京都大学
KYOTO UNIVERSITY

# Hyper Parametric Timed CTL

**Masaki Waga**[1] and Étienne André[2]

Kyoto University[1], Université Sorbonne Paris Nord[2]

EMSOFT 2024, 2nd Oct. 2024

# Safety Critical CPSs

## Study: Single Connected Car Can Trick Smart Traffic Lights Into Causing Intersection Clogging

## Waymo robotaxi accident with San Francisco cyclist draws regulatory review

By **Reuters**

February 9, 2024 5:35 AM GMT+9 · Updated 6 months ago


chigan have shown that
on systems can be
ehicle. Their research
spoofing strategy on one
n into believing that an
icle-to-infrastructure

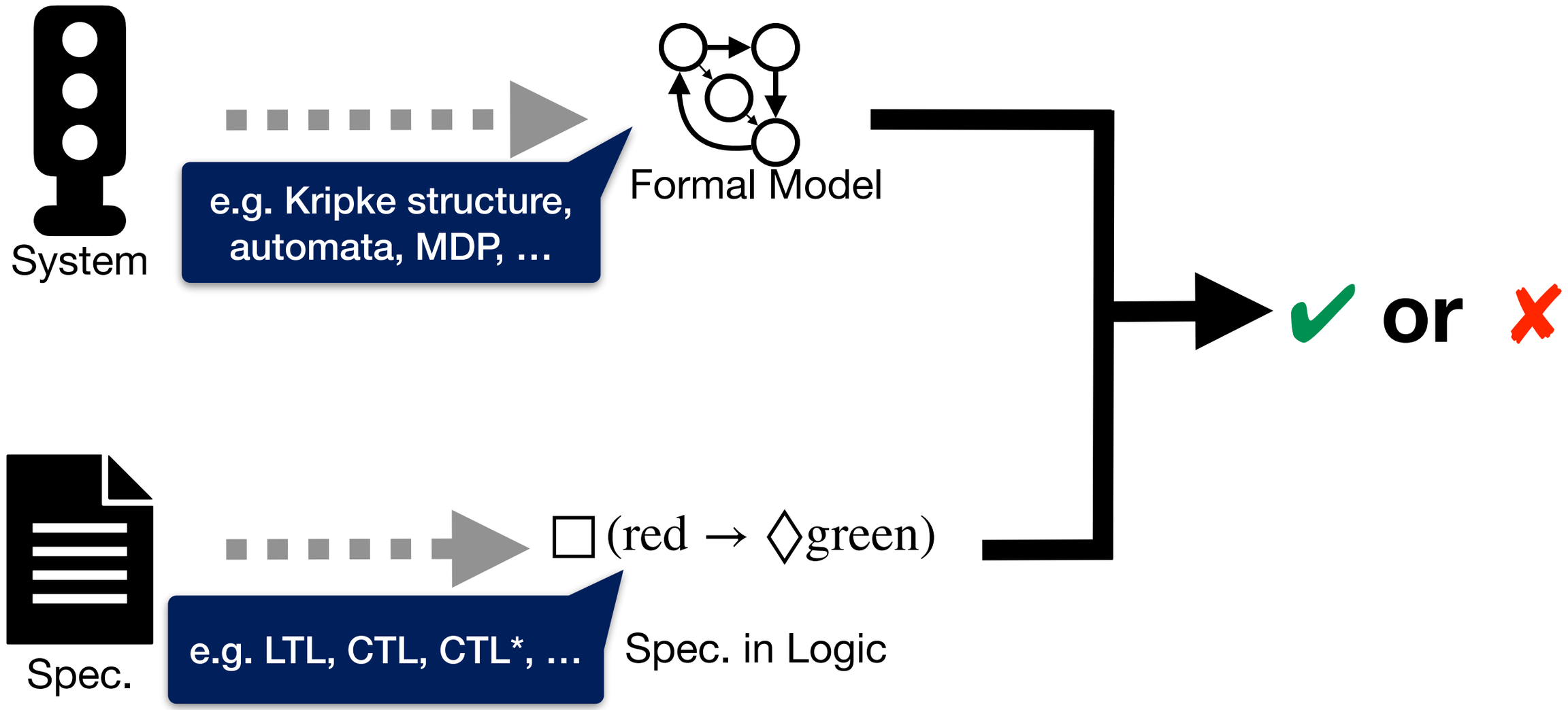
on that allows vehicles to share informatio
utomated toll collection systems, traffic ca


**Related Posts**

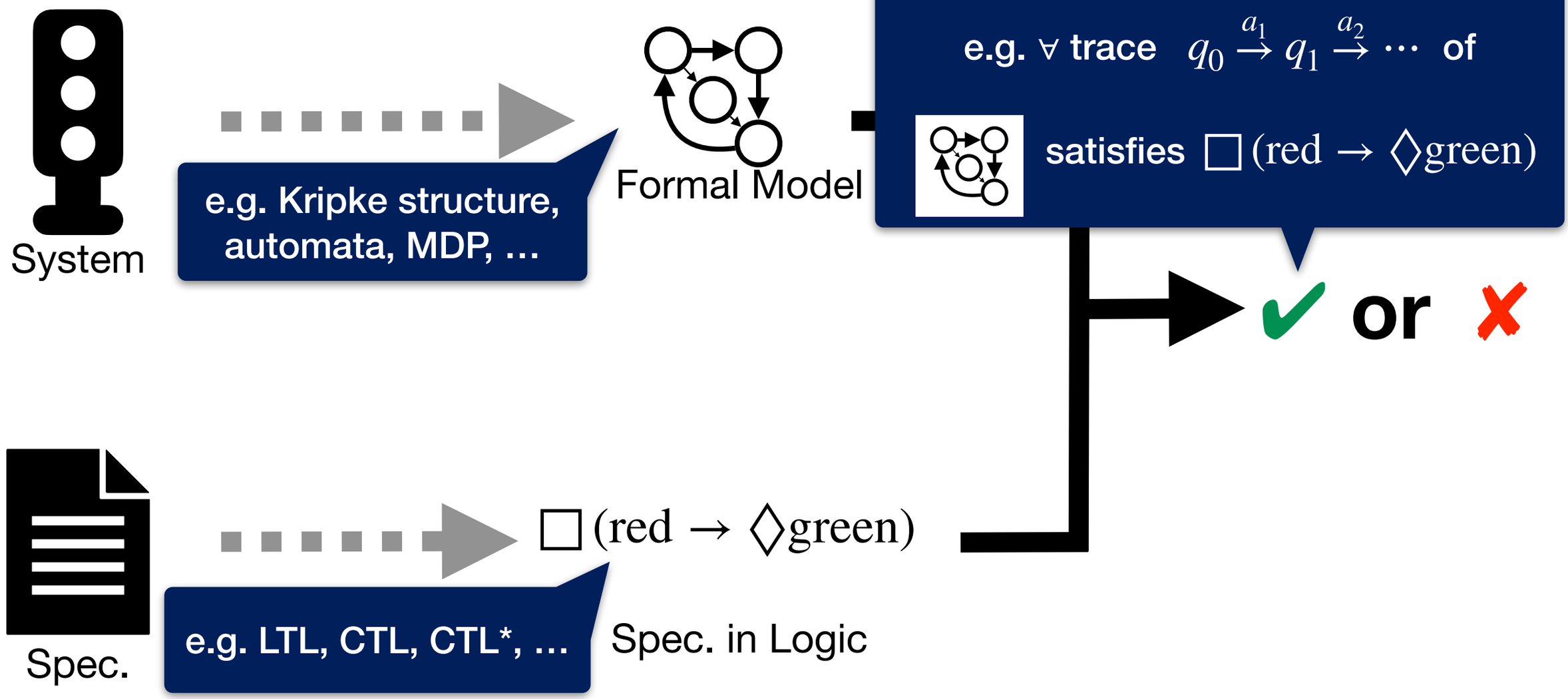
- Rising From the Underground: Hacktivism in 2024
- How to Secure Smart Home IoT Devices, Routers, and Smart Speakers
- Security for Entertainment IoT


https://www.reuters.com/world/us/driverless-waymo-car-hits-cyclist-san-francisco-causes-minor-scratches-2024-02-07/
https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/connected-car-can-trick-smart-traffic-lights-causing-intersection-clogging

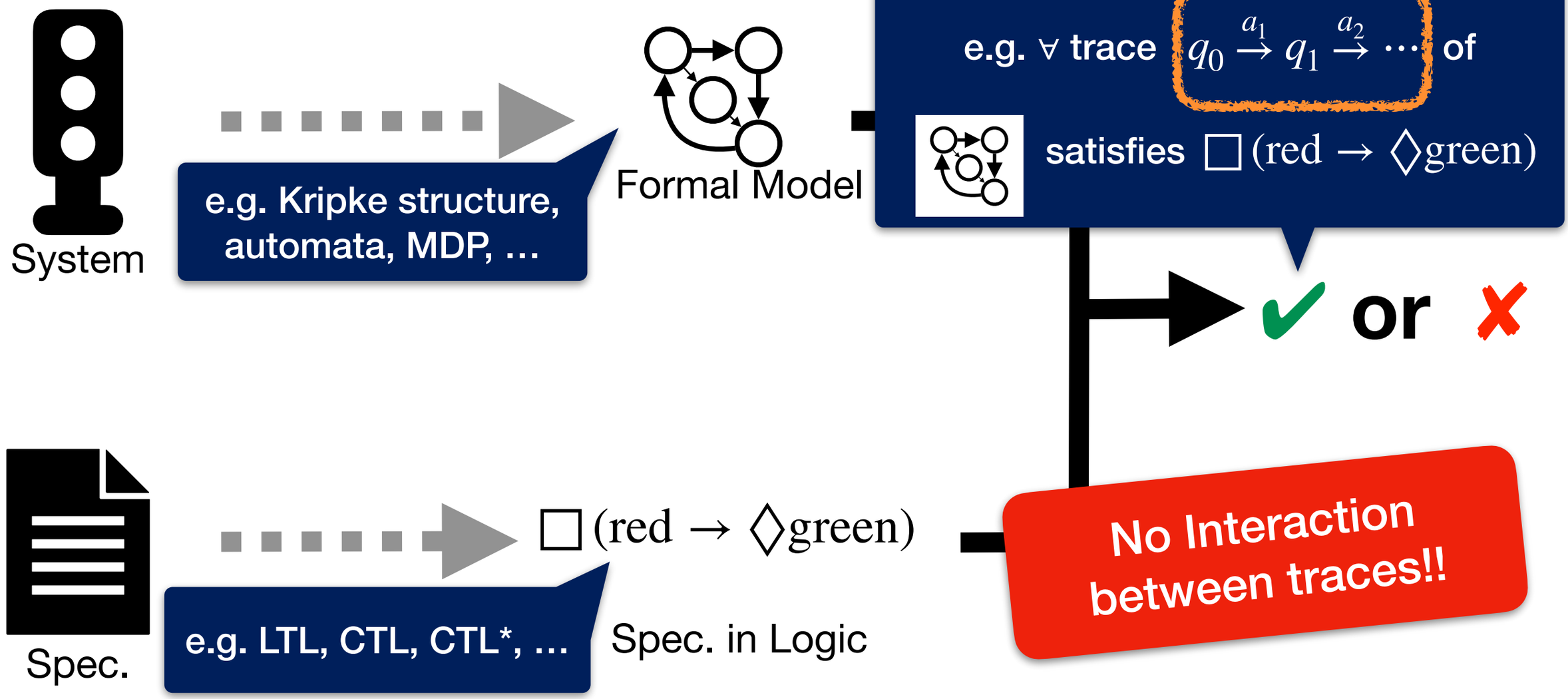
# Model Checking



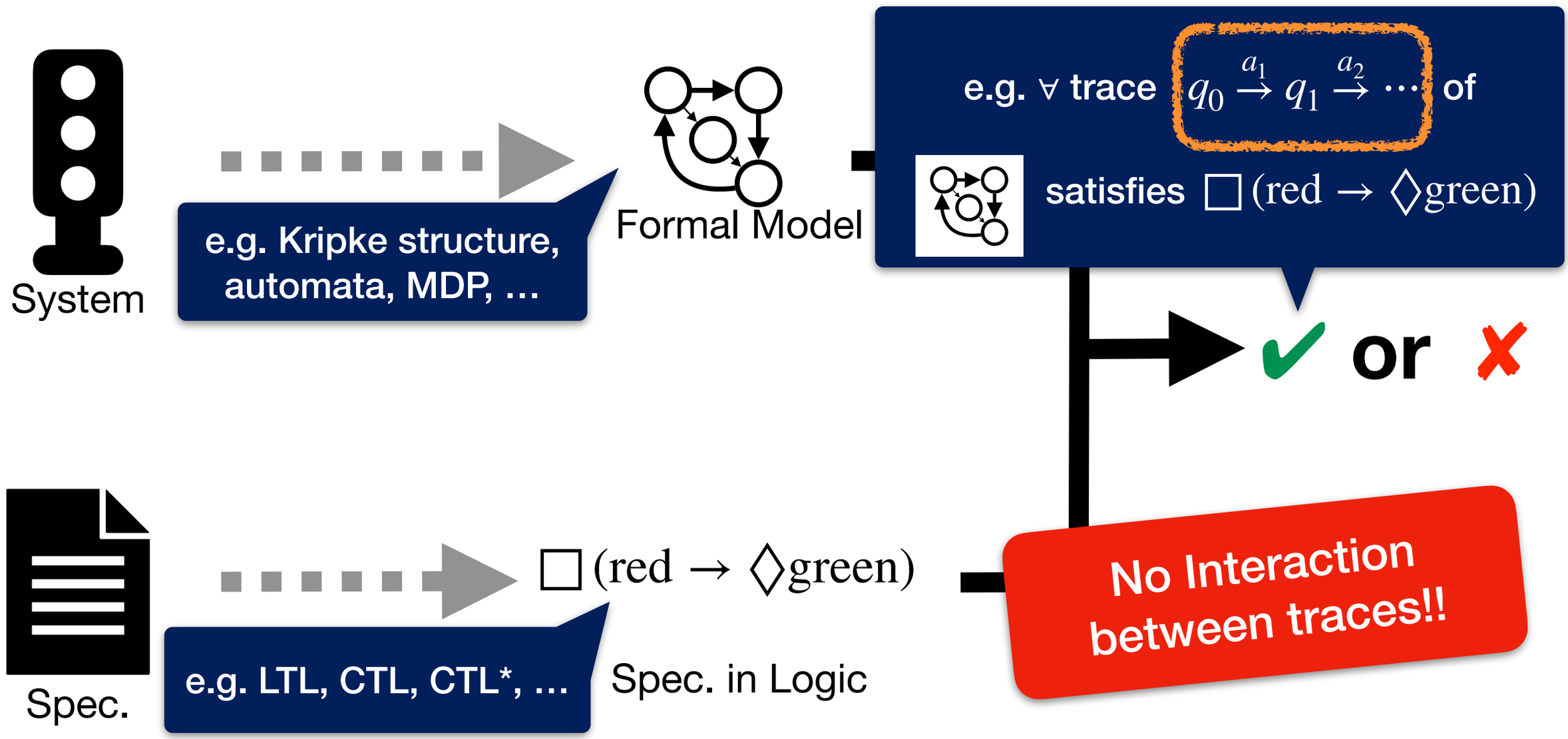
# Model Checking



# Model Checking



# Model Checking of Trace Properties



# Hyperproperties

[Clarkson & Schneider, J. Comput. Secur. 2010]

Properties addressing multiple independent traces

**Example (Observational determinism)**

For the same inputs, the outputs are the same

In other words…

(or $\forall \pi_1, \pi_2 \,.\, (\mathrm{Out}_{\pi_1} = \mathrm{Out}_{\pi_2}) \mathscr{W} (\mathrm{In}_{\pi_1} \neq \mathrm{In}_{\pi_2})$ in HyperLTL)

# Hyperproperties

[Clarkson & Schneider, J. Comput. Secur. 2010]

Properties addressing multiple independent traces

**Example (Observational determinism)**

For the same inputs, the outputs are the same

In other words…

$$\forall \quad q_0 \xrightarrow{in_1/out_1} q_1 \xrightarrow{in_2/out_2} q_3 \xrightarrow{in_3/out_3} \cdots$$

$$q'_0 \xrightarrow{in'_1/out'_1} q'_1 \xrightarrow{in'_2/out'_2} q'_3 \xrightarrow{in'_3/out'_3} \cdots$$

(or $\forall \pi_1, \pi_2 \,.\, (\mathrm{Out}_{\pi_1} = \mathrm{Out}_{\pi_2}) \mathscr{W} (\mathrm{In}_{\pi_1} \neq \mathrm{In}_{\pi_2})$ in HyperLTL)

# Hyperproperties

[Clarkson & Schneider, J. Comput. Secur. 2010]

Properties addressing multiple independent traces

**Example (Observational determinism)**

For the same inputs, the outputs are the same

In other words…

$$\forall \quad q_0 \xrightarrow{in_1/out_1} q_1 \xrightarrow{in_2/out_2} q_3 \xrightarrow{in_3/out_3} \cdots$$

same input

$$q_0' \xrightarrow{in_1'/out_1'} q_1' \xrightarrow{in_2'/out_2'} q_3' \xrightarrow{in_3'/out_3'} \cdots$$

(or $\forall \pi_1, \pi_2 \,.\, (\mathrm{Out}_{\pi_1} = \mathrm{Out}_{\pi_2}) \mathscr{W} (\mathrm{In}_{\pi_1} \neq \mathrm{In}_{\pi_2})$ in HyperLTL)

# Hyperproperties

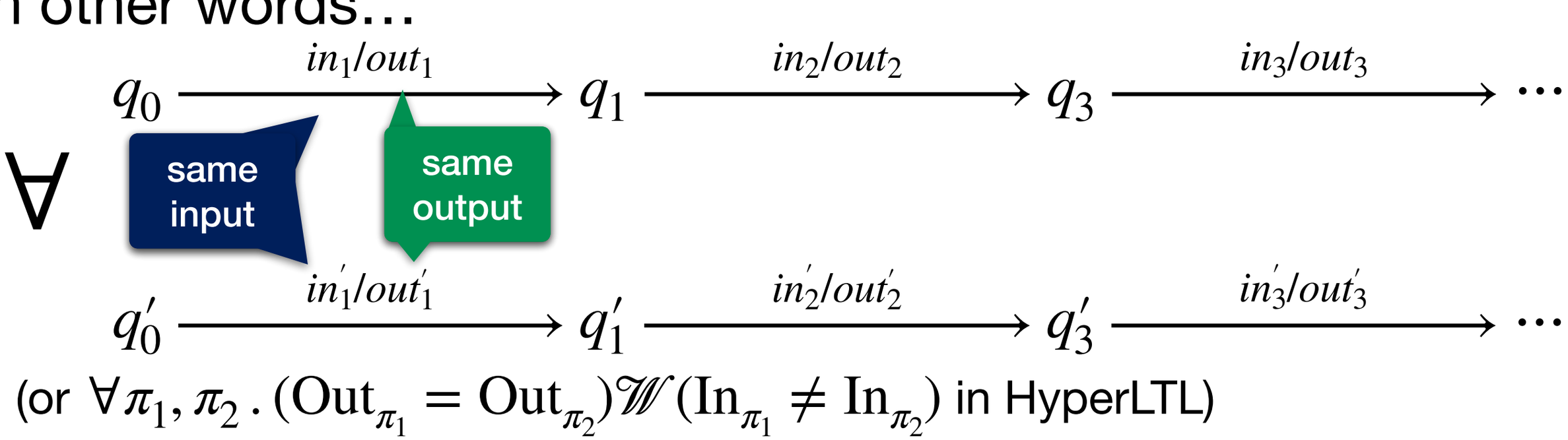
[Clarkson & Schneider, J. Comput. Secur. 2010]

Properties addressing multiple independent traces

**Example (Observational determinism)**

For the same inputs, the outputs are the same

In other words…




(or $\forall \pi_1, \pi_2 \,.\, (\mathrm{Out}_{\pi_1} = \mathrm{Out}_{\pi_2}) \mathscr{W} (\mathrm{In}_{\pi_1} \neq \mathrm{In}_{\pi_2})$ in HyperLTL)

# Hyperproperties

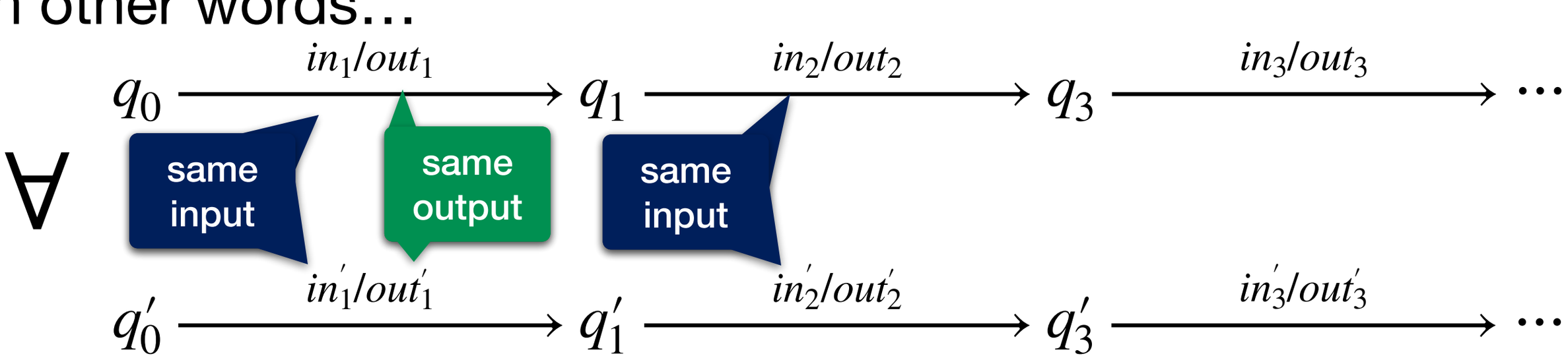
[Clarkson & Schneider, J. Comput. Secur. 2010]

Properties addressing multiple independent traces

**Example (Observational determinism)**

For the same inputs, the outputs are the same

In other words…




(or $\forall \pi_1, \pi_2 \,.\, (\mathrm{Out}_{\pi_1} = \mathrm{Out}_{\pi_2}) \mathscr{W} (\mathrm{In}_{\pi_1} \neq \mathrm{In}_{\pi_2})$ in HyperLTL)

# Hyperproperties

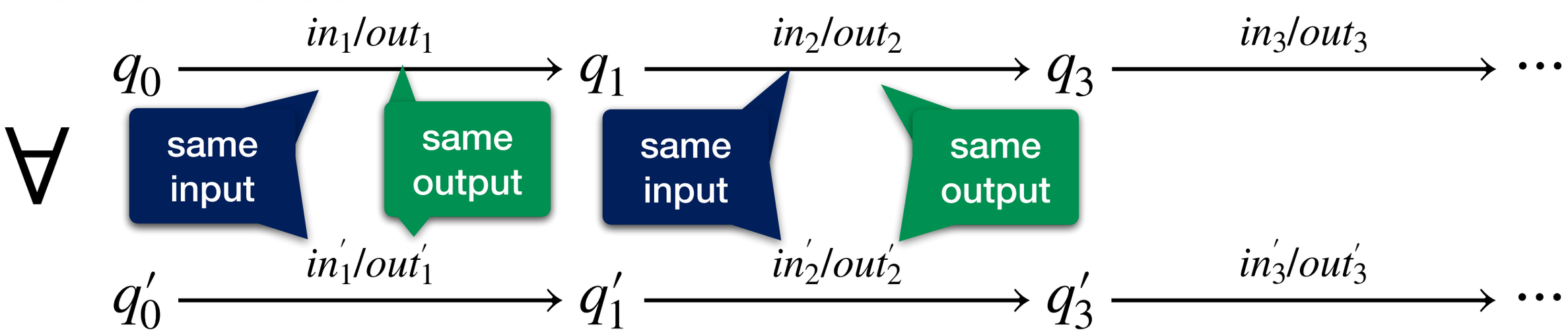
[Clarkson & Schneider, J. Comput. Secur. 2010]

Properties addressing multiple independent traces

**Example (Observational determinism)**

For the same inputs, the outputs are the same

In other words…




(or $\forall \pi_1, \pi_2 . (\mathrm{Out}_{\pi_1} = \mathrm{Out}_{\pi_2}) \mathscr{W} (\mathrm{In}_{\pi_1} \neq \mathrm{In}_{\pi_2})$ in HyperLTL)

# Hyperproperties

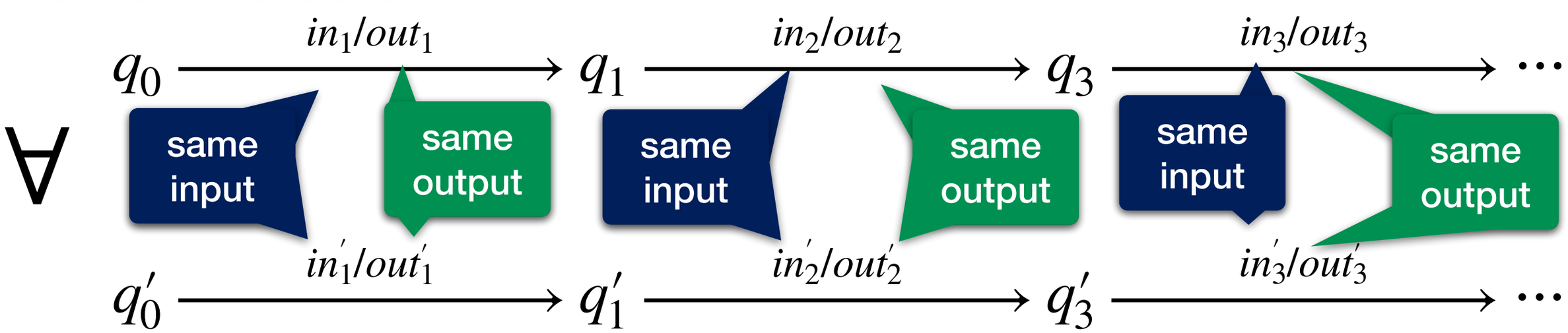
[Clarkson & Schneider, J. Comput. Secur. 2010]

Properties addressing multiple independent traces

**Example (Observational determinism)**

For the same inputs, the outputs are the same

In other words…




(or $\forall \pi_1, \pi_2 . (\mathrm{Out}_{\pi_1} = \mathrm{Out}_{\pi_2}) \mathscr{W} (\mathrm{In}_{\pi_1} \neq \mathrm{In}_{\pi_2})$ in HyperLTL)

# Hyperproperties

[Clarkson & Schneider, J. Comput. Secur. 2010]

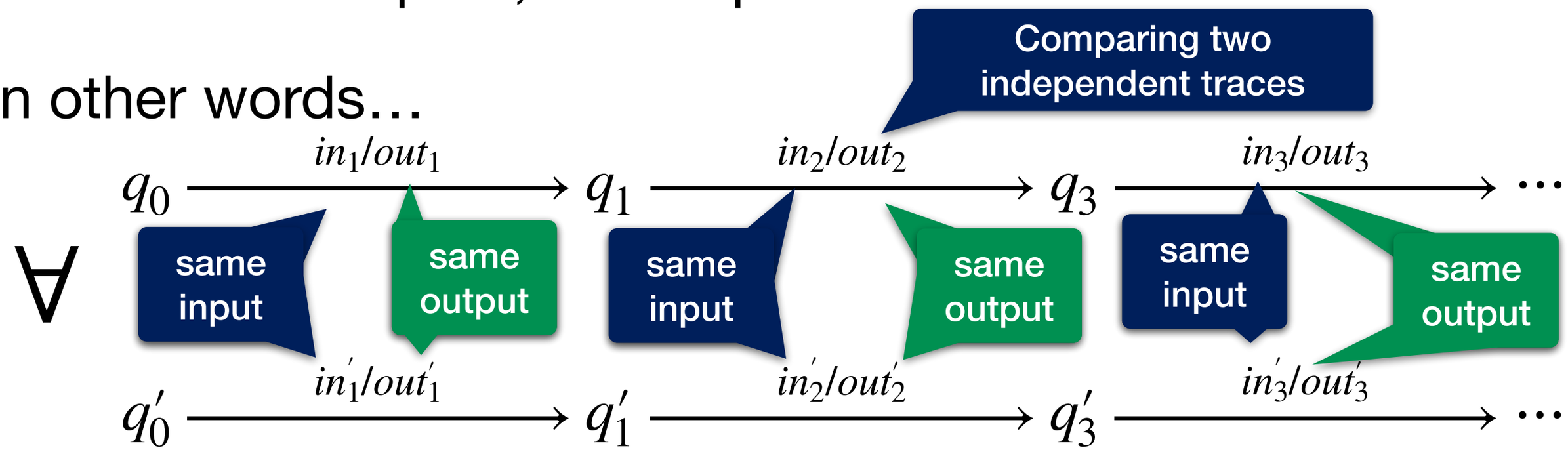
Properties addressing multiple independent traces

**Example (Observational determinism)**

For the same inputs, the outputs are the same

In other words…

Comparing two independent traces




(or $\forall \pi_1, \pi_2 \,.\, (\mathrm{Out}_{\pi_1} = \mathrm{Out}_{\pi_2}) \mathscr{W} (\mathrm{In}_{\pi_1} \neq \mathrm{In}_{\pi_2})$ in HyperLTL)

# Hyperproperties

[Clarkson & Schneider, J. Comput. Secur. 2010]

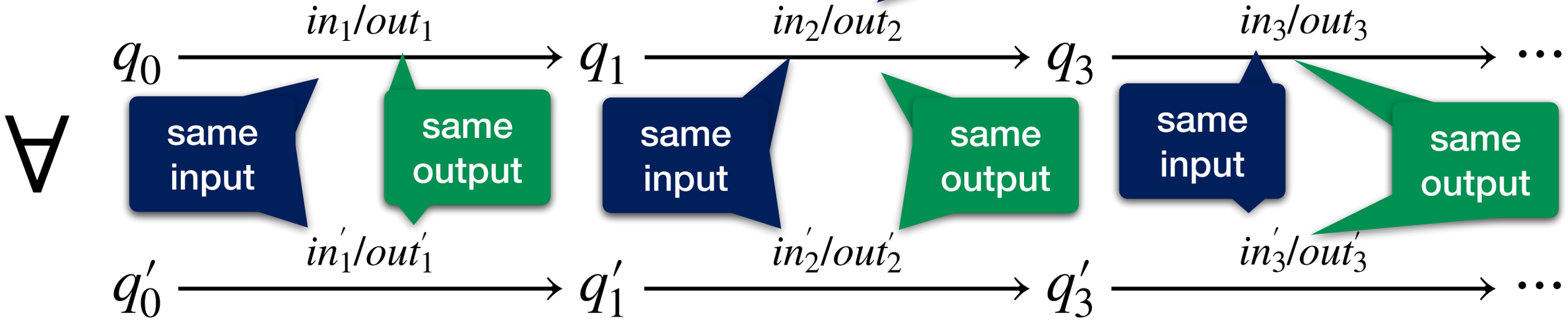
Properties addressing multiple independent traces

**Example (Observational determinism)**

For the same inputs, the outputs are the same

In other words…

Comparing two independent traces




(or $\forall \pi_1, \pi_2 \,.\, (\mathrm{Out}_{\pi_1} = \mathrm{Out}_{\pi_2}) \mathscr{W} (\mathrm{In}_{\pi_1} \neq \mathrm{In}_{\pi_2})$ in HyperLTL)

Useful for Security, Fairness, Robustness, …

# Q. Can we model check timed hyperproperties?

w/ explicit timing constraints, continuous notion of time, …

# (Ext-)Hyper Parametric TCTL

[Contribution]

Timed & Parametric Extension of HyperCTL + Additional Predicates

**Example (Parametric timed observational determinism)**
Observational determinism with small timing deviation of outputs

In other words…

# (Ext-)Hyper Parametric TCTL

[Contribution]

Timed & Parametric Extension of HyperCTL + Additional Predicates

**Example (Parametric timed observational determinism)**

Observational determinism with small timing deviation of outputs

In other words…

# (Ext-)Hyper Parametric TCTL

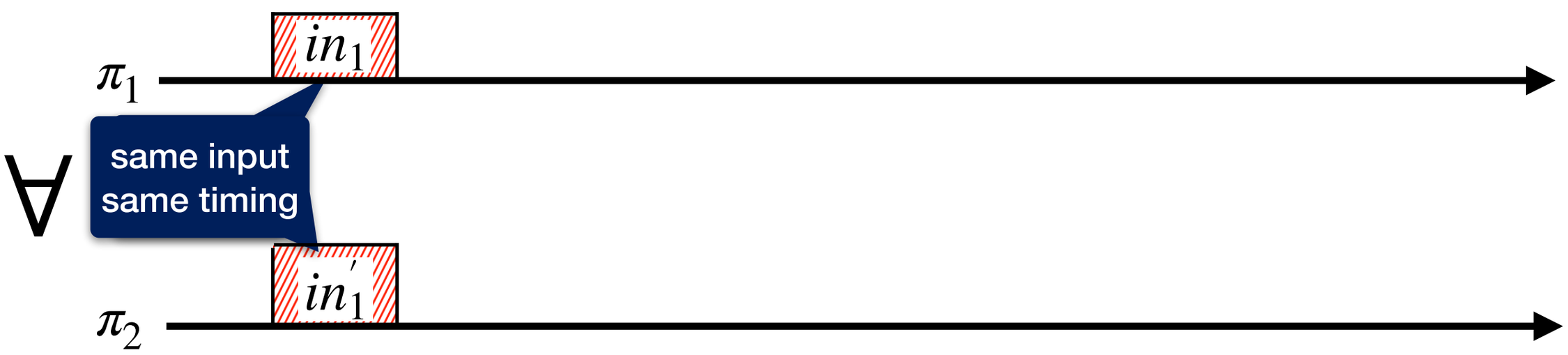
[Contribution]

Timed & Parametric Extension of HyperCTL + Additional Predicates

**Example (Parametric timed observational determinism)**

Observational determinism with small timing deviation of outputs

In other words…



# (Ext-)Hyper Parametric TCTL

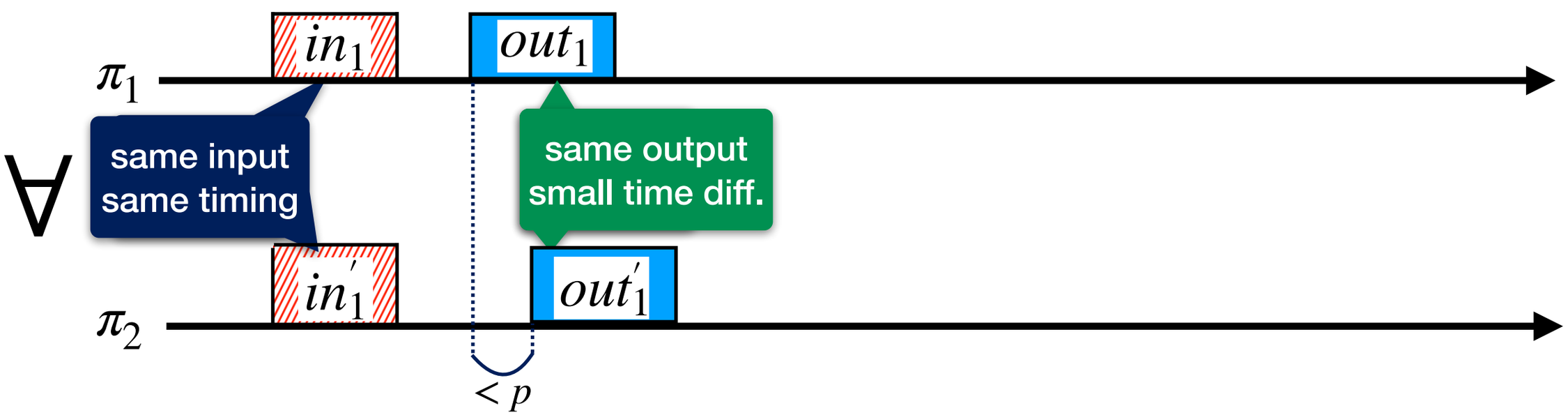
[Contribution]

Timed & Parametric Extension of HyperCTL + Additional Predicates

**Example (Parametric timed observational determinism)**

Observational determinism with small timing deviation of outputs

In other words…



# (Ext-)Hyper Parametric TCTL

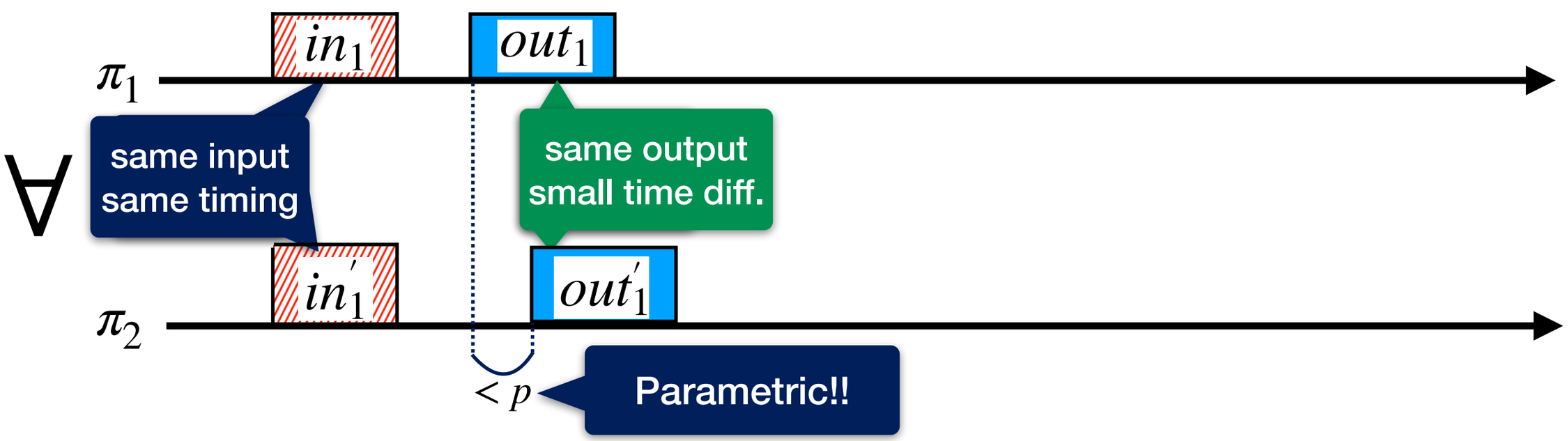
[Contribution]

Timed & Parametric Extension of HyperCTL + Additional Predicates

**Example (Parametric timed observational determinism)**

Observational determinism with small timing deviation of outputs

In other words…



# (Ext-)Hyper Parametric TCTL

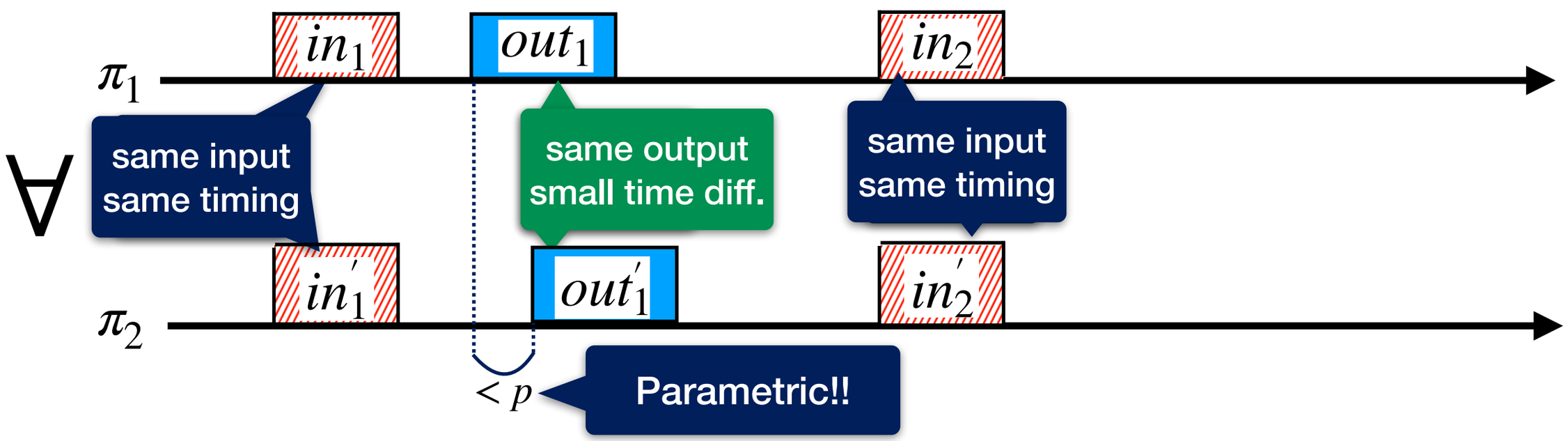
[Contribution]

Timed & Parametric Extension of HyperCTL + Additional Predicates

**Example (Parametric timed observational determinism)**

Observational determinism with small timing deviation of outputs

In other words…



# (Ext-)Hyper Parametric TCTL

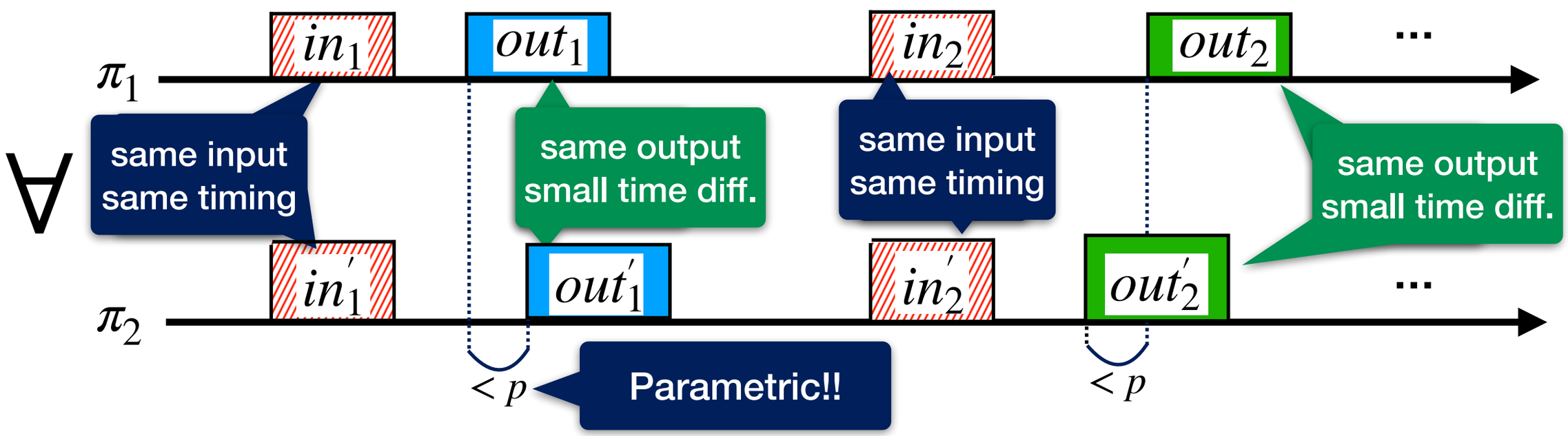
[Contribution]

Timed & Parametric Extension of HyperCTL + Additional Predicates

**Example (Parametric timed observational determinism)**

Observational determinism with small timing deviation of outputs

In other words…



# Ext-Hyper Parametric TCTL

[Henzinger et al., IaC 1994]

Branching + temporal + timing constraints

For any path

is not reachable

$$\varphi = \forall G_{[0,5)} \neg$$

within 5 time units

# Ext-Hyper **Parametric TCTL**

[Bruyère et al., TOCL 2008]

TCTL + parameters in timing constraints

For any path

is not reachable

$$\varphi = \forall G_{[0,p)} \neg$$

within $p$ time units

# Ext-Hyper Parametric TCTL

[Contribution]

PTCTL + multiple traces

$$\varphi = \forall \pi_1, \pi_2 (\pi_1 = \pi_2) \mathscr{W}_{[0,p)} (\pi_1 \neq \pi_2)$$

# Ext-Hyper Parametric TCTL

[Contribution]

PTCTL + multiple traces

For any paths $\pi_1, \pi_2$

$$\varphi = \forall \pi_1, \pi_2 (\ \pi_1 = \ \pi_2) \mathscr{W}_{[0,p)} (\ \pi_1 \neq \ \pi_2)$$

# Ext-Hyper Parametric TCTL

[Contribution]

PTCTL + multiple traces

For any paths $\pi_1, \pi_2$

$$\varphi = \forall \pi_1, \pi_2 ( \underset{\pi_1}{\text{🚦}} = \underset{\pi_2}{\text{🚦}} ) \mathscr{W}_{[0,p)} ( \underset{\pi_1}{\text{🚗}} \neq \underset{\pi_2}{\text{🚗}} )$$

Timing of 🚦 is same in $\pi_1$ and $\pi_2$

# Ext-Hyper Parametric TCTL

[Contribution]

PTCTL + multiple traces

For any paths $\pi_1, \pi_2$

Timing of  is different in $\pi_1$ and $\pi_2$

$$\varphi = \forall \pi_1, \pi_2 ( \pi_1 = \pi_2 ) \mathscr{W}_{[0,p)} ( \pi_1 \neq \pi_2 )$$

Timing of  is same in $\pi_1$ and $\pi_2$

# Ext-Hyper Parametric TCTL

[Contribution]

HyperPTCTL + additional predicates (# and $Last$)

$$\varphi = \forall \pi_1, \pi_2 (\#\,\pi_1 = \#\,\pi_2 \Rightarrow |\,Last(\pi_1) - Last(\pi_2)\,| < p)$$

$$\mathscr{W}_{[0,p)}(\,\pi_1 \neq \,\pi_2)$$

# Ext-Hyper Parametric TCTL

[Contribution]

HyperPTCTL + additional predicates (# and $Last$)

For any paths $\pi_1, \pi_2$

$$\varphi = \forall \pi_1, \pi_2 (\#\,\pi_1 = \#\,\pi_2 \Rightarrow |Last(\pi_1) - Last(\pi_2)| < p)$$

$$\mathscr{W}_{[0,p)}(\pi_1 \neq \pi_2)$$

# Ext-Hyper Parametric TCTL

[Contribution]

HyperPTCTL + additional predicates (# and $Last$)

For any paths $\pi_1, \pi_2$

Timing of last  is similar in $\pi_1$ and $\pi_2$

$$\varphi = \forall \pi_1, \pi_2 (\# \text{  }_{\pi_1} = \# \text{  }_{\pi_2} \Rightarrow |Last(\text{  }_{\pi_1}) - Last(\text{  }_{\pi_2})| < p)$$

$$\mathscr{W}_{[0,p)}(\text{  }_{\pi_1} \neq \text{  }_{\pi_2})$$

# Ext-Hyper Parametric TCTL

[Contribution]

HyperPTCTL + additional predicates (# and $Last$)

For any paths $\pi_1, \pi_2$

Timing of last  is similar in $\pi_1$ and $\pi_2$

$$\varphi = \forall \pi_1, \pi_2 (\#\ \pi_1 = \#\ \pi_2 \Rightarrow |Last(\ \pi_1) - Last(\ \pi_2)| < p)$$

$$\mathscr{W}_{[0,p)}(\ \pi_1 \neq\ \pi_2)$$

Timing of  is different in $\pi_1$ and $\pi_2$

# Ext-HyperPTCTL Model Checking

[Contribution]

Idea: Reduction to PTCTL model checking

1. Ext-HyperPTCTL→HyperPTCTL: encode w/ PTAs
2. HyperPTCTL → PTCTL: self-composition of PTAs

**Note**: PTCTL model checking is in general undecidable
→ We only have semi-algorithm

# Ext-HyperPTCTL → HyperPTCTL

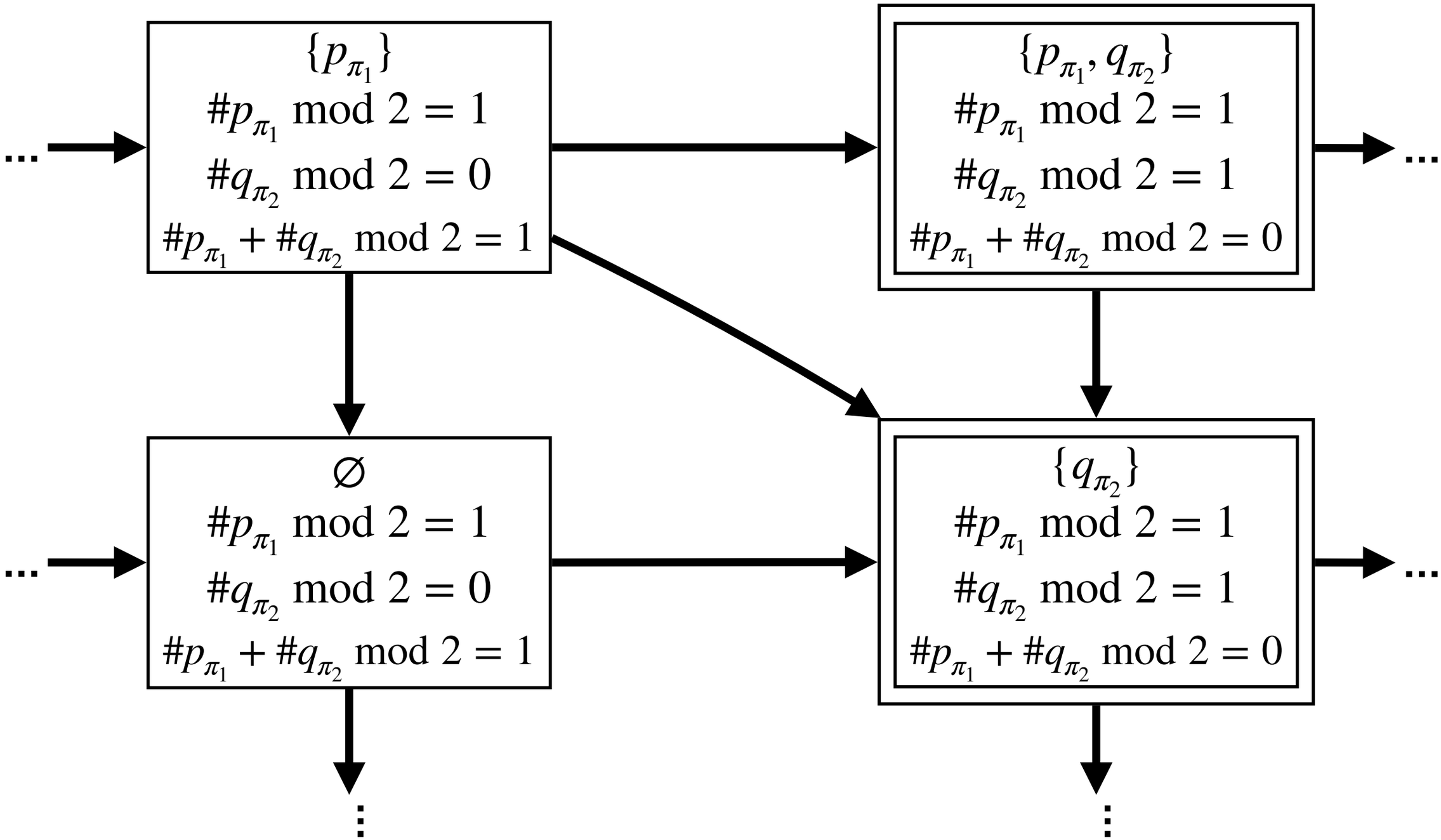
Encode extended predicates w/ observer PTAs

Encoding of general terms with PTAs is hard, but possible for some forms of terms

**Slogan**: Restrict the terms so that:

- Predicates' truth values are updated only at transitions
- Only finite (discrete) counting is sufficient

# Example: $\#p_{\pi_1} + \#q_{\pi_2} \bmod 2 = 0$

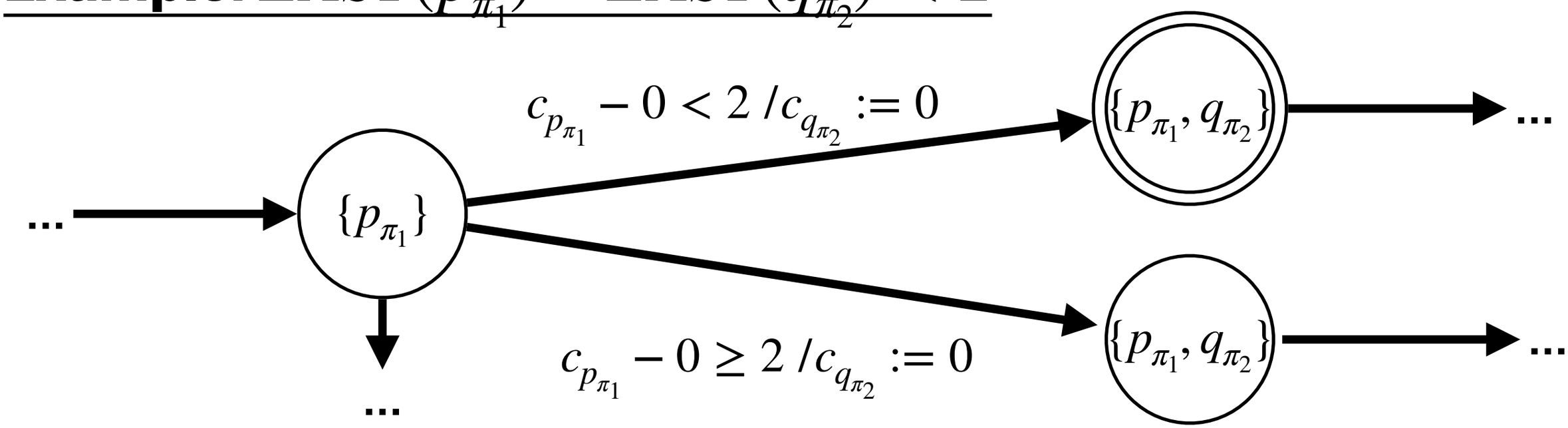


# Terms with $LAST$

Linear term over param.

- We support $LAST(p_{\pi_1}) - LAST(p'_{\pi_2}) \bowtie \mu$
  → Truth values changes only at transitions
- Encode $LAST(p_{\pi_1})$ and $LAST(p'_{\pi_2})$ with clocks

**Example:** $LAST(p_{\pi_1}) - LAST(q_{\pi_2}) < 2$



# HyperPTCTL → PTCTL

Self-composition to enc. multiple traces by one trace

- Reduction s.t.
  traces $\pi_1, \pi_2, \ldots, \pi_n$ of $\mathscr{A}$ is captured by
  trace $\pi_1 || \pi_2 || \cdots || \pi_n$ of $\mathscr{A} || \mathscr{A} || \cdots || \mathscr{A}$

**Limitation/Challenge**

Quantifier alternation ≈ autom. complement

- Complement is impossible
  → Focus on nest-free fragment

Limited, but still likely useful

- "zero-time" behavior is tricky

# Challenge: Zero-time behavior of TA

Multiple transitions may occur at the same time

$$\pi_1 = (l_0, \nu_0) \xrightarrow{\text{jump}_1} (l_1, \nu_1) \xrightarrow{\text{jump}_2} (l_2, \nu_2)$$

$$\pi_2 = (l'_0, \nu'_0) \xrightarrow{\text{jump}'_1} (l'_1, \nu'_1) \xrightarrow{\tau=2.4} (l'_2, \nu'_2)$$

Jumps in $\pi_1 || \pi_2$ can be …

- $\text{jump}_1 \rightarrow \text{jump}_2 \rightarrow \text{jump}'_1$
- $\text{jump}_1 \rightarrow \text{jump}'_1 \rightarrow \text{jump}_2$
- $\text{jump}_1 || \text{jump}'_1 \rightarrow \text{jump}_2$
- …

# Explicit Transition Ordering

Idea: Path valuation := (paths, order)

$$\pi_1 = (l_0, \nu_0) \xrightarrow{\text{jump}_1} (l_1, \nu_1) \xrightarrow{\text{jump}_2} (l_2, \nu_2)$$

$$\pi_2 = (l'_0, \nu'_0) \xrightarrow{\text{jump}'_1} (l'_1, \nu'_1) \xrightarrow{\tau=2.4} (l'_2, \nu'_2)$$

Transition ordering: $\text{jump}_1 \sim \text{jump}'_1 \prec \text{jump}_2$

Jumps in $\pi_1 || \pi_2$ is

- $\text{jump}_1 || \text{jump}'_1 \to \text{jump}_2$

# Implementation/Experiments

Model checker for PTAs

- Implemented the reduction to IMITATOR
  - HyPTCTLchecker: Published under GPLv3

- Reduction slightly differs from theoretical one
  e.g. IMITATOR's discrete var. not encoding w/ loc.

- The reduction is almost immediate
  → Report the result of synthesis with IMITATOR

- AWS EC2 m7i.4xlarge (16vCPU and 64 GiB RAM) w/ Ubuntu 22.04 LTS.

# Experimental Results

| Prop. ($\psi$) | PTA ($\mathcal{A}$) | $\lvert L\rvert$ | $\lvert\mathbb{C}\rvert$ | $\lvert\mathbb{P}\rvert_\psi$ | $\lvert\mathbb{P}\rvert_\mathcal{A}$ | $\lvert\mathcal{V}\rvert$ | Time [sec.] |
|---|---|---|---|---|---|---|---|
| Deviation | ClkGen | 2 | 1 | 1 | 1 | 2 | 4.116 |
| Opacity | Coffee | 6 | 2 | 0 | 3 | 2 | 0.723 |
| Opacity | STAC1:n | 8 | 2 | 0 | 2 | 2 | 0.178 |
| Opacity | STAC4:n | 9 | 2 | 0 | 5 | 2 | $< 0.001$ |
| Unfair | FIFO | 63 | 2 | 0 | 4 | 2 | 71.955 |
| Unfair | Priority | 72 | 2 | 0 | 4 | 2 | 6.855 |
| Unfair | R.R. | 81 | 3 | 0 | 4 | 2 | 12550.979 |
| RobOND | Coffee | 6 | 2 | 1 | 3 | 2 | 3.182 |
| RobOND | $\mathrm{WFAS}_0^1$ | 24 | 4 | 1 | 0 | 2 | 1.665 |
| RobOND | $\mathrm{WFAS}_0^2$ | 24 | 4 | 1 | 0 | 2 | 2.570 |
| RobOND | $\mathrm{WFAS}_1$ | 24 | 4 | 1 | 1 | 2 | 67.644 |
| RobOND | $\mathrm{WFAS}_2$ | 24 | 4 | 1 | 2 | 2 | 1332.310 |
| RobOND | ATM | 7 | 2 | 1 | 0 | 2 | **T.O.** |
| RobOND | ATM′ | 5 | 2 | 1 | 0 | 2 | 4179.197 |
| $\mathrm{EF}_2$ | Coffee | 6 | 2 | 1 | 0 | 2 | 0.034 |
| $\mathrm{EF}_3$ | Coffee | 6 | 2 | 1 | 0 | 3 | 159.541 |
| $\mathrm{EF}_4$ | Coffee | 6 | 2 | 1 | 0 | 4 | **T.O.** |

# Experimental Results

| Prop. ($\psi$) | PTA ($\mathcal{A}$) | $\lvert L\rvert$ | $\lvert\mathbb{C}\rvert$ | $\lvert\mathbb{P}\rvert_\psi$ | $\lvert\mathbb{P}\rvert_\mathcal{A}$ | $\lvert\mathcal{V}\rvert$ | Time [sec.] |
|---|---|---|---|---|---|---|---|
| Deviation | ClkGen | 2 | 1 | 1 | 1 | 2 | 4.116 |
| Opacity | Coffee | 6 | 2 | 0 | 3 | 2 | 0.723 |
| Opacity | STAC1:n | 8 | 2 | 0 | 2 | 2 | 0.178 |
| Opacity | STAC4:n | 9 | 2 | 0 | 5 | 2 | $< 0.001$ |
| Unfair | FIFO | 63 | 2 | 0 | 4 | 2 | 71.955 |
| Unfair | Priority | 72 | 2 | 0 | 4 | 2 | 6.855 |
| Unfair | R.R. | 81 | 3 | 0 | 4 | 2 | 12550.979 |
| RobOND | Coffee | 6 | 2 | 1 | 3 | 2 | 3.182 |
| RobOND | $\mathrm{WFAS}_0^1$ | 24 | 4 | 1 | 0 | 2 | 1.665 |
| RobOND | $\mathrm{WFAS}_0^2$ | 24 | 4 | 1 | 0 | 2 | 2.570 |
| RobOND | $\mathrm{WFAS}_1$ | 24 | 4 | 1 | 1 | 2 | 67.644 |
| RobOND | $\mathrm{WFAS}_2$ | 24 | 4 | 1 | 2 | 2 | 1332.310 |
| RobOND | ATM | 7 | 2 | 1 | 0 | 2 | **T.O.** |
| RobOND | ATM′ | 5 | 2 | 1 | 0 | 2 | 4179.197 |
| $\mathrm{EF}_2$ | Coffee | 6 | 2 | 1 | 0 | 2 | 0.034 |
| $\mathrm{EF}_3$ | Coffee | 6 | 2 | 1 | 0 | 3 | 159.541 |
| $\mathrm{EF}_4$ | Coffee | 6 | 2 | 1 | 0 | 4 | **T.O.** |

Fast for simple spec.

# Experimental Results

| Prop. ($\psi$) | PTA ($\mathcal{A}$) | $\lvert L\rvert$ | $\lvert\mathbb{C}\rvert$ | $\lvert\mathbb{P}\rvert_\psi$ | $\lvert\mathbb{P}\rvert_\mathcal{A}$ | $\lvert\mathcal{V}\rvert$ | Time [sec.] |
|---|---|---|---|---|---|---|---|
| Deviation | ClkGen | 2 | 1 | 1 | 1 | 2 | 4.116 |
| Opacity | Coffee | 6 | 2 | 0 | 3 | 2 | 0.723 |
| Opacity | STAC1:n | 8 | 2 | 0 | 2 | 2 | 0.178 |
| Opacity | STAC4:n | 9 | 2 | 0 | 5 | 2 | $< 0.001$ |
| Unfair | FIFO | 63 | 2 | 0 | 4 | 2 | 71.955 |
| Unfair | Priority | 72 | 2 | 0 | 4 | 2 | 6.855 |
| Unfair | R.R. | 81 | 3 | 0 | 4 | 2 | 12550.979 |
| RobOND | Coffee | 6 | 2 | 1 | 3 | 2 | 3.182 |
| RobOND | $\mathrm{WFAS}_0^1$ | 24 | 4 | 1 | 0 | 2 | 1.665 |
| RobOND | $\mathrm{WFAS}_0^2$ | 24 | 4 | 1 | 0 | 2 | 2.570 |
| RobOND | $\mathrm{WFAS}_1$ | 24 | 4 | 1 | 1 | 2 | 67.644 |
| RobOND | $\mathrm{WFAS}_2$ | 24 | 4 | 1 | 2 | 2 | 1332.310 |
| RobOND | ATM | 7 | 2 | 1 | 0 | 2 | **T.O.** |
| RobOND | ATM′ | 5 | 2 | 1 | 0 | 2 | 4179.197 |
| $\mathrm{EF}_2$ | Coffee | 6 | 2 | 1 | 0 | 2 | 0.034 |
| $\mathrm{EF}_3$ | Coffee | 6 | 2 | 1 | 0 | 3 | 159.541 |
| $\mathrm{EF}_4$ | Coffee | 6 | 2 | 1 | 0 | 4 | **T.O.** |

Fast for small models

# Experimental Results

| Prop. ($\psi$) | PTA ($\mathcal{A}$) | $\lvert L\rvert$ | $\lvert\mathbb{C}\rvert$ | $\lvert\mathbb{P}\rvert_\psi$ | $\lvert\mathbb{P}\rvert_\mathcal{A}$ | $\lvert\mathcal{V}\rvert$ | Time [sec.] |
|---|---|---|---|---|---|---|---|
| Deviation | ClkGen | 2 | 1 | 1 | 1 | 2 | 4.116 |
| Opacity | Coffee | 6 | 2 | 0 | 3 | 2 | 0.723 |
| Opacity | STAC1:n | 8 | 2 | 0 | 2 | 2 | 0.178 |
| Opacity | STAC4:n | 9 | 2 | 0 | 5 | 2 | $< 0.001$ |
| Unfair | FIFO | 63 | 2 | 0 | 4 | 2 | 71.955 |
| Unfair | Priority | 72 | 2 | 0 | 4 | 2 | 6.855 |
| Unfair | R.R. | 81 | 3 | 0 | 4 | 2 | 12550.979 |
| RobOND | Coffee | 6 | 2 | 1 | 3 | 2 | 3.182 |
| RobOND | $\mathrm{WFAS}_0^1$ | 24 | 4 | 1 | 0 | 2 | 1.665 |
| RobOND | $\mathrm{WFAS}_0^2$ | 24 | 4 | 1 | 0 | 2 | 2.570 |
| RobOND | $\mathrm{WFAS}_1$ | 24 | 4 | 1 | 1 | 2 | 67.644 |
| RobOND | $\mathrm{WFAS}_2$ | 24 | 4 | 1 | 2 | 2 | 1332.310 |
| RobOND | ATM | 7 | 2 | 1 | 0 | 2 | **T.O.** |
| RobOND | ATM′ | 5 | 2 | 1 | 0 | 2 | 4179.197 |
| $\mathrm{EF}_2$ | Coffee | 6 | 2 | 1 | 0 | 2 | 0.034 |
| $\mathrm{EF}_3$ | Coffee | 6 | 2 | 1 | 0 | 3 | 159.541 |
| $\mathrm{EF}_4$ | Coffee | 6 | 2 | 1 | 0 | 4 | **T.O.** |

Slow for large models

# Experimental Results

| Prop. ($\psi$) | PTA ($\mathcal{A}$) | $\lvert L\rvert$ | $\lvert\mathbb{C}\rvert$ | $\lvert\mathbb{P}\rvert_\psi$ | $\lvert\mathbb{P}\rvert_\mathcal{A}$ | $\lvert\mathcal{V}\rvert$ | Time [sec.] |
|---|---|---|---|---|---|---|---|
| Deviation | ClkGen | 2 | 1 | 1 | 1 | 2 | 4.116 |
| Opacity | Coffee | 6 | 2 | 0 | 3 | 2 | 0.723 |
| Opacity | STAC1:n | 8 | 2 | 0 | 2 | 2 | 0.178 |
| Opacity | STAC4:n | 9 | 2 | 0 | 5 | 2 | $< 0.001$ |
| Unfair | FIFO | 63 | 2 | 0 | 4 | 2 | 71.955 |
| Unfair | Priority | 72 | 2 | 0 | 4 | 2 | 6.855 |
| Unfair | R.R. | 81 | 3 | 0 | 4 | 2 | 12550.979 |
| RobOND | Coffee | 6 | 2 | 1 | 3 | 2 | 3.182 |
| RobOND | $\mathrm{WFAS}_0^1$ | 24 | 4 | 1 | 0 | 2 | 1.665 |
| RobOND | $\mathrm{WFAS}_0^2$ | 24 | 4 | 1 | 0 | 2 | 2.570 |
| RobOND | $\mathrm{WFAS}_1$ | 24 | 4 | 1 | 1 | 2 | 67.644 |
| RobOND | $\mathrm{WFAS}_2$ | 24 | 4 | 1 | 2 | 2 | 1332.310 |
| RobOND | ATM | 7 | 2 | 1 | 0 | 2 | **T.O.** |
| RobOND | ATM′ | 5 | 2 | 1 | 0 | 2 | 4179.197 |
| $\mathrm{EF}_2$ | Coffee | 6 | 2 | 1 | 0 | 2 | 0.034 |
| $\mathrm{EF}_3$ | Coffee | 6 | 2 | 1 | 0 | 3 | 159.541 |
| $\mathrm{EF}_4$ | Coffee | 6 | 2 | 1 | 0 | 4 | **T.O.** |

Parametric Unfairness for Round-Robin Scheduler < 3.5 h

Slow for large models

# Experimental Results

| Prop. ($\psi$) | PTA ($\mathcal{A}$) | $\lvert L\rvert$ | $\lvert\mathbb{C}\rvert$ | $\lvert\mathbb{P}\rvert_\psi$ | $\lvert\mathbb{P}\rvert_\mathcal{A}$ | $\lvert\mathcal{V}\rvert$ | Time [sec.] |
|---|---|---|---|---|---|---|---|
| Deviation | ClkGen | 2 | 1 | 1 | 1 | 2 | 4.116 |
| Opacity | Coffee | 6 | 2 | 0 | 3 | 2 | 0.723 |
| Opacity | STAC1:n | 8 | 2 | 0 | 2 | 2 | 0.178 |
| Opacity | STAC4:n | 9 | 2 | 0 | 5 | 2 | $< 0.001$ |
| Unfair | FIFO | 63 | 2 | 0 | 4 | 2 | 71.955 |
| Unfair | Priority | 72 | 2 | 0 | 4 | 2 | 6.855 |
| Unfair | R.R. | 81 | 3 | 0 | 4 | 2 | 12550.979 |
| RobOND | Coffee | 6 | 2 | 1 | 3 | 2 | 3.182 |
| RobOND | $\text{WFAS}_0^1$ | 24 | 4 | 1 | 0 | 2 | 1.665 |
| RobOND | $\text{WFAS}_0^2$ | 24 | 4 | 1 | 0 | 2 | 2.570 |
| RobOND | $\text{WFAS}_1$ | 24 | 4 | 1 | 1 | 2 | 67.644 |
| RobOND | $\text{WFAS}_2$ | 24 | 4 | 1 | 2 | 2 | 1332.310 |
| RobOND | ATM | 7 | 2 | 1 | 0 | 2 | **T.O.** |
| RobOND | ATM′ | 5 | 2 | 1 | 0 | 2 | 4179.197 |
| $\text{EF}_2$ | Coffee | 6 | 2 | 1 | 0 | 2 | 0.034 |
| $\text{EF}_3$ | Coffee | 6 | 2 | 1 | 0 | 3 | 159.541 |
| $\text{EF}_4$ | Coffee | 6 | 2 | 1 | 0 | 4 | **T.O.** |

**Scalability wrt # of path is not good due to self-composition**

# Experimental Results

| Prop. ($\psi$) | PTA ($\mathcal{A}$) | $\lvert L\rvert$ | $\lvert\mathbb{C}\rvert$ | $\lvert\mathbb{P}\rvert_\psi$ | $\lvert\mathbb{P}\rvert_\mathcal{A}$ | $\lvert\mathcal{V}\rvert$ | Time [sec.] |
|---|---|---|---|---|---|---|---|
| Deviation | ClkGen | 2 | 1 | 1 | 1 | 2 | 4.116 |
| Opacity | Coffee | 6 | 2 | 0 | 3 | 2 | 0.723 |
| Opacity | STAC1:n | 8 | 2 | 0 | 2 | 2 | 0.178 |
| Opacity | STAC4:n | 9 | 2 | 0 | 5 | 2 | $< 0.001$ |
| Unfair | FIFO | 63 | 2 | 0 | 4 | 2 | 71.955 |
| Unfair | Priority | 72 | 2 | 0 | 4 | 2 | 6.855 |
| Unfair | R.R. | 81 | 3 | 0 | 4 | 2 | 12550.979 |
| RobOND | Coffee | 6 | 2 | 1 | 3 | 2 | 3.182 |
| RobOND | $\mathrm{WFAS}_0^1$ | 24 | 4 | 1 | 0 | 2 | 1.665 |
| RobOND | $\mathrm{WFAS}_0^2$ | 24 | 4 | 1 | 0 | 2 | 2.570 |
| RobOND | $\mathrm{WFAS}_1$ | 24 | 4 | 1 | 1 | 2 | 67.644 |
| RobOND | $\mathrm{WFAS}_2$ | 24 | 4 | 1 | 2 | 2 | 1332.310 |
| RobOND | ATM | 7 | 2 | 1 | 0 | 2 | T.O. |
| RobOND | ATM′ | 5 | 2 | 1 | 0 | 2 | 4179.197 |
| $\mathrm{EF}_2$ | Coffee | 6 | 2 | 1 | 0 | 2 | 0.034 |
| $\mathrm{EF}_3$ | Coffee | 6 | 2 | 1 | 0 | 3 | 159.541 |
| $\mathrm{EF}_4$ | Coffee | 6 | 2 | 1 | 0 | 4 | T.O. |

Scalability wrt # of path is not good due to self-composition

Can handle 3 paths

# Related Logics/Methods

| | Logic | Continuous Time? | Parametric? | Model Checking? | Quantifier Alternation in Model Checking? |
|---|---|---|---|---|---|
| **[Ours]** | Ext-HyperPTCTL | **Yes** | **Yes** | **Yes** | **No** |
| **[Ho+, 2021]** | HyperMITL | **Yes** | **No** | **Yes** | **Only for untimed models** |
| **[Bonakdarpour+, 2020]** | HyperMTL | **No** | **No** | **Yes** | **Yes** |
| **[Bartocci+, 2023]** | HyperSTL | **Yes** | **Yes** | **No (Req. Mining)** | N/A |

# Conclusions

- Introduce HyperPTCTL and Ext-HyperPTCTL
- Semi-algorithm for model checking/synthesis of PTAs against nest-free Ext-HyperPTCTL
- Show decidable subclasses even w/ param.
- Implementation & Experiments
  - Works for mild size PTAs

# Appendix

# Syntax of (Ext-)HyperPTCTL

proposition on loc.
(Edge labels are simplification for illustration)

## HyperPTCTL

$$\varphi ::= \top \mid \sigma_\pi \mid \neg\varphi \mid \varphi \vee \varphi \mid \exists \pi_1, \pi_2, \ldots, \pi_n . \varphi \, \mathcal{U}_{\bowtie\gamma} \, \varphi \mid \forall \pi_1, \pi_2, \ldots, \pi_n . \varphi \, \mathcal{U}_{\bowtie\gamma} \, \varphi$$

temporal level

$$\psi ::= \varphi \mid p \bowtie lt_{\geq 0} \mid \neg\psi \mid \psi \vee \psi \mid \exists p \, \psi$$

top level

## Ext-HyperPTCTL

$$\varphi ::= \top \mid \sigma_\pi \mid LAST(\sigma_\pi) - LAST(\sigma_\pi) \bowtie lt \mid cnt_{\geq 0} \bowtie d \mid (cnt \bmod N) \bowtie d \mid \cdots$$

# Semantics of HyperPTCTL

- $(\Pi, \trianglelefteq_\Pi), s \models_{v,\mathcal{A}} \sigma_\pi$ if $\pi \in \mathbf{dom}(\Pi)$ and $\sigma \in \Lambda(\mathit{Init}(\Pi(\pi)))$;
- $(\Pi, \trianglelefteq_\Pi), s \models_{v,\mathcal{A}} \neg\varphi$ if we have $(\Pi, \trianglelefteq_\Pi), s \not\models_{v,\mathcal{A}} \varphi$;
- $(\Pi, \trianglelefteq_\Pi), s \models_{v,\mathcal{A}} \varphi_1 \vee \varphi_2$ if $(\Pi, \trianglelefteq_\Pi), s \models_{v,\mathcal{A}} \varphi_1$ or $(\Pi, \trianglelefteq_\Pi), s \models_{v,\mathcal{A}} \varphi_2$ holds;
- $(\Pi, \trianglelefteq_\Pi), s \models_{v,\mathcal{A}} \exists \pi_1, \pi_2, \ldots, \pi_n. \varphi_1 \mathcal{U}_{\bowtie\gamma} \varphi_2$ if for some extension $(\Pi^1, \trianglelefteq_{\Pi^1})$ of $(\Pi, \trianglelefteq_\Pi)$ satisfying $\mathbf{dom}(\Pi^1) = \mathbf{dom}(\Pi) \sqcup \{\pi_1, \pi_2, \ldots, \pi_n\}$ and $\Pi^1(\pi_i) \in \mathit{Paths}(v(\mathcal{A}), s)$ for each $i \in \{1, 2, \ldots, n\}$, there is $(\Pi^2, \trianglelefteq_{\Pi^2})$ satisfying $(\Pi^1, \trianglelefteq_{\Pi^1}) \succeq (\Pi^2, \trianglelefteq_{\Pi^2})$, $\mathit{Dur}(\Pi^1 - \Pi^2) \bowtie v(\gamma)$, $(\Pi^2, \trianglelefteq_{\Pi^2}), \mathit{Init}(\Pi^2(\pi_n)) \models_{v,\mathcal{A}} \varphi_2$, and for any $(\Pi^3, \trianglelefteq_{\Pi^3})$ satisfying $(\Pi^1, \trianglelefteq_{\Pi^1}) \succeq (\Pi^3, \trianglelefteq_{\Pi^3}) \succ (\Pi^2, \trianglelefteq_{\Pi^2})$, $(\Pi^3, \trianglelefteq_{\Pi^3}), \mathit{Init}(\Pi^3(\pi_n)) \models_{v,\mathcal{A}} \varphi_1$ holds.

$\forall\mathcal{U}$ is omitted

# Terms with #

- Encode term's values with discrete states
- $\#p_{\pi_1}$ changes only when satisfied prop. changes on $\pi_1$
  → Truth values changes only at transitions
- ((linear term with #) $\mathrm{mod} N$) $\bowtie d$: Encode LHS values with $N$ states for each $\#p_{\pi}$
- (positive linear with #) $\bowtie d$: LHS strictly increases
  → merge > d

Like the abstraction for regions

# Terms with $LAST$

Linear term over param.

- We support $LAST(p_{\pi_1}) - LAST(p'_{\pi_2}) \bowtie \mu$
  - → Truth values changes only at transitions

- Encode $LAST(p_{\pi_1})$ and $LAST(p'_{\pi_2})$ with clocks

# Specifications in Experiments (1/3)

**Deviation**:

$$\exists \pi_1, \pi_2 \,.\, (\text{AtMostOneDiff}) \mathcal{U}_{\geq 0} (\text{SameCount} \wedge \text{LargeDeviation})$$

- AtMostOneDiff: $(\#H_{\pi_1} - \#H_{\pi_2}) \bmod 4 \in \{0,1,3\}$
- SameCount: $(\#H_{\pi_1} - \#H_{\pi_2}) \bmod 4 = 0$
- LargeDeviation: $Last(H_{\pi_1}) - Last(H_{\pi_2}) \notin [-p, p]$

**Opacity**:

$$\exists \pi_1, \pi_2 \,.\, (\neg \text{Goal}_{\pi_1} \wedge \neg \text{Goal}_{\pi_2}) \mathcal{U}_{=p} (\text{Goal}_{\pi_1} \wedge \text{Goal}_{\pi_2} \wedge \#Private_{\pi_1} = 0 \wedge \#Private_{\pi_2} > 0)$$

# Specifications in Experiments (2/3)

**Unfair**: $\exists \pi_1, \pi_2 \,.\, (\text{SyncSub}) \mathcal{U}_{\geq 0} (\text{SameCount} \wedge \text{LargeDeviation})$

- SyncSub: $\text{Sub}^1_{\pi_1} = \text{Sub}^2_{\pi_2}$
- SameCount: $(\#\text{Run}^1_{\pi_1} - \#\text{Run}^2_{\pi_2}) \bmod 4 = 0$
- LargeDeviation: $\mathit{Last}(\text{Run}^1_{\pi_1}) - \mathit{Last}(\text{Run}^2_{\pi_2}) \notin (-5,5)$

**RobOND**: $\exists \pi_1, \pi_2 \,.\, (\text{SyncIn} \wedge \text{AtMostOneDiff}) \mathcal{U}_{\geq 0} (\text{LargeDeviation})$

- SyncIn: $\forall i \in \{1,2,\ldots,m\} \,.\, \text{In}^i_{\pi_1} = \text{In}^i_{\pi_2}$
- AtMostOneDiff: $\forall j \in \{1,2,\ldots,n\} \,.\, (\#\text{Out}^i_{\pi_1} - \#\text{Out}^i_{\pi_2}) \bmod 4 \in \{0,1,3\}$
- LargeDeviation:
  $\exists j \in \{1,2,\ldots,n\} \,.\, (\#\text{Out}^j_{\pi_1} - \#\text{Out}^j_{\pi_2}) \bmod 4 = 0 \wedge \mathit{Last}(\text{Out}^j_{\pi_1}) - \mathit{Last}(\text{Out}^j_{\pi_2}) \notin [-p, p]$

# Specifications in Experiments (3/3)

Not supported in theory, but supported in our implementation w/ IMITATOR's discrete variables

**EF$_i$**: $\exists \pi_1, \pi_2, \ldots, \pi_i \,.\, \Diamond_{[p,p]} \forall j \in \{1,2,\ldots,i\} \#a_{\pi_j} - \#a_{\pi_{j+1}} = 1$