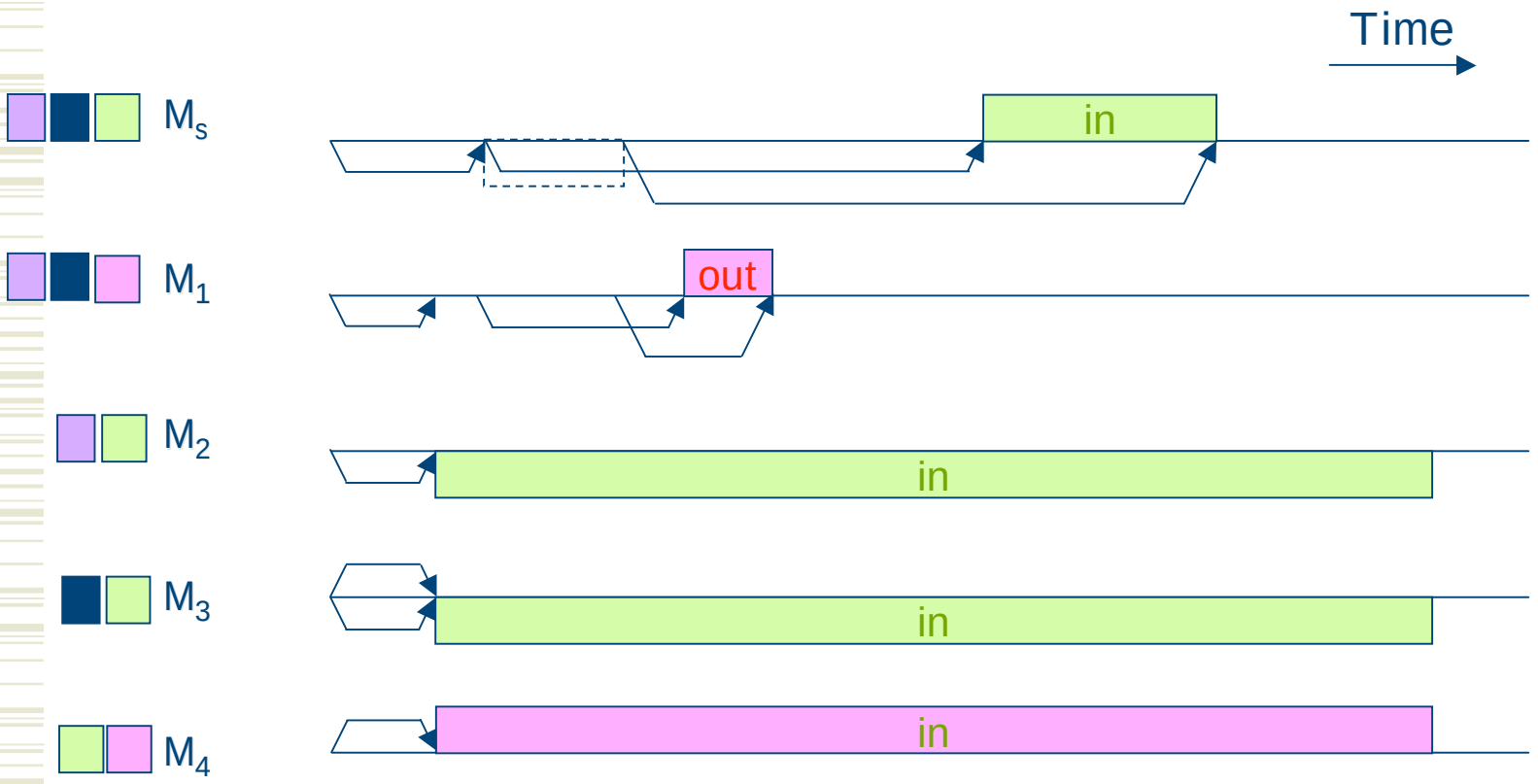
Verification method (2)



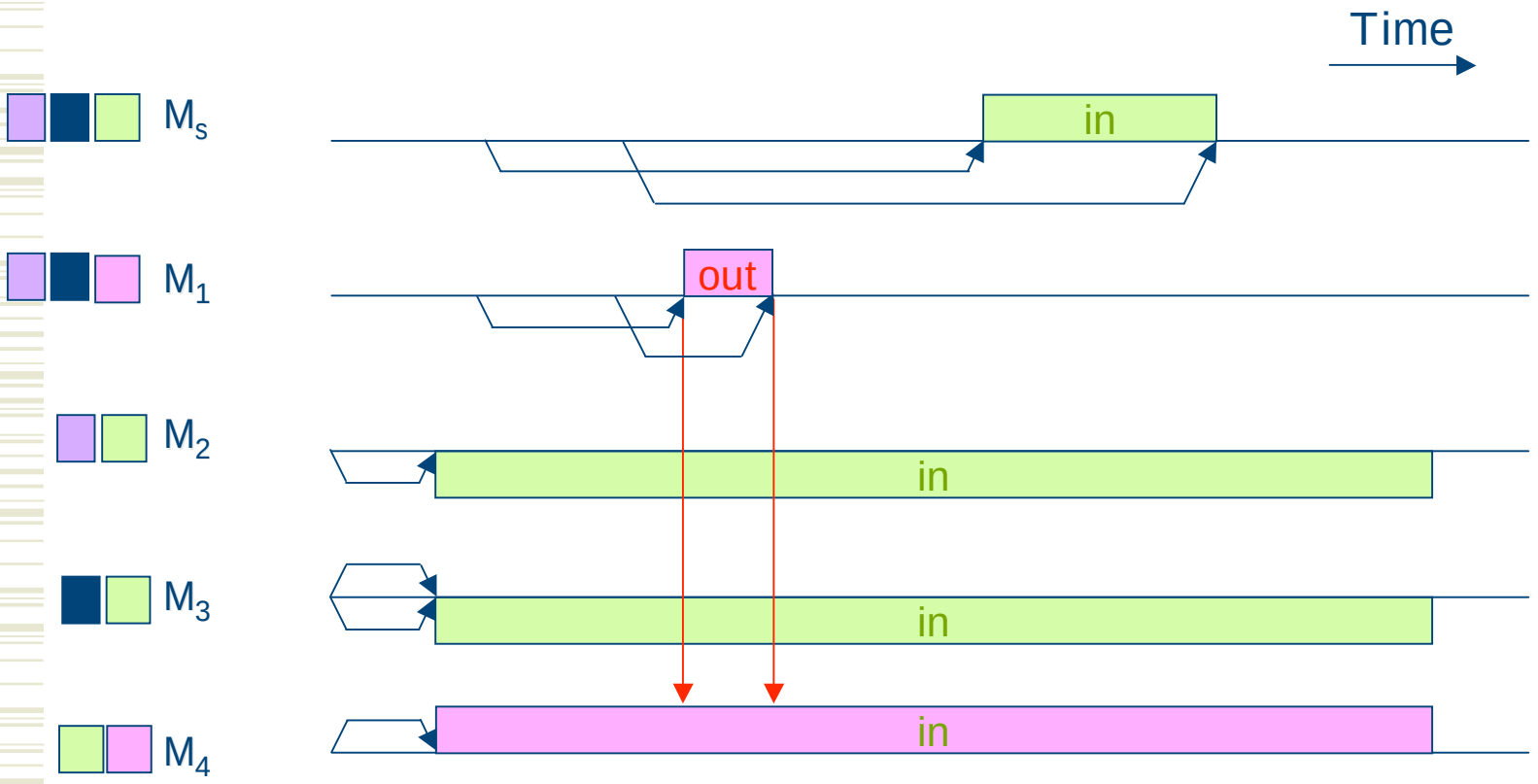
Verification method (2)



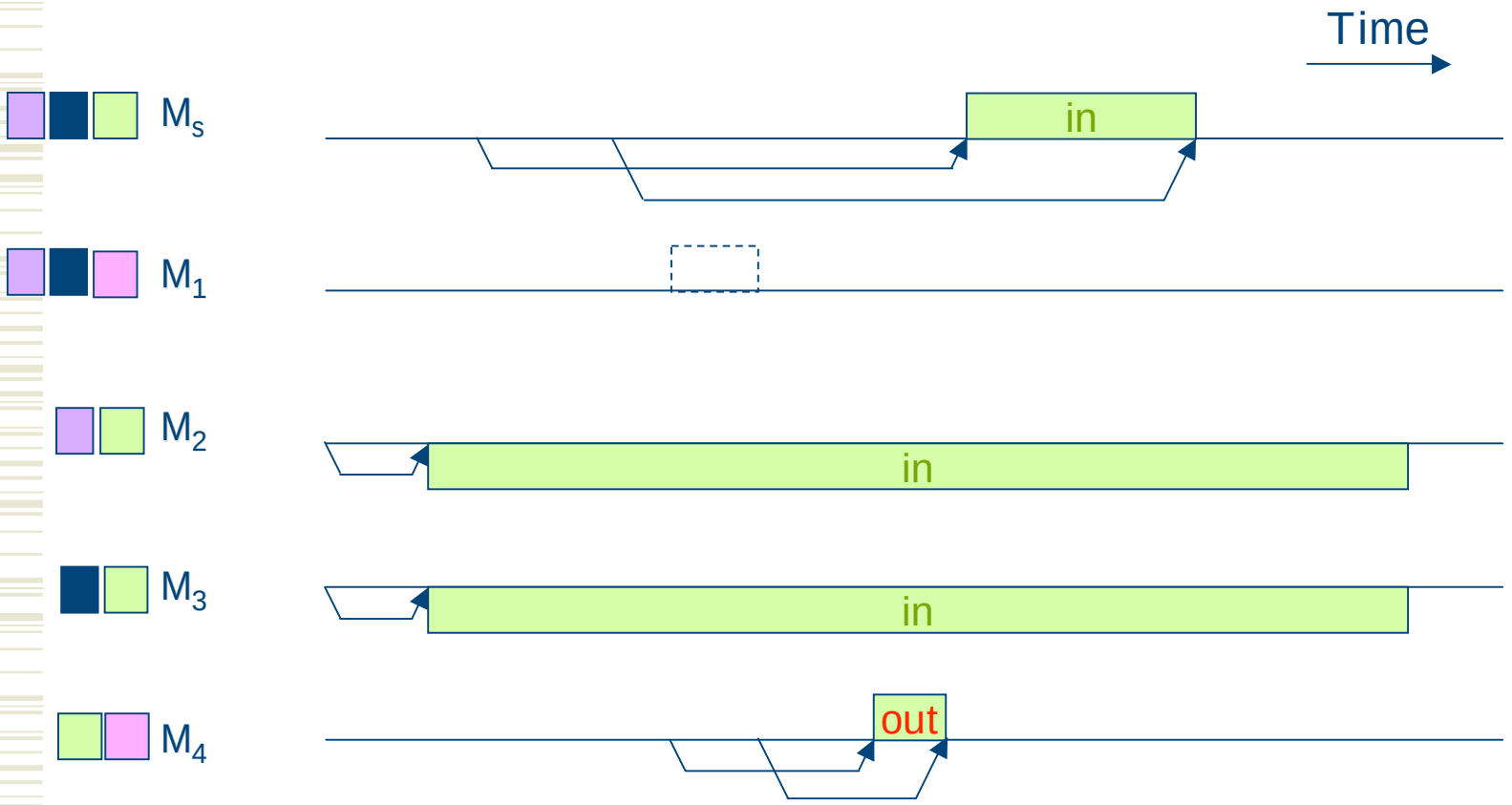
Verification method (2)



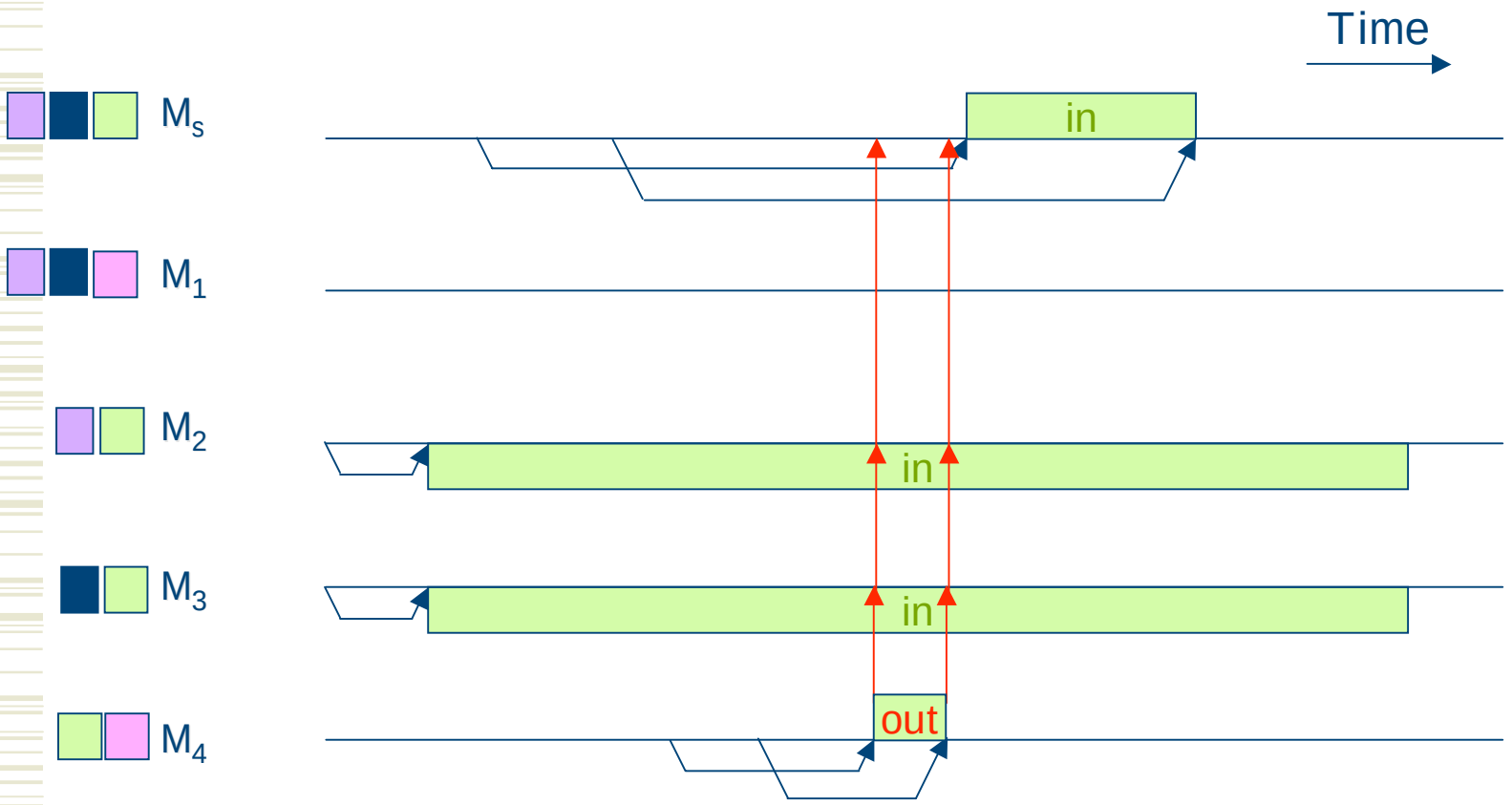
Verification method (2)



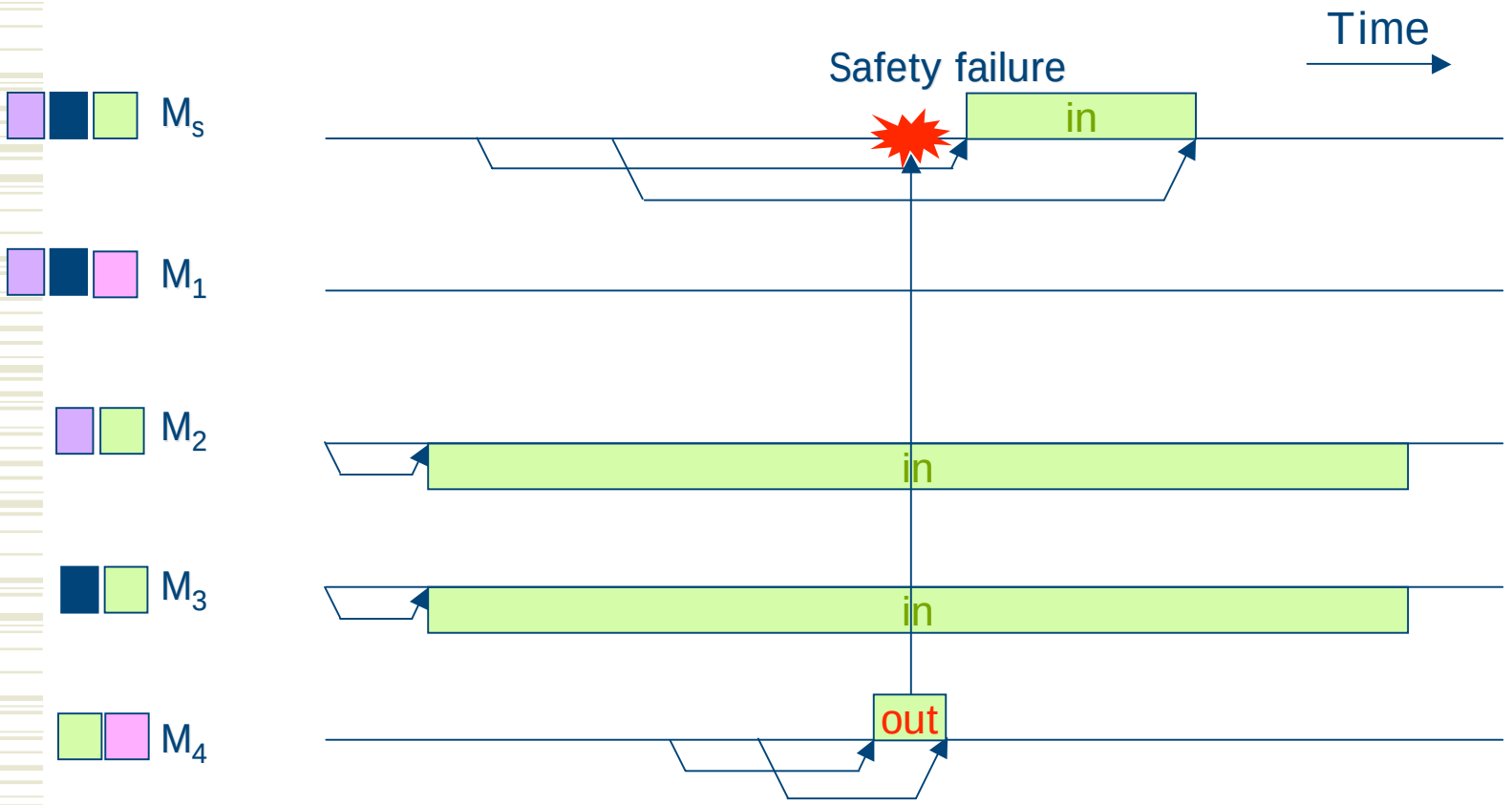
Verification method (2)



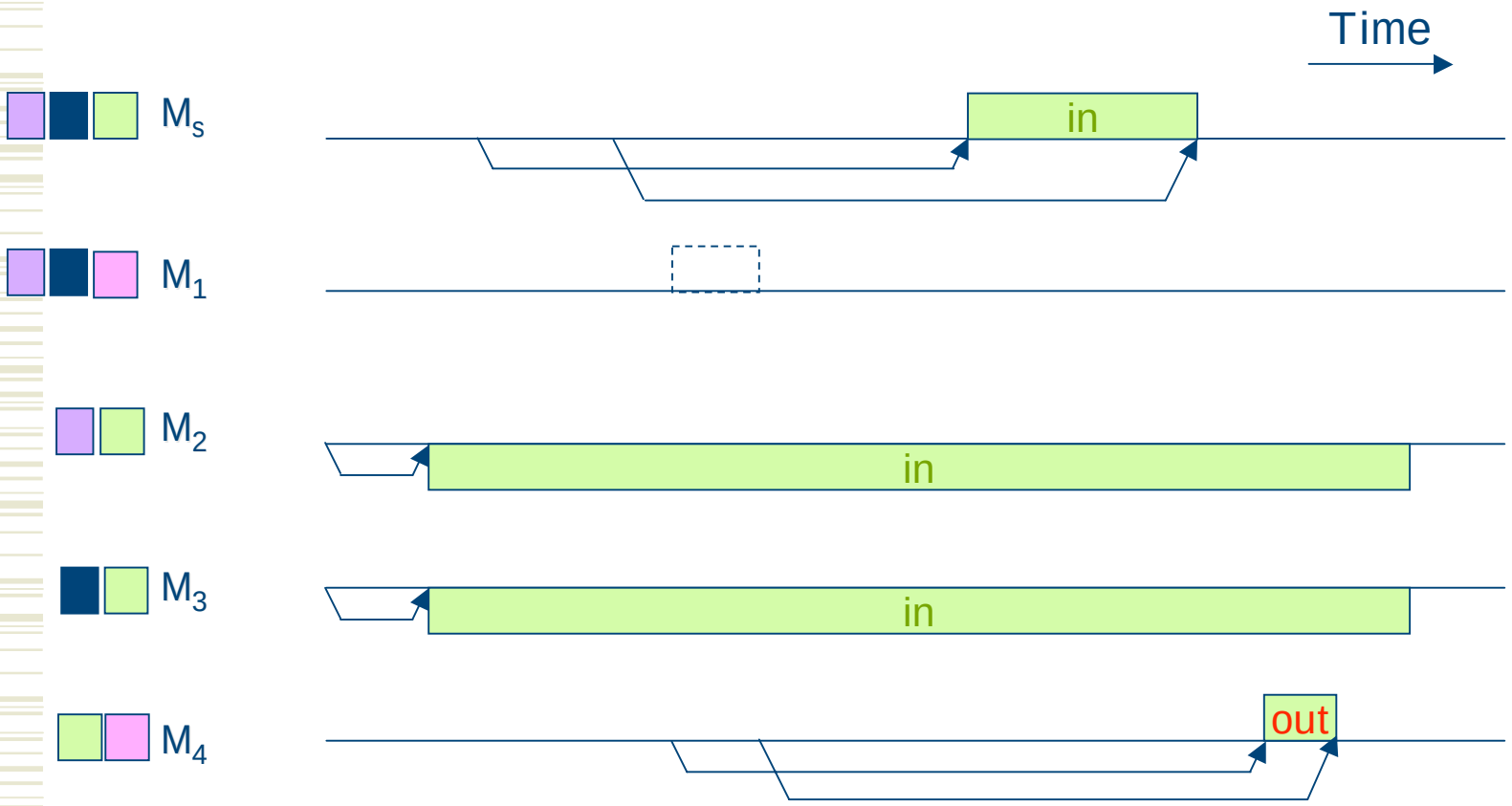
Verification method (2)



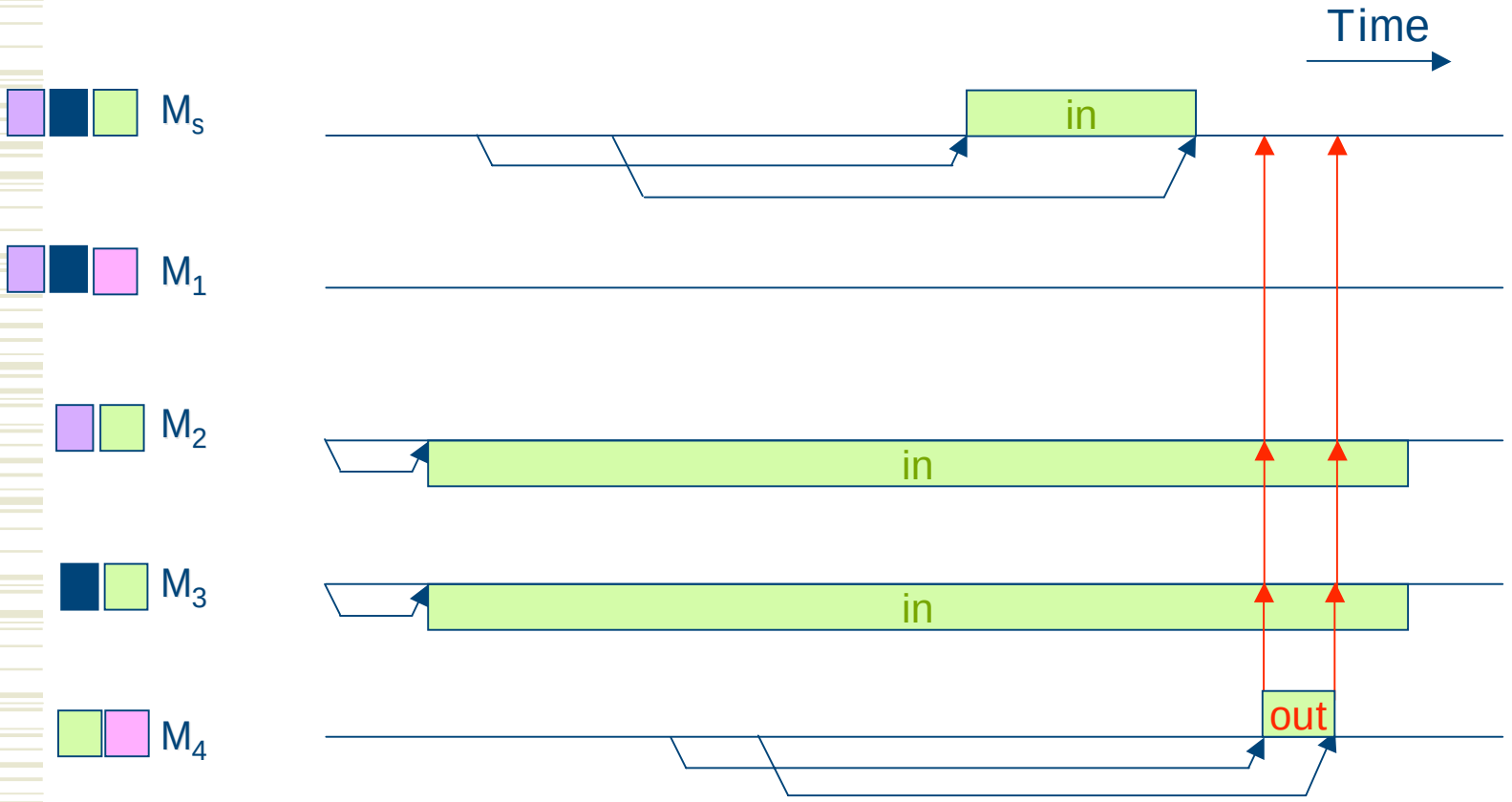
Verification method (2)



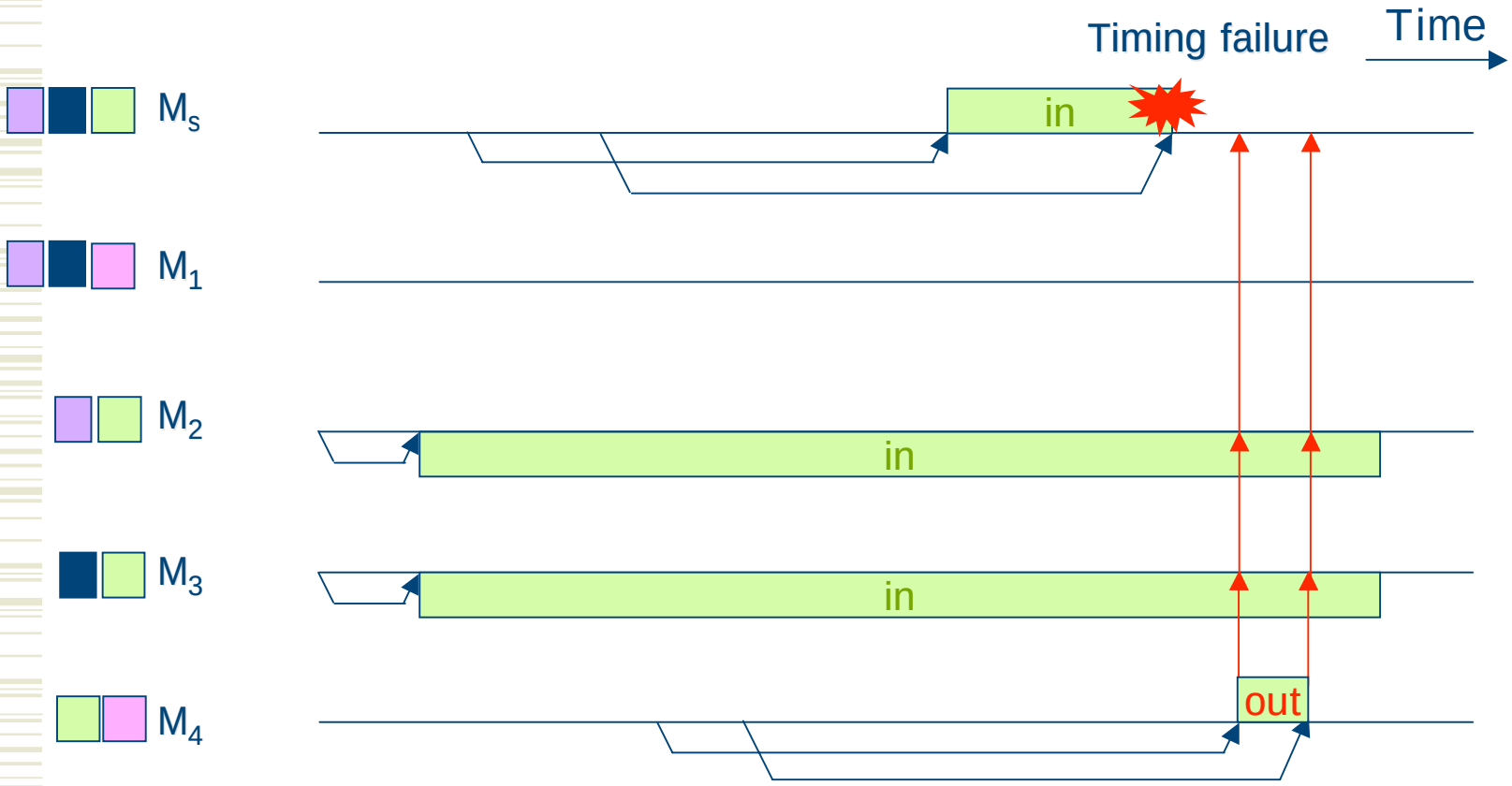
Verification method (2)



Verification method (2)



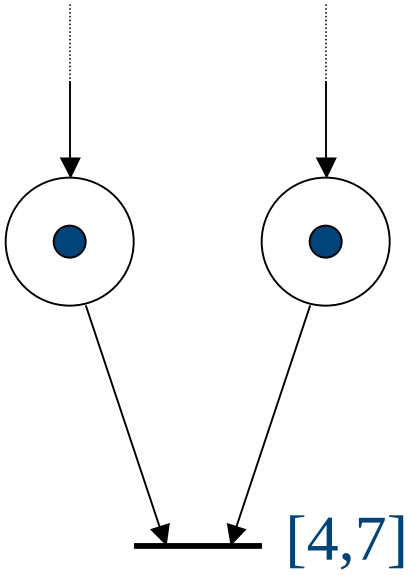
Verification method (2)

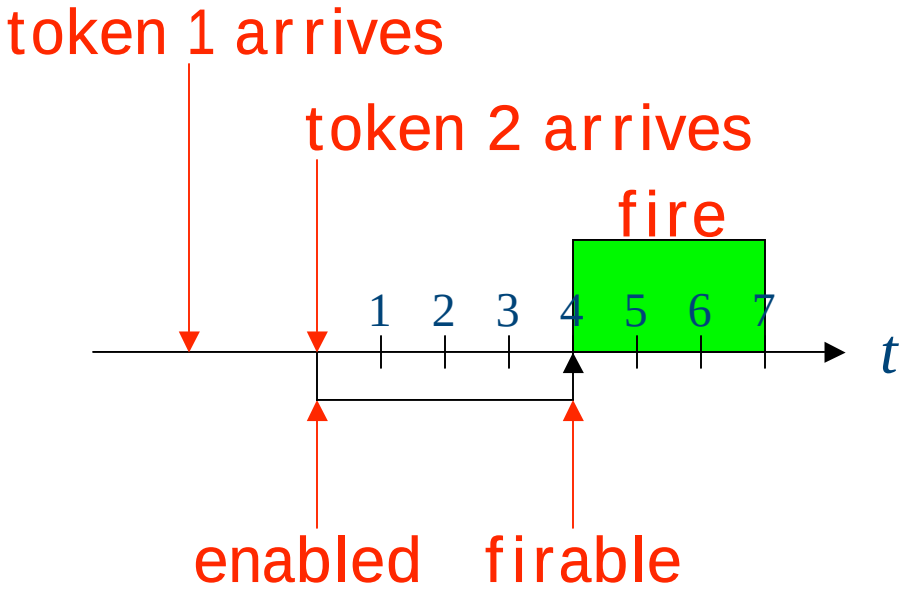


Verification method (3)

- Advantages
  - More intuitive than temporal logics
    - It is not easy to express complicated properties or expected behavior using temporal logics
  - Several methods for performance improvement
    - Partial order reduction
    - Hierarchical verification
- Drawbacks
  - Spec. must be deterministic
  - A little less expressive

Time Petri nets





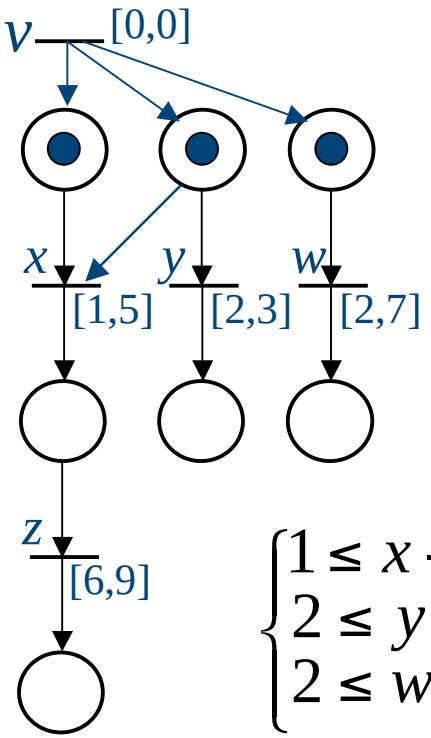
Timed state space exploration

- State
  - marking
  - a set of inequalities

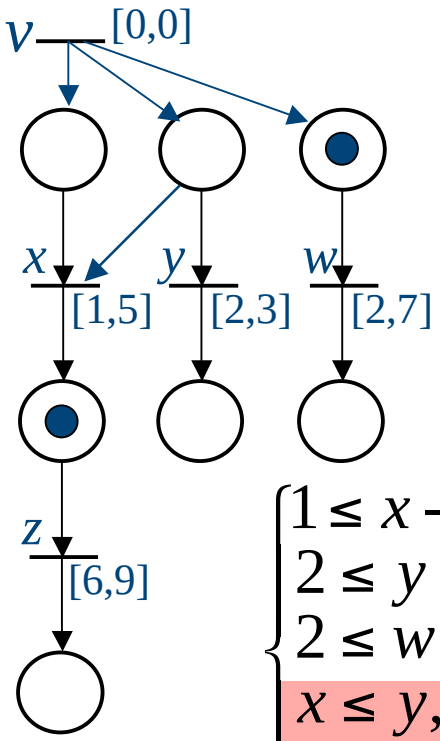
Decision of existence of solutions

↓

Floyd's shortest path algorithm



x fires



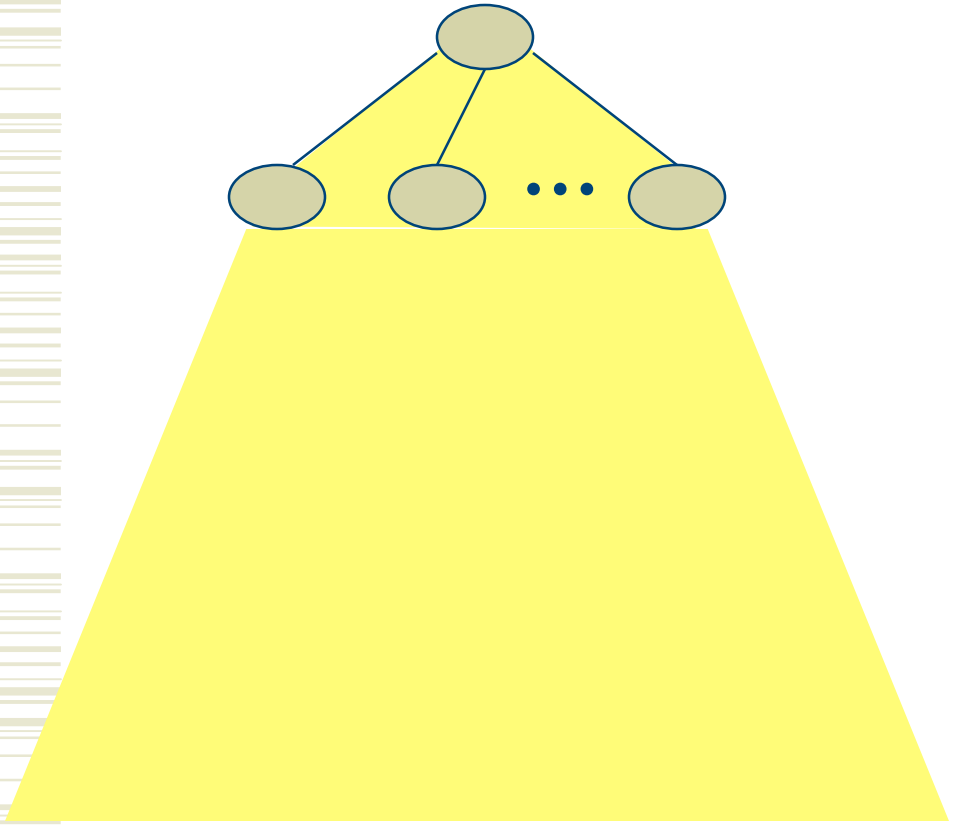
$$\begin{cases} 1 \le x - v \le 5 \\ 2 \le y - v \le 3 \\ 2 \le w - v \le 7 \end{cases}$$

$$\begin{cases} 1 \le x - v \le 5 \\ 2 \le y - v \le 3 \\ 2 \le w - v \le 7 \\ x \le y,\ x \le w \\ 6 \le z - x \le 9 \end{cases}$$

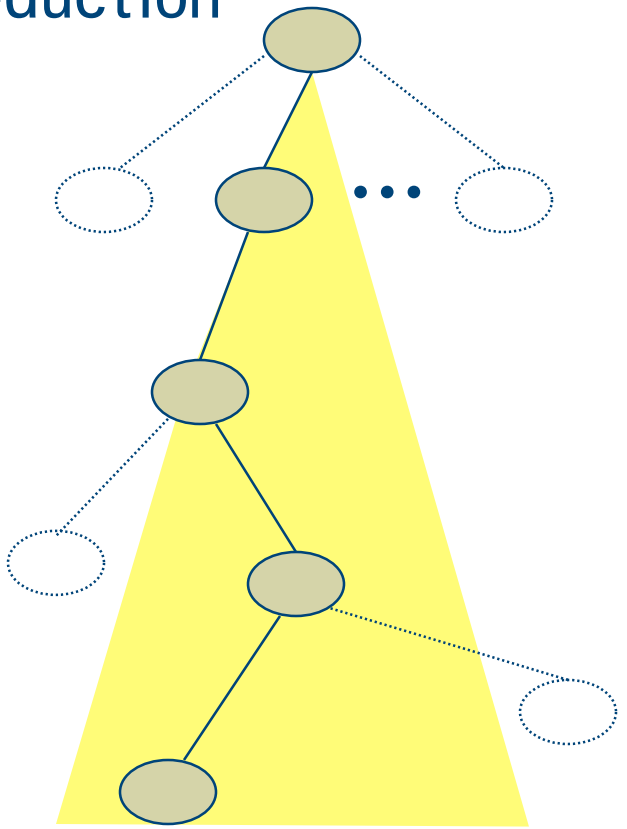
variables for times of transition firings

Partial Order Reduction (1)

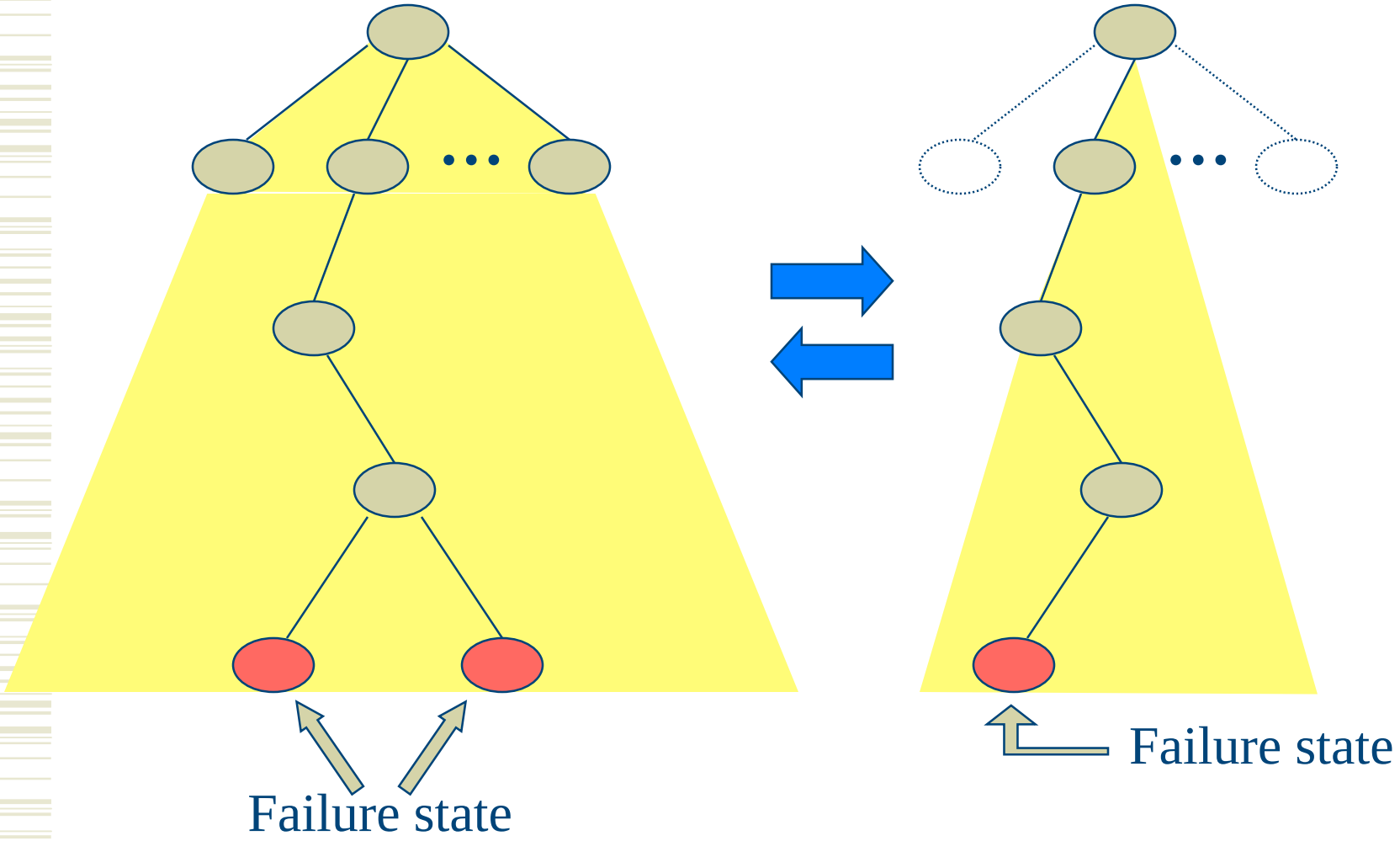
Full state space exploration



State space exploration based on Partial Order Reduction

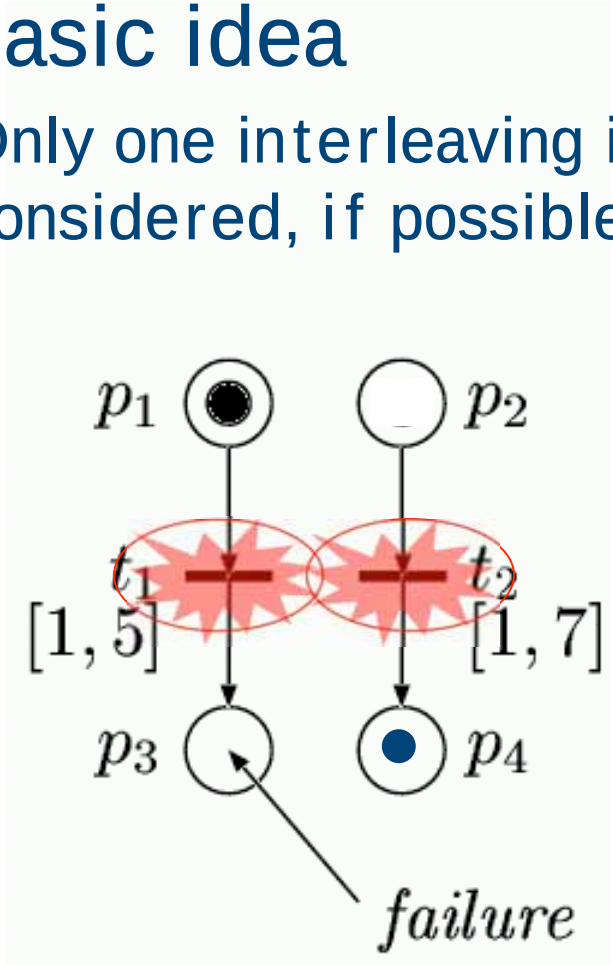


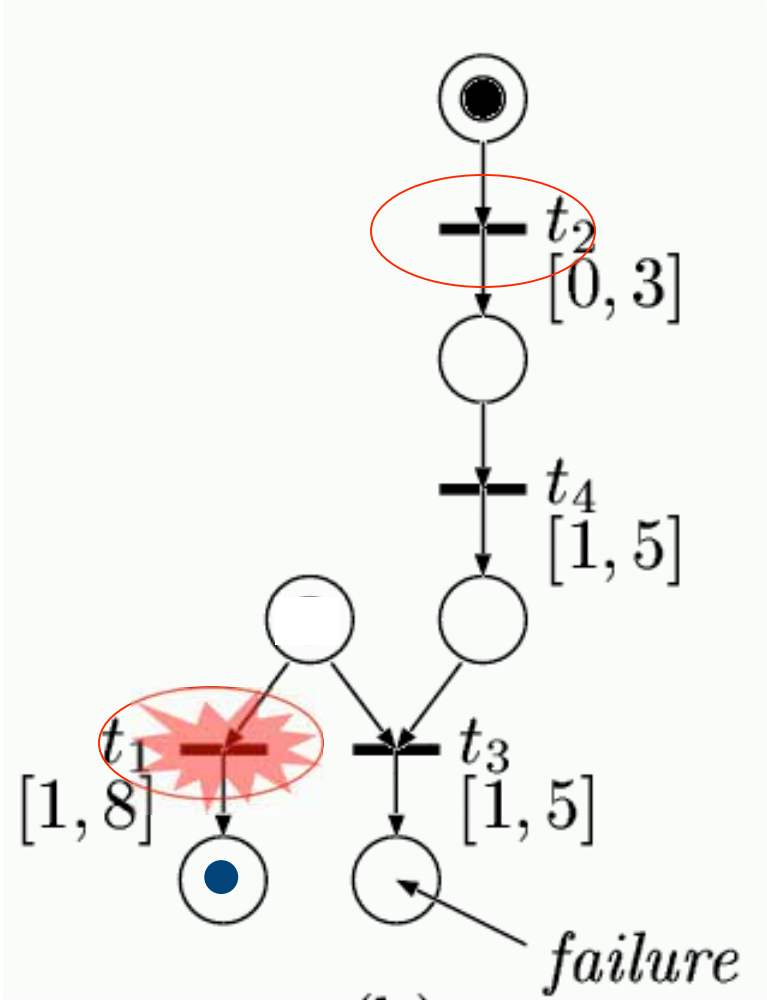
Partial Order Reduction (2)



Partial Order Reduction (3)

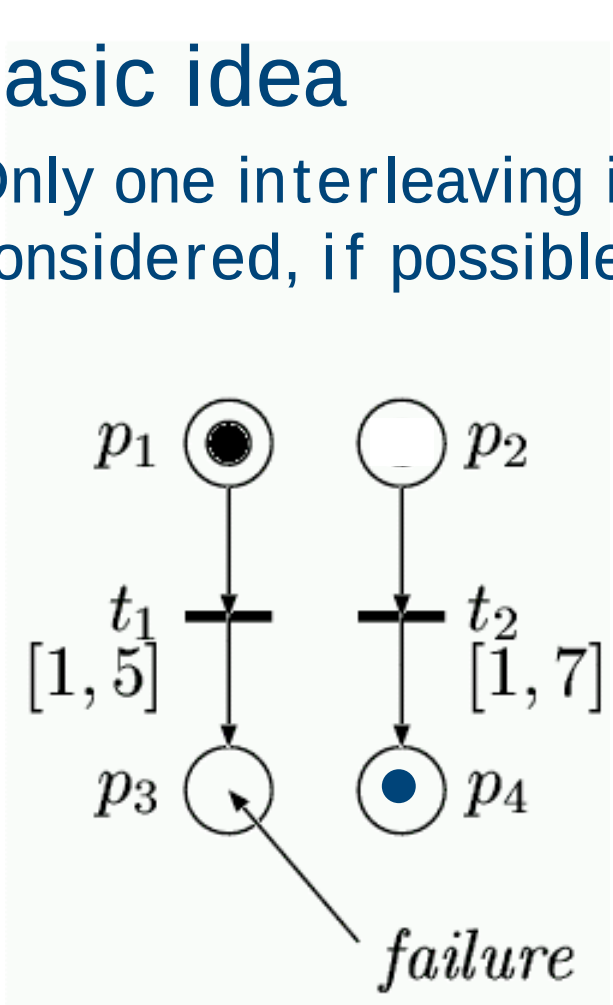
- Basic idea
  - Only one interleaving is considered, if possible

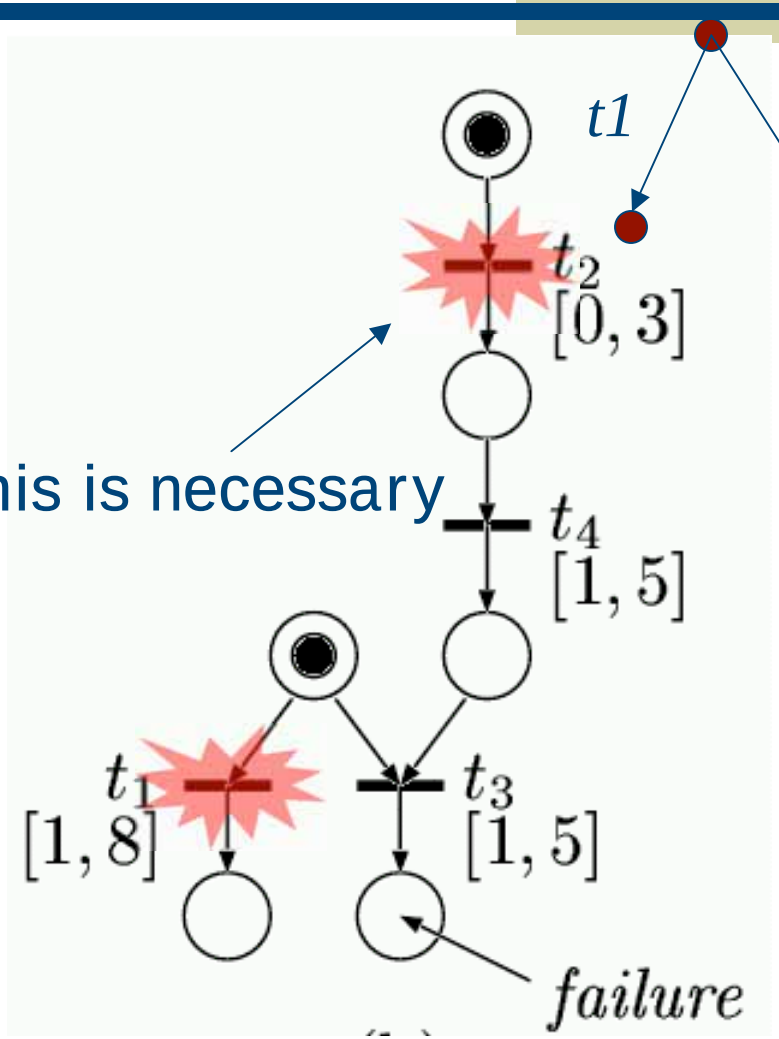




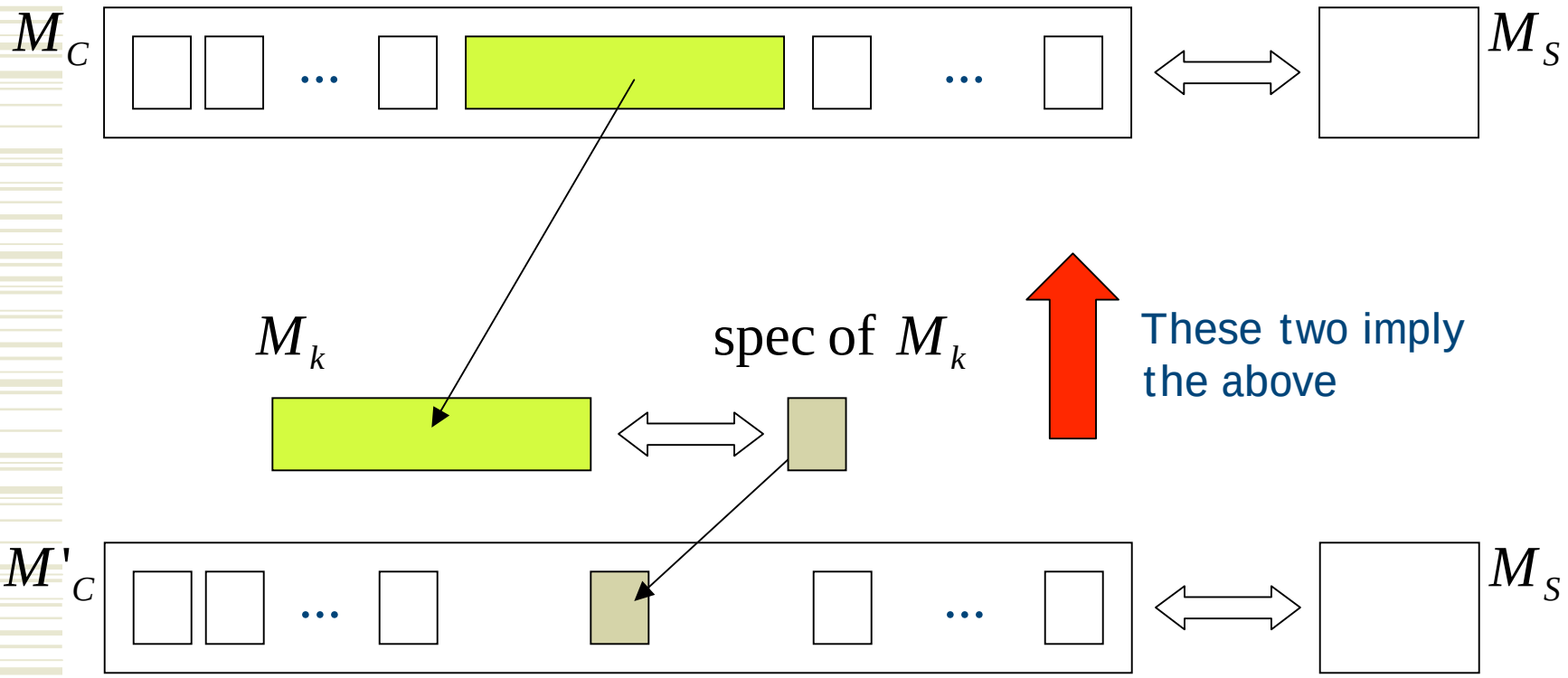
Partial Order Reduction (3)

- Basic idea
  - Only one interleaving is considered, if possible



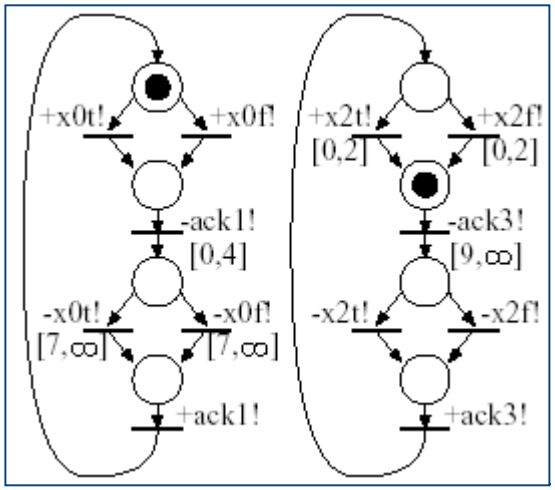


Hierarchical verification

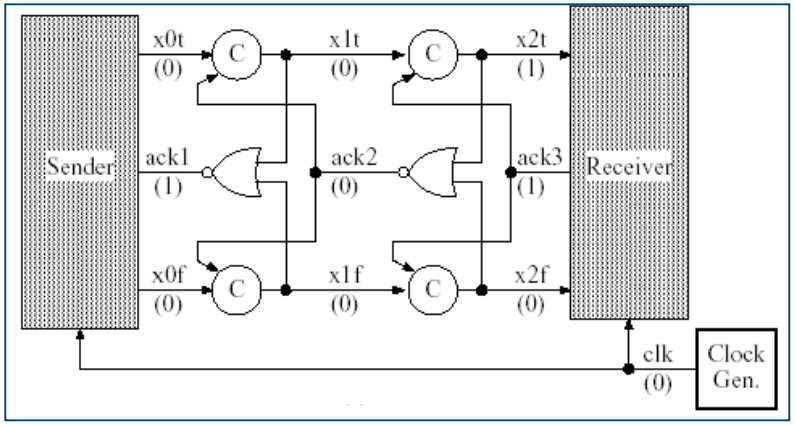


Experimental results (1)

- Verification of STARI circuits



verification

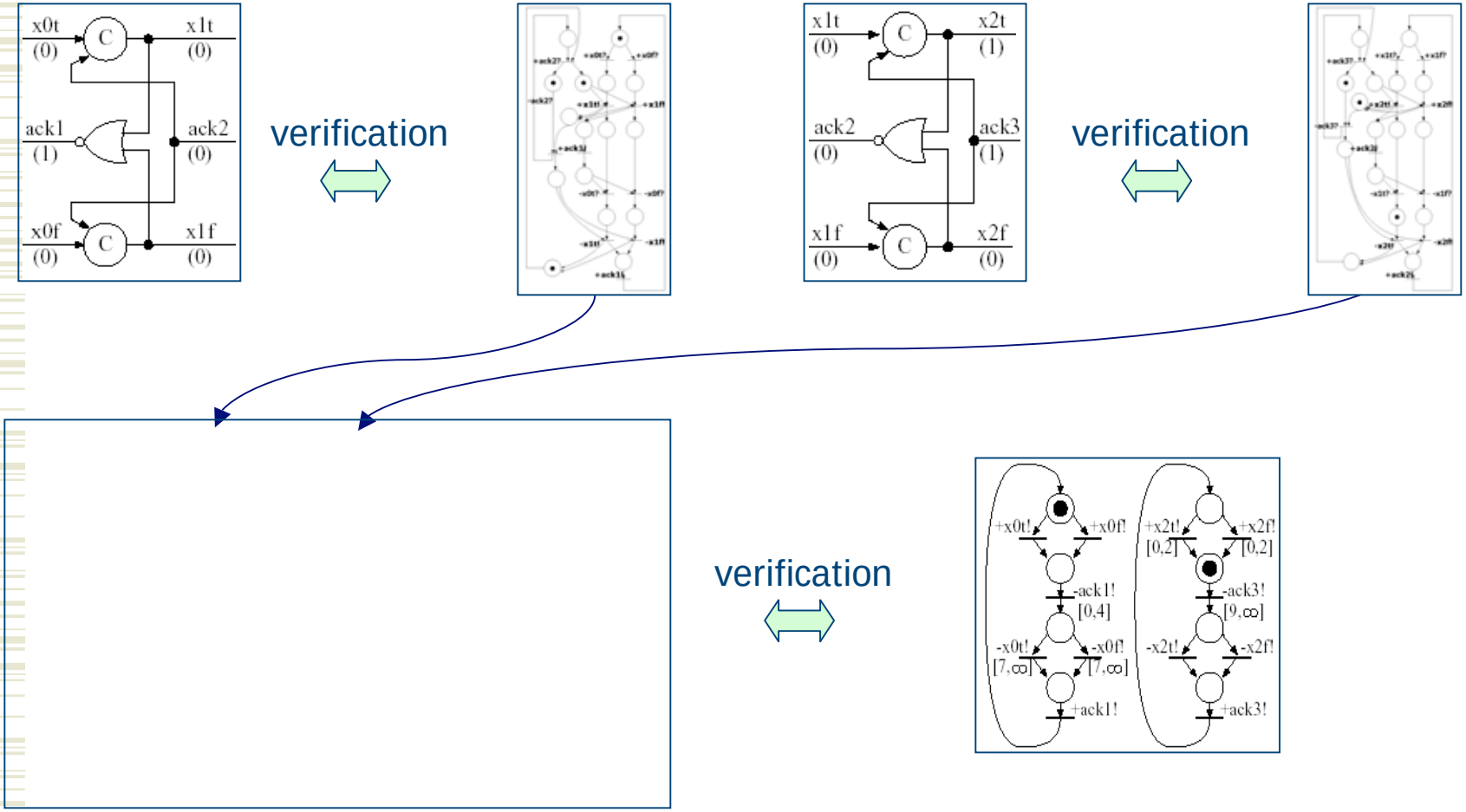


Spec. of STARI circuit

Two stage STARI circuit

Experimental results (1)

- Hierarchical verification



Experimental results (1)

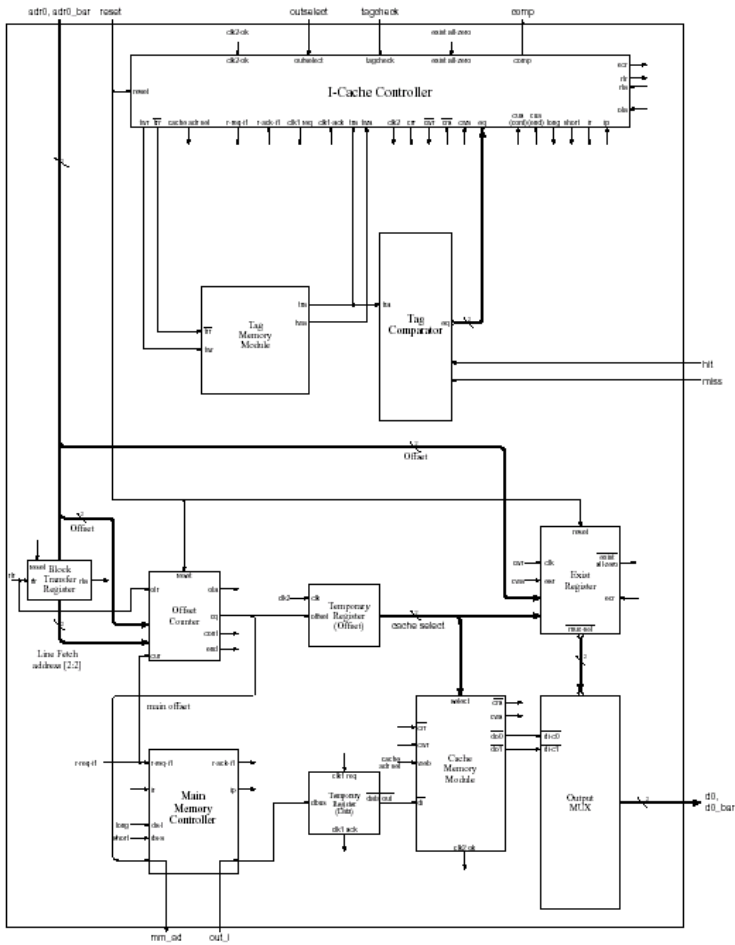
Total order vs Partial order

flat verification				
no. of stage	CPU time (sec.)		Memory(MB)	
	total	partial	total	partial
7	1057.93	0.20	144.98	0.91
8	2014.90	0.29	323.43	1.04
9	3650.61	0.35	604.72	1.27
10	4860.52	0.43	863.09	1.56
11	-	1.14	-	3.19

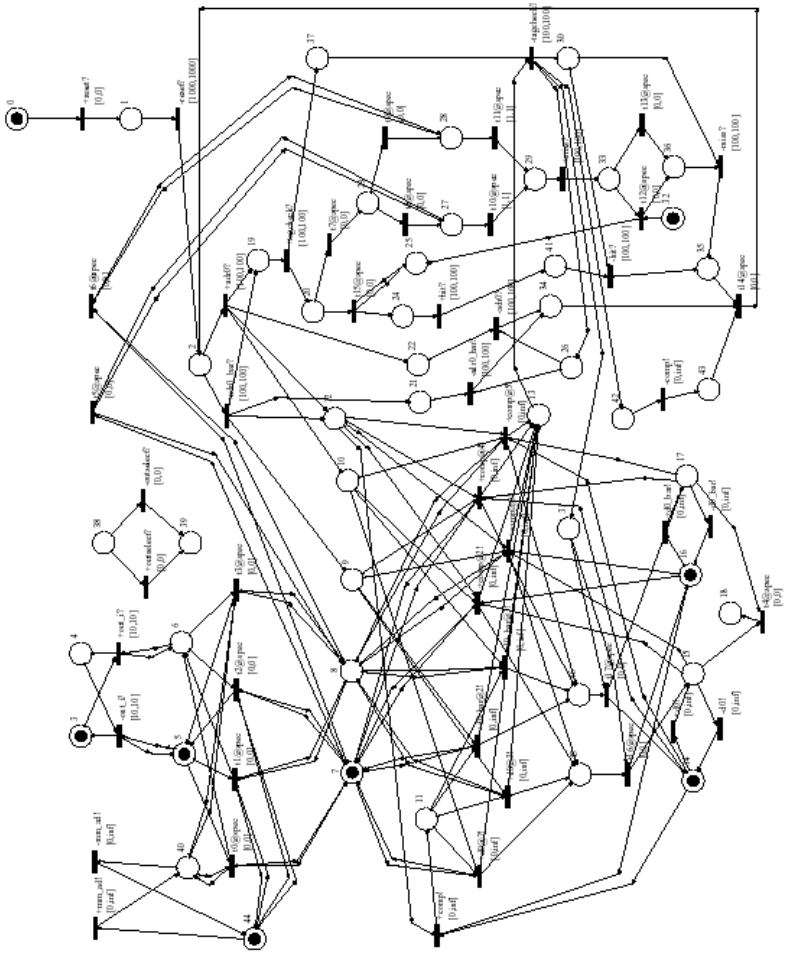
Flat vs Hierarchical

partial order method				
no. of stage	CPU time (sec.)		Memory(MB)	
	flat	hierarchical	flat	hierarchical
12	9.13	1.68	24.38	7.18
13	12.10	2.04	31.26	8.97
14	25.36	3.28	58.19	15.65
15	60.59	4.98	125.33	22.41
16	-	62.04	-	300.94

Experimental results (2)



verification

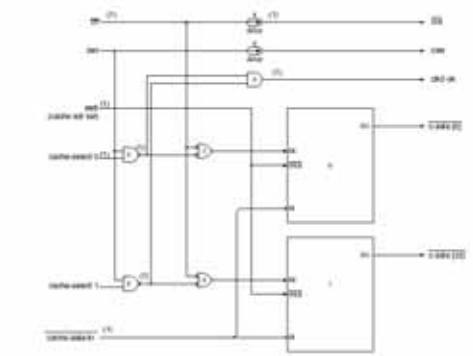


Abstracted Circuit of ICACHE

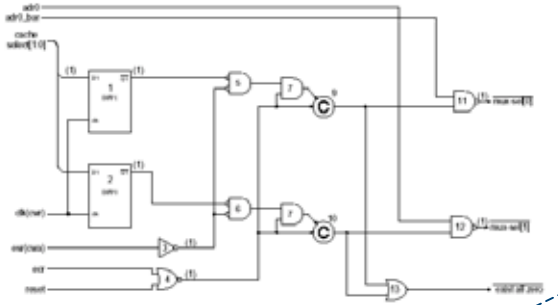
Spec. of ICACHE

Experimental results (2)

- low level

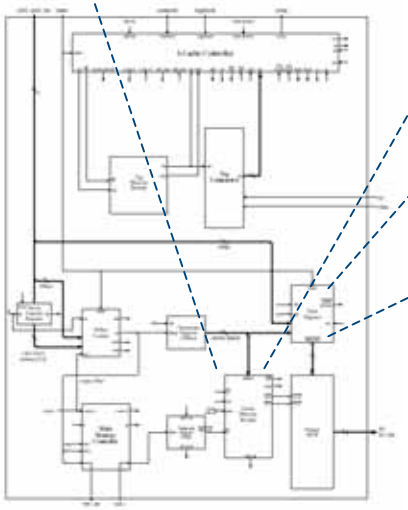


Cache Memory Module



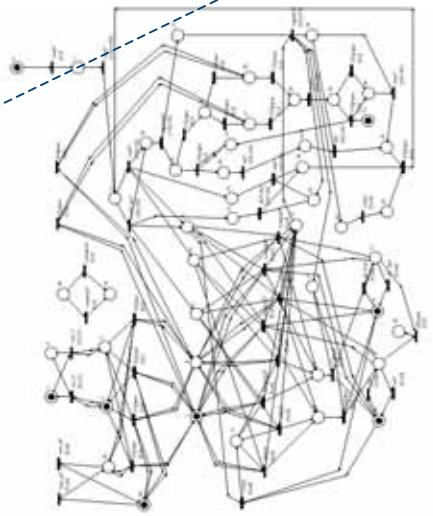
Exist Register

- upper level



Abstracted Circuit of ICACHE

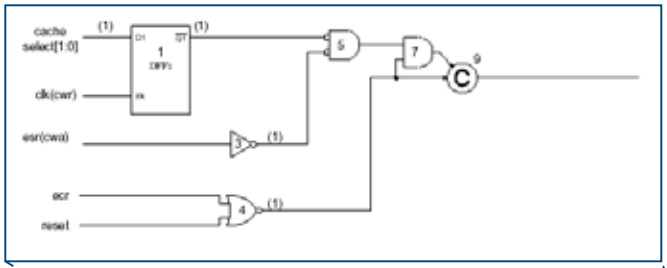
verification



Spec. of ICACHE

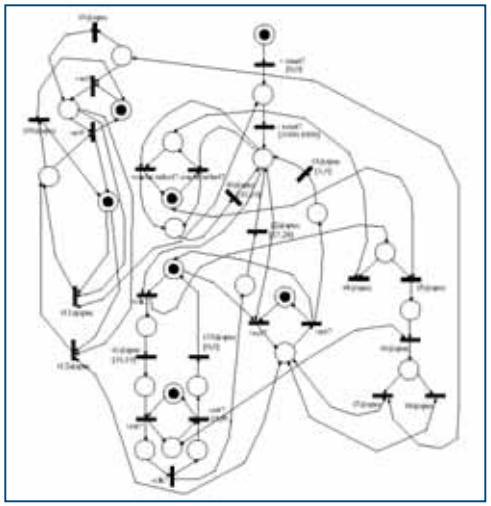
Experimental results (2)

- low level

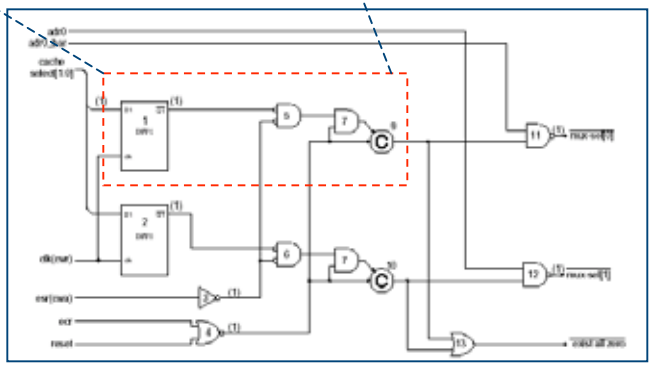


Subcircuit

verification



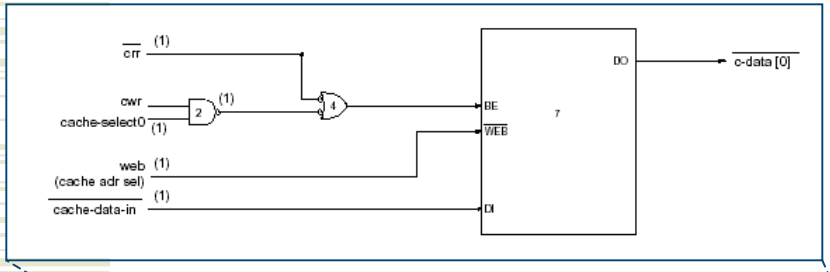
Subspec.



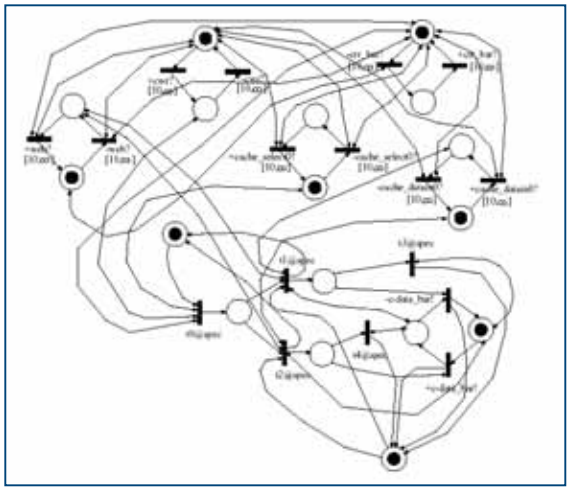
Exist Register

Experimental results (2)

- low level

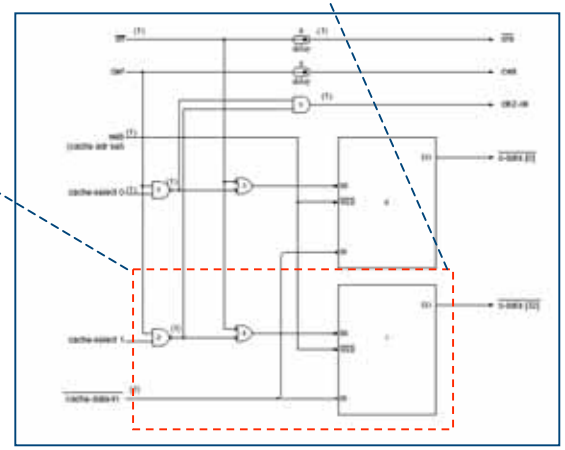


verification



Subcircuit

Subspec.



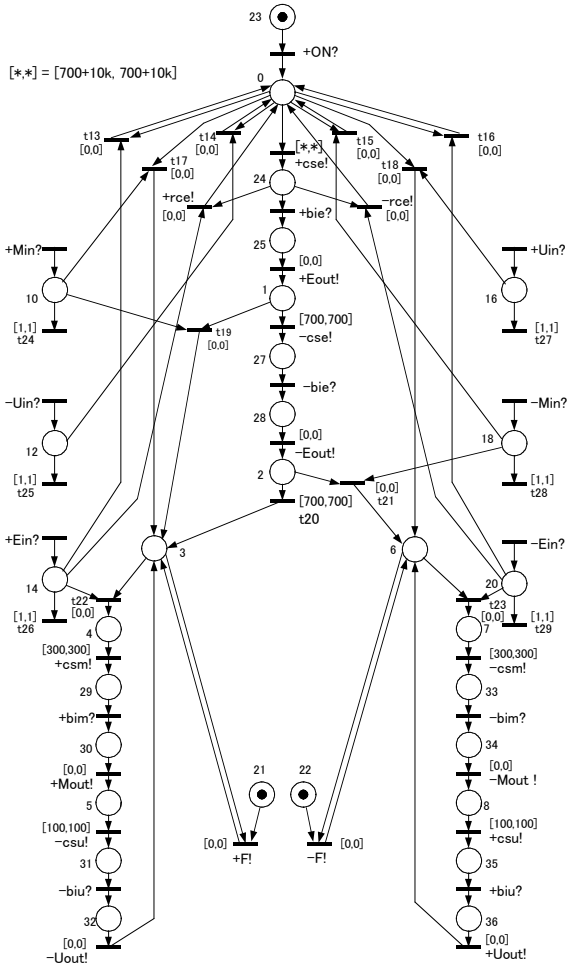
Cache Memory Module

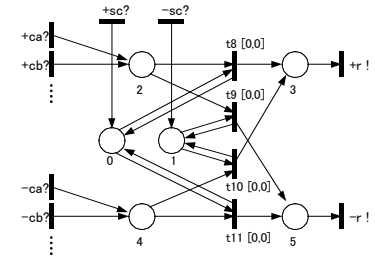
Experimental results (2)

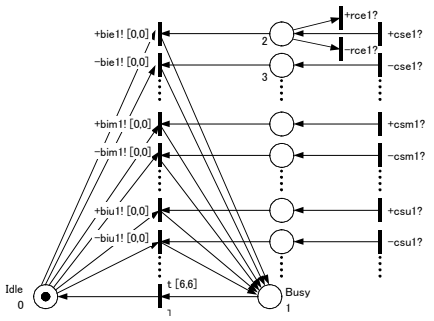
Verification of ICACHE				
Method	CPU time (sec.)		Memory(MB)	
	non-op.	op.	non-op.	op.
flat	12.50	5.98	8.15	3.98
Hierarchical	10.81	5.30	4.69	2.99

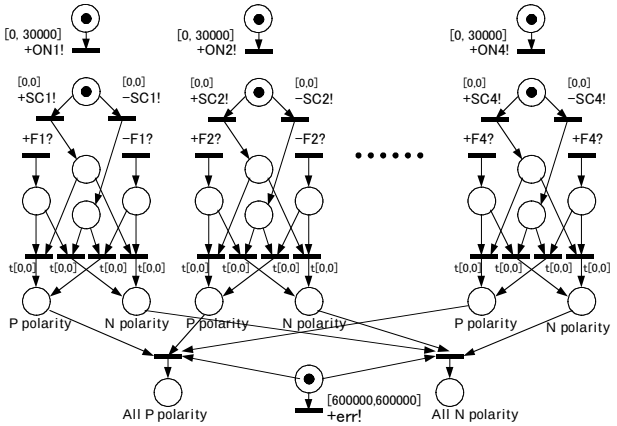
Experimental results (3)

- Distributed algorithm to initiate an air-conditioner network









No. of places: 354

No. of transitions: 569

No. of generated states: 361530

Verification time: 18 min.

Conclusion

- Formal verification of time dependent systems
- Approach
  - Timed extension of Conformance Checking
- Formal model
  - Time Petri nets
- Improvement
  - Partial Order Reduction
  - Hierarchical verification