ICECCS 2012

20th July 2012
Paris, France

Parameter Synthesis for Hierarchical Concurrent Real-Time Systems

Étienne ANDRÉ

Laboratoire d'Informatique de Paris Nord
Université Paris 13, Sorbonne Paris Cité, France

Joint work with Liu Yang, Sun Jun, Dong Jin Song

Context: Verifying Complex Timed Systems (1/2)

- Need for early bug detection
  - Bugs discovered when final testing: expensive
  - Need for thorough modeling and verification

Context: Verifying Complex Timed Systems (1/2)

- Need for early bug detection
  - Bugs discovered when final testing: expensive
  - Need for thorough modeling and verification
- Input

A timed concurrent system

Context: Verifying Complex Timed Systems (1/2)

- Need for early bug detection
  - Bugs discovered when final testing: expensive
  - Need for thorough modeling and verification
- Input

A timed concurrent system

A good behavior expected for the system

Context: Verifying Complex Timed Systems (1/2)

- Need for early bug detection
  - Bugs discovered when final testing: expensive
  - Need for thorough modeling and verification
- Input

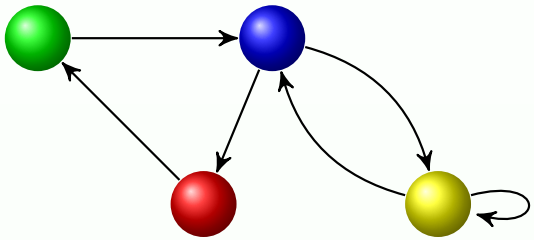
A timed concurrent system

A good behavior expected for the system

- Question: does the system behave well?

Context: Verifying Complex Timed Systems (2/2)

- Use formal methods

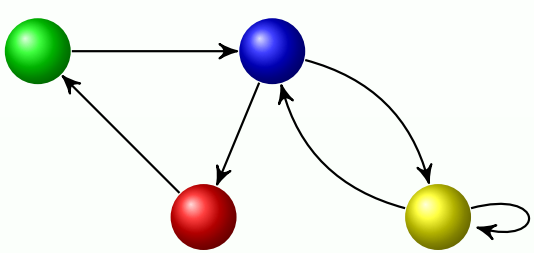


A finite model of the system

A formula to be satisfied

Context: Verifying Complex Timed Systems (2/2)

- Use formal methods



$\stackrel{?}{\models}$

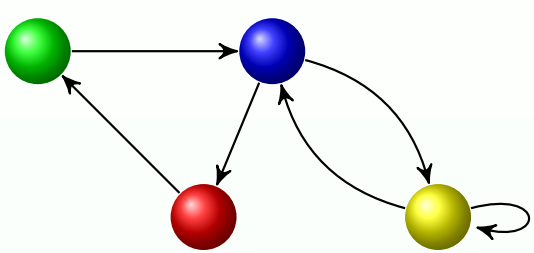
A finite model of the system

A formula to be satisfied

- Question: does the model of the system satisfy the formula?

Context: Verifying Complex Timed Systems (2/2)

- Use formal methods



$\stackrel{?}{\models}$

$AG\neg$ 

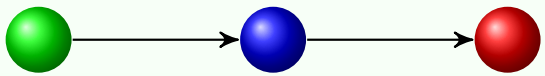
A finite model of the system

A formula to be satisfied

- Question: does the model of the system satisfy the formula?

Yes

No



Counterexample

Motivation: Parameter Synthesis

- Timed systems are characterized by a set of timing constants
  - "The packet transmission lasts for $50\,ms$"
  - "The sensor reads the value every $10\,s$"
  - etc.
- Verification for one set of constants does not guarantee the correctness for other values
- Challenges
  - Numerous verifications: is the system correct for any value within $[40; 60]$?
  - Optimization: until what value can we increase 10?
  - Robustness: What happens if 50 is implemented with 49.99?

Motivation: Parameter Synthesis

- Timed systems are characterized by a set of timing constants
  - "The packet transmission lasts for $50\,ms$"
  - "The sensor reads the value every $10\,s$"
  - etc.
- Verification for one set of constants does not guarantee the correctness for other values
- Challenges
  - Numerous verifications: is the system correct for any value within $[40; 60]$?
  - Optimization: until what value can we increase 10?
  - Robustness: What happens if 50 is implemented with 49.99?
- Parameter synthesis
  - Consider that timing constants are parameters
  - Find good values for the parameters

Outline

Outline

Stateful Timed CSP: Motivation

- Need for an intuitive formal modeling language
  - Easy to understand for an engineer
  - With a formal semantics allowing verification
- Quantitative verification of timed concurrent systems
- Hierarchical design

Stateful Timed CSP: Features

- Standard constructions of CSP [Hoare, 1978]
  - Events
  - Conditional and general choice
  - Sequential and parallel composition
  - Operations on shared variables
- Data structures

Stateful Timed CSP: Features

- Standard constructions of CSP [Hoare, 1978]
  - Events
  - Conditional and general choice
  - Sequential and parallel composition
  - Operations on shared variables
- Data structures
- Additional timed constructs [Schneider, 2000, Sun et al., 2009]
  - `Wait`[d]: waits exactly d time units
  - P `timeout`[d] Q: the first observable event of P shall occur before d time units; otherwise, behaves like Q
  - P `interrupt`[d] Q: behaves like P until d time units; then, like Q
  - P `within`[d]: the first observable event of P shall occur before d time units
  - P `deadline`[d]: P shall terminate before d time units

Stateful Timed CSP: Semantics

- Use implicit clocks
  - Clocks: real-valued variables increasing linearly at the same rate
  - Created and started when some processes are activated
  - Deleted when no longer used
- Configurations: Variables + Process + Value for each clock
  - Problem of real-time: infinite set of values
    $\rightsquigarrow$ Infinite representation of the state space
- Abstract configurations: Variables + Process + Clock zone [Sun et al., 2009]
  - Clock zone: constraint on the clocks
    $\rightsquigarrow$ Finite representation of the state space

An Example (1/2)

- An Example of STCSP Process
  - (with no variable)

$$P \triangleq (a \rightarrow \texttt{Wait}[5]; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[3]\ c \rightarrow P$$

- Intuitive behavior:

An Example (1/2)

- An Example of STCSP Process
  - (with no variable)

$$P \triangleq (a \rightarrow \texttt{Wait}[5]; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[3]\ c \rightarrow P$$

- Intuitive behavior:
  - The behavior is infinite (because of the recursion)
  - b will never happen (because of $\texttt{interrupt}[3]$)

An Example (2/2)

$\mathbf{P} \triangleq (\mathbf{a} \rightarrow \texttt{Wait}[\mathbf{5}]; \mathbf{b} \rightarrow \texttt{Stop})\ \texttt{interrupt}[\mathbf{3}]\ \mathbf{c} \rightarrow \mathbf{P}$

- P

  true

An Example (2/2)

$\mathbf{P} \triangleq (\mathbf{a} \rightarrow \texttt{Wait}[\mathbf{5}]; \mathbf{b} \rightarrow \texttt{Stop})\ \texttt{interrupt}[\mathbf{3}]\ \mathbf{c} \rightarrow \mathbf{P}$

- $(a \rightarrow \texttt{Wait}[5]; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[3] \quad c \rightarrow P$
  $\texttt{true}$

An Example (2/2)

$\mathbf{P} \triangleq (\mathbf{a} \rightarrow \texttt{Wait}[\mathbf{5}]; \mathbf{b} \rightarrow \texttt{Stop})\ \texttt{interrupt}[\mathbf{3}]\ \mathbf{c} \rightarrow \mathbf{P}$

- $(a \rightarrow \texttt{Wait}[5]; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[3]_{x_1}\ c \rightarrow P$
  $0 \leq x_1 \leq 3$

An Example (2/2)

$\mathbf{P} \triangleq (\mathbf{a} \rightarrow \texttt{Wait}[\mathbf{5}]; \mathbf{b} \rightarrow \texttt{Stop})\ \texttt{interrupt}[\mathbf{3}]\ \mathbf{c} \rightarrow \mathbf{P}$

- $(a \rightarrow \texttt{Wait}[5]; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[3]_{x_1}\ c \rightarrow P$
  $0 \leq x_1 \leq 3$
- $(\texttt{Wait}[5]\ \ ; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[3]_{x_1}\ c \rightarrow P$
  $0 \leq x_1 \leq 3$

An Example (2/2)

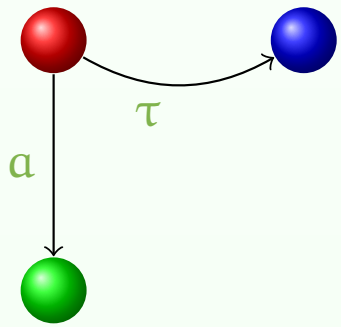
$\mathbf{P} \triangleq (\mathbf{a} \rightarrow \texttt{Wait}[\mathbf{5}]; \mathbf{b} \rightarrow \texttt{Stop})\ \texttt{interrupt}[\mathbf{3}]\ \mathbf{c} \rightarrow \mathbf{P}$

- $(a \rightarrow \texttt{Wait}[5]; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[3]_{x_1}\ c \rightarrow P$
  $0 \leq x_1 \leq 3$
- $(\texttt{Wait}[5]_{x_2}; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[3]_{x_1}\ c \rightarrow P$
  $0 \leq x_1 \leq 3 \wedge 0 \leq x_2 \leq 5 \wedge 0 \leq x_1 - x_2 \leq 3$

An Example (2/2)

$\mathbf{P} \triangleq (\mathbf{a} \rightarrow \mathtt{Wait}[\mathbf{5}]; \mathbf{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[\mathbf{3}]\ \mathbf{c} \rightarrow \mathbf{P}$

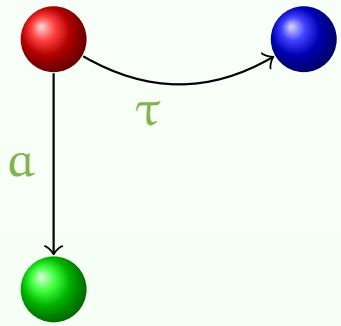
- $(a \rightarrow \mathtt{Wait}[5]; b \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[3]_{x_1}\ c \rightarrow P$
  $0 \leq x_1 \leq 3$
- $(\mathtt{Wait}[5]_{x_2}; b \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[3]_{x_1}\ c \rightarrow P$
  $0 \leq x_1 \leq 3 \wedge 0 \leq x_2 \leq 5 \wedge 0 \leq x_1 - x_2 \leq 3$
- $c \rightarrow P$
  $x_1 \geq 3$



An Example (2/2)

$\mathbf{P} \triangleq (\mathbf{a} \rightarrow \texttt{Wait}[\mathbf{5}]; \mathbf{b} \rightarrow \texttt{Stop})\ \texttt{interrupt}[\mathbf{3}]\ \mathbf{c} \rightarrow \mathbf{P}$

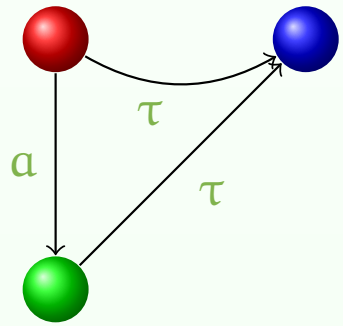
- $(a \rightarrow \texttt{Wait}[5]; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[3]_{x_1}\ c \rightarrow P$
  $0 \leq x_1 \leq 3$
- $(\texttt{Wait}[5]_{x_2}; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[3]_{x_1}\ c \rightarrow P$
  $0 \leq x_1 \leq 3 \wedge 0 \leq x_2 \leq 5 \wedge 0 \leq x_1 - x_2 \leq 3$
- $c \rightarrow P$
  $\texttt{true}$



An Example (2/2)

$\mathbf{P} \triangleq (\mathbf{a} \rightarrow \mathtt{Wait}[\mathbf{5}]; \mathbf{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[\mathbf{3}]\ \mathbf{c} \rightarrow \mathbf{P}$

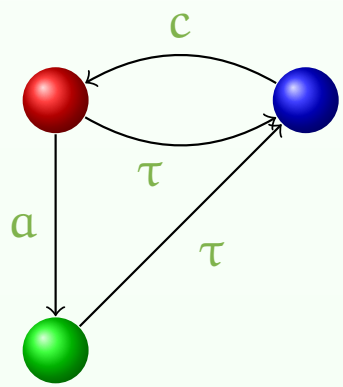
- $(a \rightarrow \mathtt{Wait}[5]; b \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[3]_{x_1}\ c \rightarrow P$
  $0 \leq x_1 \leq 3$
- $(\mathtt{Wait}[5]_{x_2}; b \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[3]_{x_1}\ c \rightarrow P$
  $0 \leq x_1 \leq 3 \wedge 0 \leq x_2 \leq 5 \wedge 0 \leq x_1 - x_2 \leq 3$
- $c \rightarrow P$
  $\mathtt{true}$



An Example (2/2)

$\mathbf{P} \triangleq (\mathbf{a} \rightarrow \mathtt{Wait}[\mathbf{5}]; \mathbf{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[\mathbf{3}]\ \mathbf{c} \rightarrow \mathbf{P}$

- $(a \rightarrow \mathtt{Wait}[5]; b \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[3]_{x_1}\ c \rightarrow P$
  $0 \leq x_1 \leq 3$
- $(\mathtt{Wait}[5]_{x_2}; b \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[3]_{x_1}\ c \rightarrow P$
  $0 \leq x_1 \leq 3 \wedge 0 \leq x_2 \leq 5 \wedge 0 \leq x_1 - x_2 \leq 3$
- $c \rightarrow P$
  $\mathtt{true}$



Related Formalisms

- Timed Automata [Alur and Dill, 1994]
  - Expressiveness: incomparable with Stateful Timed CSP
  - Possible use of data structures (e.g., in UPPAAL)
  - Explicit set of clocks
  - Limited hierarchical definition
- Time Petri Nets [Merlin, 1974]
  - Expressiveness: more or less equivalent to Timed Automata
  - Possible use of data structures (e.g., in colored Time Petri Nets)
  - Possible use of hierarchical structures
  - Composition less straightforward

Presentation of Parametric Stateful Timed CSP

- Goals
  - Avoid numerous verifications for many timing constants
  - Synthesis of parameters w.r.t. a given property
  - Optimize timing constants
  - Quantify the robustness of the system

Presentation of Parametric Stateful Timed CSP

- Goals
  - Avoid numerous verifications for many timing constants
  - Synthesis of parameters w.r.t. a given property
  - Optimize timing constants
  - Quantify the robustness of the system
- Extension of Stateful Timed CSP
  - Constants in timed constructs can be unkown, i.e., parameters

Configurations in Parametric Stateful Timed CSP

- Semantics of Stateful Timed CSP
  - Abstract configurations: Variables + Process + Clock zone
    $\rightsquigarrow$ Finite representation of the state space
- Semantics of Parametric Stateful Timed CSP
  - (Symbolic) configurations: Variables + Process + Constraint on the clocks and the parameters
  - Non-necessarily finite representation of the state space!

An Example (1/2)

- Remember the example of STCSP Process

$$P \triangleq (a \rightarrow \texttt{Wait}[5]; b \rightarrow \texttt{Stop}) \ \texttt{interrupt}[3] \ c \rightarrow P$$

- Now consider a parametric version of P
  - Use 2 parameters: u_3 and u_5

$$P \triangleq (a \rightarrow \texttt{Wait}[u_5]; b \rightarrow \texttt{Stop}) \ \texttt{interrupt}[u_3] \ c \rightarrow P$$

- Intuitive behavior:

An Example (1/2)

- Remember the example of STCSP Process

$$P \triangleq (a \rightarrow \texttt{Wait}[5]; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[3]\ c \rightarrow P$$

- Now consider a parametric version of P
  - Use 2 parameters: u_3 and u_5

$$P \triangleq (a \rightarrow \texttt{Wait}[u_5]; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]\ c \rightarrow P$$

- Intuitive behavior: b may now happen
  - Depends on the relation between u_3 and u_5

An Example (2/2)

$\mathbf{P} \triangleq (\mathtt{a} \rightarrow \mathtt{Wait}[u_5]; \mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]\ \mathtt{c} \rightarrow \mathbf{P}$

P

true

true

An Example (2/2)

$\mathbf{P} \triangleq (\mathtt{a} \rightarrow \mathtt{Wait}[u_5]; \mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]\ \mathtt{c} \rightarrow \mathbf{P}$

- $(\mathtt{a} \rightarrow \mathtt{Wait}[u_5]; \mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]\ \mathtt{c} \rightarrow \mathtt{P}$
  $\mathtt{true}$ $\mathtt{true}$

An Example (2/2)

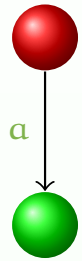
$\mathbf{P} \triangleq (\mathtt{a} \rightarrow \mathtt{Wait}[u_5]; \mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]\ \mathtt{c} \rightarrow \mathbf{P}$

- $(\mathtt{a} \rightarrow \mathtt{Wait}[u_5]; \mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ \mathtt{c} \rightarrow \mathtt{P}$
  $x_1 = 0$ $\qquad$ $\mathtt{true}$

An Example (2/2)

$\mathbf{P} \triangleq (a \rightarrow \texttt{Wait}[u_5]; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]\ c \rightarrow \mathbf{P}$

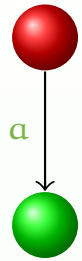
- $(a \rightarrow \texttt{Wait}[u_5]; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $x_1 = 0$ true
- $(\texttt{Wait}[u_5]\ ; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $0 \leq x_1 \leq u_3$ true



An Example (2/2)

$\mathbf{P} \triangleq (a \rightarrow \texttt{Wait}[u_5]; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]\ c \rightarrow \mathbf{P}$

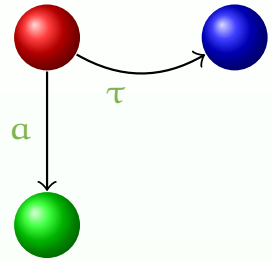
- $(a \rightarrow \texttt{Wait}[u_5]; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $x_1 = 0$ | true
- $(\texttt{Wait}[u_5]_{x_2}; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $0 \leq x_1 \leq u_3 \wedge x_2 = 0$ | true



An Example (2/2)

$\mathbf{P} \triangleq (\mathtt{a} \rightarrow \mathtt{Wait}[u_5]; \mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]\ \mathtt{c} \rightarrow \mathbf{P}$

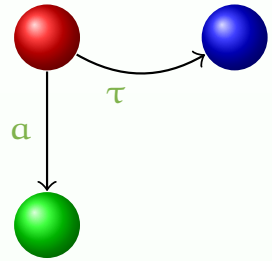
- $(\mathtt{a} \rightarrow \mathtt{Wait}[u_5]; \mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ \mathtt{c} \rightarrow \mathtt{P}$
  $x_1 = 0$ true
- $(\mathtt{Wait}[u_5]_{x_2}; \mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ \mathtt{c} \rightarrow \mathtt{P}$
  $0 \leq x_1 \leq u_3 \wedge x_2 = 0$ true
- $\mathtt{c} \rightarrow \mathtt{P}$
  $x_1 \geq 0 \wedge x_1 = u_3$ true



An Example (2/2)

$\mathbf{P} \triangleq (\mathtt{a} \rightarrow \mathtt{Wait}[u_5]; \mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]\ \mathtt{c} \rightarrow \mathbf{P}$

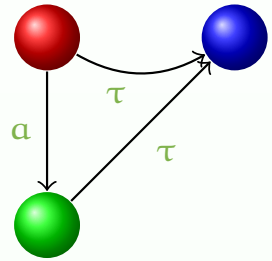
- $(\mathtt{a} \rightarrow \mathtt{Wait}[u_5]; \mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ \mathtt{c} \rightarrow \mathtt{P}$
  $x_1 = 0$ — true
- $(\mathtt{Wait}[u_5]_{x_2}; \mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ \mathtt{c} \rightarrow \mathtt{P}$
  $0 \leq x_1 \leq u_3 \wedge x_2 = 0$ — true
- $\mathtt{c} \rightarrow \mathtt{P}$
  true — true



An Example (2/2)

$\mathbf{P} \triangleq (\mathtt{a} \rightarrow \mathtt{Wait}[u_5]; \mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]\ \mathtt{c} \rightarrow \mathbf{P}$

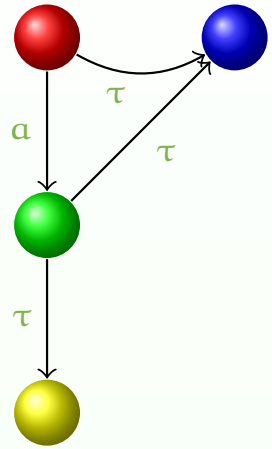
- $(\mathtt{a} \rightarrow \mathtt{Wait}[u_5]; \mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ \mathtt{c} \rightarrow \mathtt{P}$
  $x_1 = 0$ — true
- $(\mathtt{Wait}[u_5]_{x_2}; \mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ \mathtt{c} \rightarrow \mathtt{P}$
  $0 \leq x_1 \leq u_3 \wedge x_2 = 0$ — true
- $\mathtt{c} \rightarrow \mathtt{P}$
  true — true



An Example (2/2)

$\mathbf{P} \triangleq (\mathtt{a} \rightarrow \mathtt{Wait}[u_5]; \mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]\ \mathtt{c} \rightarrow \mathbf{P}$

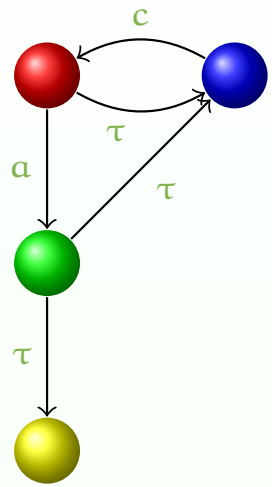
- $(\mathtt{a} \rightarrow \mathtt{Wait}[u_5]; \mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ \mathtt{c} \rightarrow \mathtt{P}$
  $x_1 = 0$ — true
- $(\mathtt{Wait}[u_5]_{x_2}; \mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ \mathtt{c} \rightarrow \mathtt{P}$
  $0 \leq x_1 \leq u_3 \wedge x_2 = 0$ — true
- $\mathtt{c} \rightarrow \mathtt{P}$
  true — true
- $(\mathtt{Skip}; \mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ \mathtt{c} \rightarrow \mathtt{P}$
  $u_5 \leq x_1 \leq u_3$ — $u_5 \leq u_3$



An Example (2/2)

$\mathbf{P} \triangleq (\mathtt{a} \rightarrow \mathtt{Wait}[u_5]; \mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]\ \mathtt{c} \rightarrow \mathbf{P}$

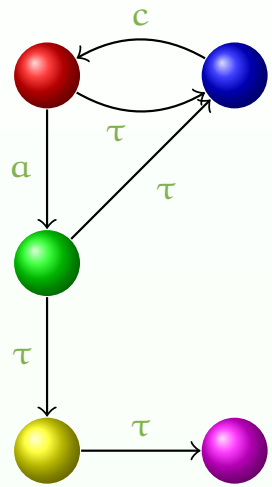
- $(\mathtt{a} \rightarrow \mathtt{Wait}[u_5]; \mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ \mathtt{c} \rightarrow \mathtt{P}$
  $x_1 = 0$ — true
- $(\mathtt{Wait}[u_5]_{x_2}; \mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ \mathtt{c} \rightarrow \mathtt{P}$
  $0 \leq x_1 \leq u_3 \wedge x_2 = 0$ — true
- $\mathtt{c} \rightarrow \mathtt{P}$
  true — true
- $(\mathtt{Skip}; \mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ \mathtt{c} \rightarrow \mathtt{P}$
  $u_5 \leq x_1 \leq u_3$ — $u_5 \leq u_3$



An Example (2/2)

$\mathbf{P} \triangleq (\mathtt{a} \rightarrow \mathtt{Wait}[u_5]; \mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]\ \mathtt{c} \rightarrow \mathbf{P}$

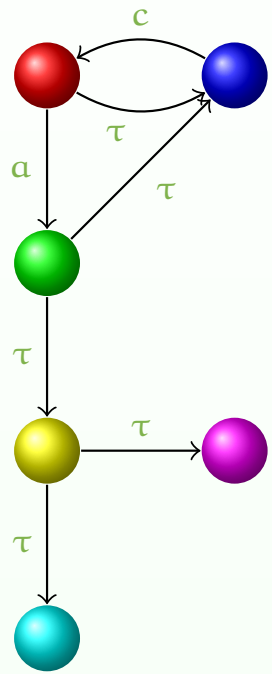
- $(\mathtt{a} \rightarrow \mathtt{Wait}[u_5]; \mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ \mathtt{c} \rightarrow \mathtt{P}$
  $x_1 = 0$ — true
- $(\mathtt{Wait}[u_5]_{x_2}; \mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ \mathtt{c} \rightarrow \mathtt{P}$
  $0 \leq x_1 \leq u_3 \wedge x_2 = 0$ — true
- $\mathtt{c} \rightarrow \mathtt{P}$
  true — true
- $(\mathtt{Skip}; \mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ \mathtt{c} \rightarrow \mathtt{P}$
  $u_5 \leq x_1 \leq u_3$ — $u_5 \leq u_3$
- $(\mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ \mathtt{c} \rightarrow \mathtt{P}$
  $u_5 \leq x_1 \leq u_3$ — $u_5 \leq u_3$



An Example (2/2)

$\mathbf{P} \triangleq (a \rightarrow \texttt{Wait}[u_5]; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]\ c \rightarrow \mathbf{P}$

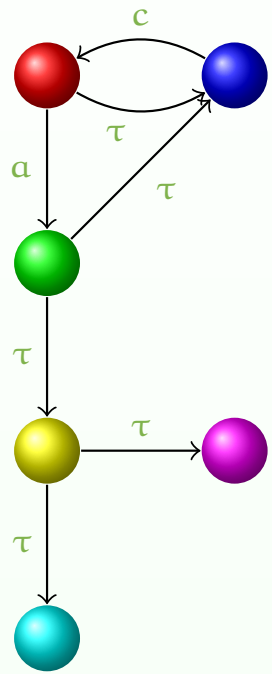
- $(a \rightarrow \texttt{Wait}[u_5]; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $x_1 = 0$ — true
- $(\texttt{Wait}[u_5]_{x_2}; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $0 \leq x_1 \leq u_3 \wedge x_2 = 0$ — true
- $c \rightarrow P$
  true — true
- $(\texttt{Skip}; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $u_5 \leq x_1 \leq u_3$ — $u_5 \leq u_3$
- $(b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $u_5 \leq x_1 \leq u_3$ — $u_5 \leq u_3$
- $c \rightarrow P$
  $u_5 \leq x_1 \wedge x_1 = u_3$ — $u_5 \leq u_3$



An Example (2/2)

$\mathbf{P} \triangleq (\mathtt{a} \rightarrow \mathtt{Wait}[u_5]; \mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]\ \mathtt{c} \rightarrow \mathbf{P}$

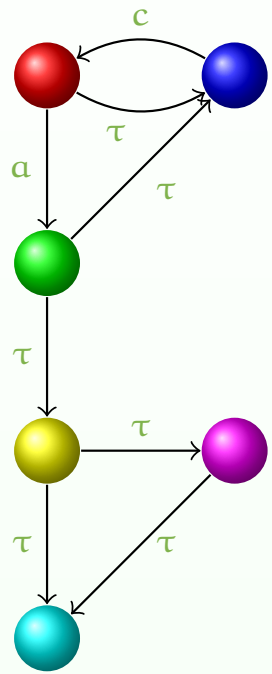
- $(\mathtt{a} \rightarrow \mathtt{Wait}[u_5]; \mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ \mathtt{c} \rightarrow \mathtt{P}$
  $x_1 = 0$ — true
- $(\mathtt{Wait}[u_5]_{x_2}; \mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ \mathtt{c} \rightarrow \mathtt{P}$
  $0 \leq x_1 \leq u_3 \wedge x_2 = 0$ — true
- $\mathtt{c} \rightarrow \mathtt{P}$
  true — true
- $(\mathtt{Skip}; \mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ \mathtt{c} \rightarrow \mathtt{P}$
  $u_5 \leq x_1 \leq u_3$ — $u_5 \leq u_3$
- $(\mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ \mathtt{c} \rightarrow \mathtt{P}$
  $u_5 \leq x_1 \leq u_3$ — $u_5 \leq u_3$
- $\mathtt{c} \rightarrow \mathtt{P}$
  $u_5 \leq u_3$ — $u_5 \leq u_3$



An Example (2/2)

$\mathbf{P} \triangleq (a \rightarrow \texttt{Wait}[u_5]; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]\ c \rightarrow \mathbf{P}$

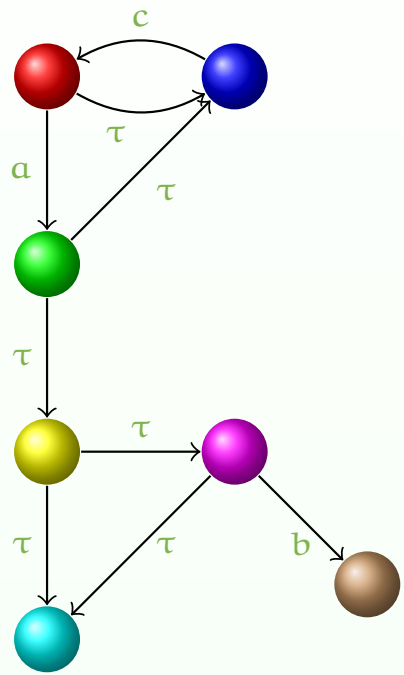
- $(a \rightarrow \texttt{Wait}[u_5]; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $x_1 = 0$ — true
- $(\texttt{Wait}[u_5]_{x_2}; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $0 \leq x_1 \leq u_3 \wedge x_2 = 0$ — true
- $c \rightarrow P$
  true — true
- $(\texttt{Skip}; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $u_5 \leq x_1 \leq u_3$ — $u_5 \leq u_3$
- $(b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $u_5 \leq x_1 \leq u_3$ — $u_5 \leq u_3$
- $c \rightarrow P$
  $u_5 \leq u_3$ — $u_5 \leq u_3$



An Example (2/2)

$\mathbf{P} \triangleq (a \rightarrow \texttt{Wait}[u_5]; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]\ c \rightarrow \mathbf{P}$

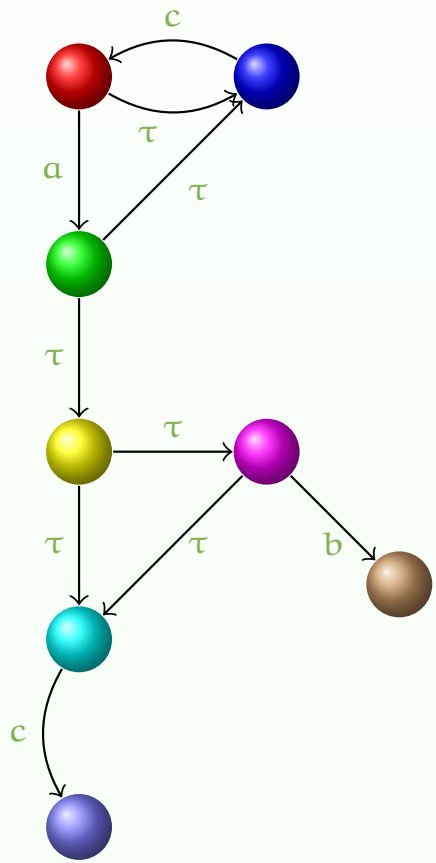
- $(a \rightarrow \texttt{Wait}[u_5]; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $x_1 = 0$ — true
- $(\texttt{Wait}[u_5]_{x_2}; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $0 \leq x_1 \leq u_3 \wedge x_2 = 0$ — true
- $c \rightarrow P$
  true — true
- $(\texttt{Skip}; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $u_5 \leq x_1 \leq u_3$ — $u_5 \leq u_3$
- $(b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $u_5 \leq x_1 \leq u_3$ — $u_5 \leq u_3$
- $c \rightarrow P$
  $u_5 \leq u_3$ — $u_5 \leq u_3$
- $\texttt{Stop}\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $u_5 \leq x_1 \leq u_3$ — $u_5 \leq u_3$



An Example (2/2)

$\mathbf{P} \triangleq (\mathtt{a} \rightarrow \mathtt{Wait}[u_5]; \mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]\ \mathtt{c} \rightarrow \mathbf{P}$

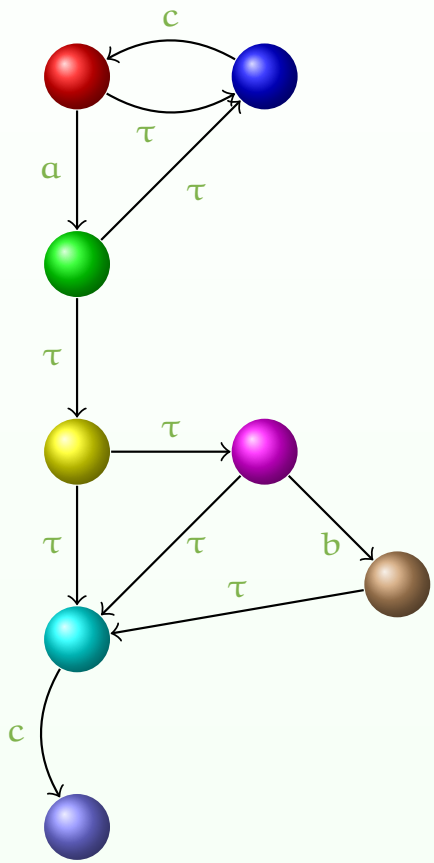
- $(\mathtt{a} \rightarrow \mathtt{Wait}[u_5]; \mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ \mathtt{c} \rightarrow \mathtt{P}$
  $x_1 = 0$ — true
- $(\mathtt{Wait}[u_5]_{x_2}; \mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ \mathtt{c} \rightarrow \mathtt{P}$
  $0 \leq x_1 \leq u_3 \wedge x_2 = 0$ — true
- $\mathtt{c} \rightarrow \mathtt{P}$
  true — true
- $(\mathtt{Skip}; \mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ \mathtt{c} \rightarrow \mathtt{P}$
  $u_5 \leq x_1 \leq u_3$ — $u_5 \leq u_3$
- $(\mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ \mathtt{c} \rightarrow \mathtt{P}$
  $u_5 \leq x_1 \leq u_3$ — $u_5 \leq u_3$
- $\mathtt{c} \rightarrow \mathtt{P}$
  $u_5 \leq u_3$ — $u_5 \leq u_3$
- $\mathtt{Stop}\ \mathtt{interrupt}[u_3]_{x_1}\ \mathtt{c} \rightarrow \mathtt{P}$
  $u_5 \leq x_1 \leq u_3$ — $u_5 \leq u_3$
- $\mathtt{P}$
  $u_5 \leq u_3$ — $u_5 \leq u_3$



An Example (2/2)

$\mathbf{P} \triangleq (\mathtt{a} \rightarrow \mathtt{Wait}[u_5]; \mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]\ \mathtt{c} \rightarrow \mathbf{P}$

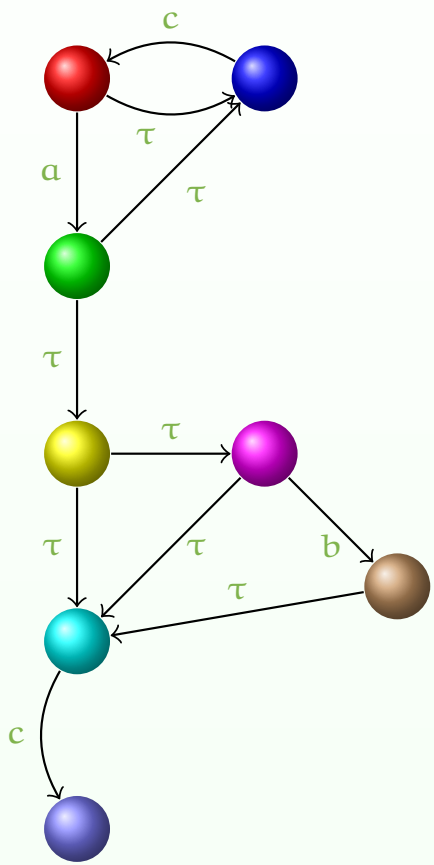
- $(\mathtt{a} \rightarrow \mathtt{Wait}[u_5]; \mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ \mathtt{c} \rightarrow \mathtt{P}$
  $x_1 = 0$ — true
- $(\mathtt{Wait}[u_5]_{x_2}; \mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ \mathtt{c} \rightarrow \mathtt{P}$
  $0 \leq x_1 \leq u_3 \wedge x_2 = 0$ — true
- $\mathtt{c} \rightarrow \mathtt{P}$
  true — true
- $(\mathtt{Skip}; \mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ \mathtt{c} \rightarrow \mathtt{P}$
  $u_5 \leq x_1 \leq u_3$ — $u_5 \leq u_3$
- $(\mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ \mathtt{c} \rightarrow \mathtt{P}$
  $u_5 \leq x_1 \leq u_3$ — $u_5 \leq u_3$
- $\mathtt{c} \rightarrow \mathtt{P}$
  $u_5 \leq u_3$ — $u_5 \leq u_3$
- $\mathtt{Stop}\ \mathtt{interrupt}[u_3]_{x_1}\ \mathtt{c} \rightarrow \mathtt{P}$
  $u_5 \leq x_1 \leq u_3$ — $u_5 \leq u_3$
- $\mathtt{P}$
  $u_5 \leq u_3$ — $u_5 \leq u_3$



An Example (2/2)

$\mathbf{P} \triangleq (a \rightarrow \texttt{Wait}[u_5]; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]\ c \rightarrow \mathbf{P}$

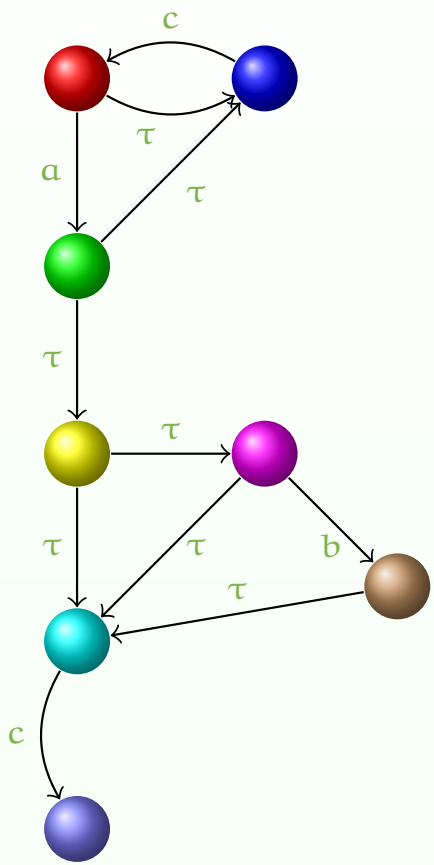
- $(a \rightarrow \texttt{Wait}[u_5]; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $x_1 = 0$ — true
- $(\texttt{Wait}[u_5]_{x_2}; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $0 \leq x_1 \leq u_3 \wedge x_2 = 0$ — true
- $c \rightarrow P$
  true — true
- $(\texttt{Skip}; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $u_5 \leq x_1 \leq u_3$ — $u_5 \leq u_3$
- $(b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $u_5 \leq x_1 \leq u_3$ — $u_5 \leq u_3$
- $c \rightarrow P$
  $u_5 \leq u_3$ — $u_5 \leq u_3$
- $\texttt{Stop}\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $u_5 \leq x_1 \leq u_3$ — $u_5 \leq u_3$
- $(a \rightarrow \texttt{Wait}[u_5]; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]\ c \rightarrow P$
  $u_5 \leq u_3$ — $u_5 \leq u_3$



An Example (2/2)

$\mathbf{P} \triangleq (a \rightarrow \texttt{Wait}[u_5]; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]\ c \rightarrow \mathbf{P}$

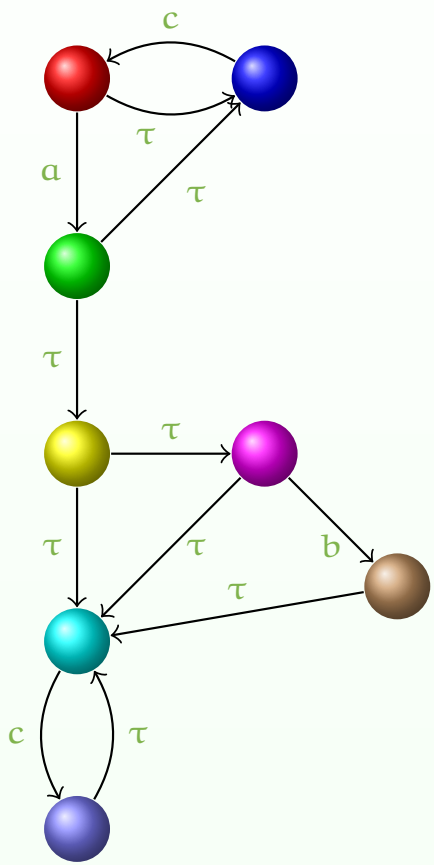
- $(a \rightarrow \texttt{Wait}[u_5]; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $x_1 = 0$ — true
- $(\texttt{Wait}[u_5]_{x_2}; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $0 \leq x_1 \leq u_3 \wedge x_2 = 0$ — true
- $c \rightarrow P$
  true — true
- $(\texttt{Skip}; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $u_5 \leq x_1 \leq u_3$ — $u_5 \leq u_3$
- $(b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $u_5 \leq x_1 \leq u_3$ — $u_5 \leq u_3$
- $c \rightarrow P$
  $u_5 \leq u_3$ — $u_5 \leq u_3$
- $\texttt{Stop}\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $u_5 \leq x_1 \leq u_3$ — $u_5 \leq u_3$
- $(a \rightarrow \texttt{Wait}[u_5]; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $u_5 \leq u_3 \wedge x_1 = 0$ — $u_5 \leq u_3$



An Example (2/2)

$\mathbf{P} \triangleq (a \rightarrow \texttt{Wait}[u_5]; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]\ c \rightarrow \mathbf{P}$

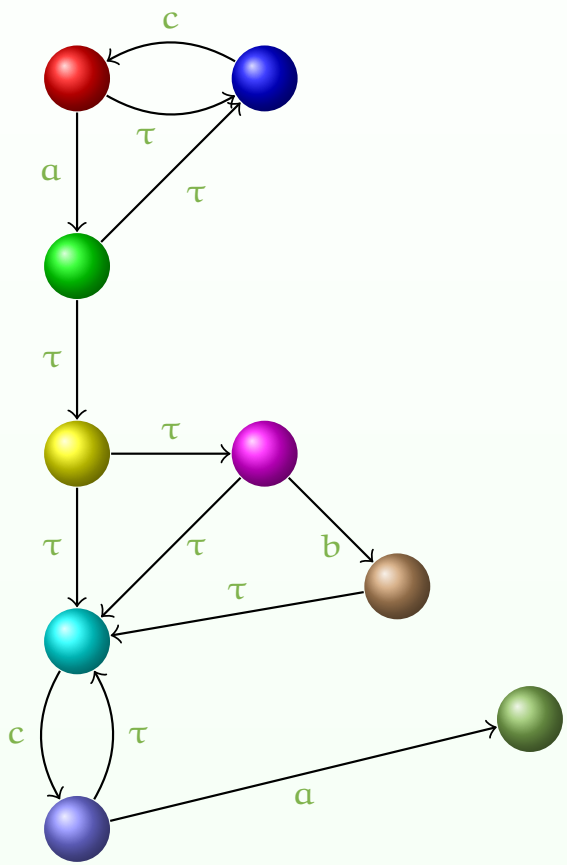
- $(a \rightarrow \texttt{Wait}[u_5]; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $x_1 = 0$ — true
- $(\texttt{Wait}[u_5]_{x_2}; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $0 \leq x_1 \leq u_3 \wedge x_2 = 0$ — true
- $c \rightarrow P$
  true — true
- $(\texttt{Skip}; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $u_5 \leq x_1 \leq u_3$ — $u_5 \leq u_3$
- $(b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $u_5 \leq x_1 \leq u_3$ — $u_5 \leq u_3$
- $c \rightarrow P$
  $u_5 \leq u_3$ — $u_5 \leq u_3$
- $\texttt{Stop}\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $u_5 \leq x_1 \leq u_3$ — $u_5 \leq u_3$
- $(a \rightarrow \texttt{Wait}[u_5]; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $u_5 \leq u_3 \wedge x_1 = 0$ — $u_5 \leq u_3$



An Example (2/2)

$\mathbf{P} \triangleq (a \rightarrow \texttt{Wait}[u_5]; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]\ c \rightarrow \mathbf{P}$

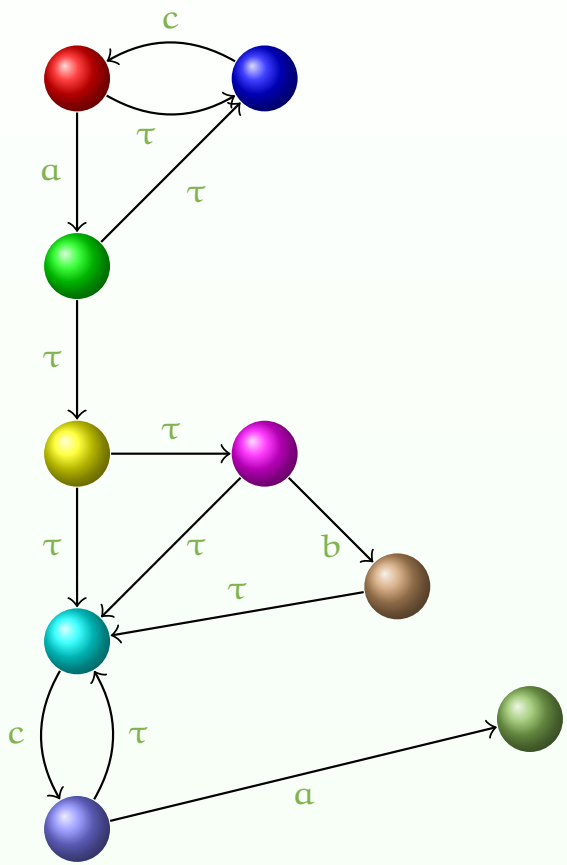
- $(a \rightarrow \texttt{Wait}[u_5]; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $x_1 = 0$ — true
- $(\texttt{Wait}[u_5]_{x_2}; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $0 \leq x_1 \leq u_3 \wedge x_2 = 0$ — true
- $c \rightarrow P$
  true — true
- $(\texttt{Skip}; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $u_5 \leq x_1 \leq u_3$ — $u_5 \leq u_3$
- $(b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $u_5 \leq x_1 \leq u_3$ — $u_5 \leq u_3$
- $c \rightarrow P$
  $u_5 \leq u_3$ — $u_5 \leq u_3$
- $\texttt{Stop}\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $u_5 \leq x_1 \leq u_3$ — $u_5 \leq u_3$
- $(a \rightarrow \texttt{Wait}[u_5]; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $u_5 \leq u_3 \wedge x_1 = 0$ — $u_5 \leq u_3$
- $(\texttt{Wait}[u_5]\ ; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $0 \leq x_1 \leq u_3 \wedge u_5 \leq u_3$ — $u_5 \leq u_3$



An Example (2/2)

$\mathbf{P} \triangleq (a \rightarrow \texttt{Wait}[u_5]; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]\ c \rightarrow \mathbf{P}$

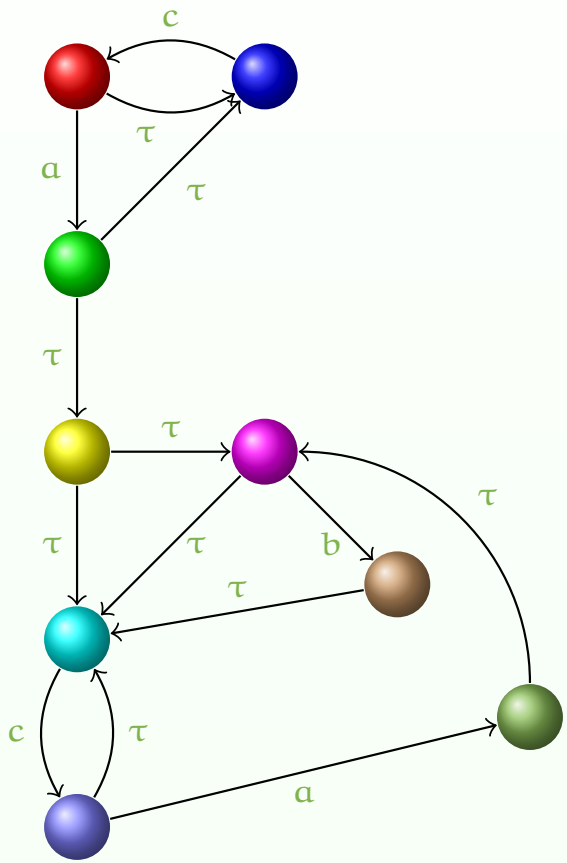
- $(a \rightarrow \texttt{Wait}[u_5]; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $x_1 = 0$ — true
- $(\texttt{Wait}[u_5]_{x_2}; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $0 \leq x_1 \leq u_3 \wedge x_2 = 0$ — true
- $c \rightarrow P$
  true — true
- $(\texttt{Skip}; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $u_5 \leq x_1 \leq u_3$ — $u_5 \leq u_3$
- $(b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $u_5 \leq x_1 \leq u_3$ — $u_5 \leq u_3$
- $c \rightarrow P$
  $u_5 \leq u_3$ — $u_5 \leq u_3$
- $\texttt{Stop}\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $u_5 \leq x_1 \leq u_3$ — $u_5 \leq u_3$
- $(a \rightarrow \texttt{Wait}[u_5]; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $u_5 \leq u_3 \wedge x_1 = 0$ — $u_5 \leq u_3$
- $(\texttt{Wait}[u_5]_{x_2}; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $0 \leq x_1 \leq u_3 \wedge u_5 \leq u_3 \wedge x_2 = 0$ — $u_5 \leq u_3$



An Example (2/2)

$\mathbf{P} \triangleq (a \rightarrow \texttt{Wait}[u_5]; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]\ c \rightarrow \mathbf{P}$

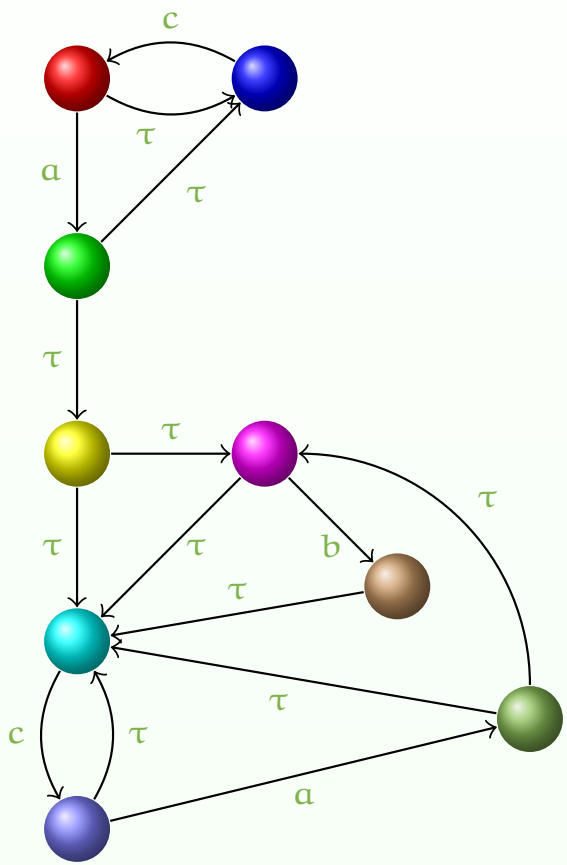
- $(a \rightarrow \texttt{Wait}[u_5]; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $x_1 = 0$ — true
- $(\texttt{Wait}[u_5]_{x_2}; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $0 \leq x_1 \leq u_3 \wedge x_2 = 0$ — true
- $c \rightarrow P$
  true — true
- $(\texttt{Skip}; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $u_5 \leq x_1 \leq u_3$ — $u_5 \leq u_3$
- $(b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $u_5 \leq x_1 \leq u_3$ — $u_5 \leq u_3$
- $c \rightarrow P$
  $u_5 \leq u_3$ — $u_5 \leq u_3$
- $\texttt{Stop}\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $u_5 \leq x_1 \leq u_3$ — $u_5 \leq u_3$
- $(a \rightarrow \texttt{Wait}[u_5]; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $u_5 \leq u_3 \wedge x_1 = 0$ — $u_5 \leq u_3$
- $(\texttt{Wait}[u_5]_{x_2}; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $0 \leq x_1 \leq u_3 \wedge u_5 \leq u_3 \wedge x_2 = 0$ — $u_5 \leq u_3$



An Example (2/2)

$\mathbf{P} \triangleq (a \rightarrow \texttt{Wait}[u_5]; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]\ c \rightarrow \mathbf{P}$

- $(a \rightarrow \texttt{Wait}[u_5]; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $x_1 = 0$ — true
- $(\texttt{Wait}[u_5]_{x_2}; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $0 \leq x_1 \leq u_3 \wedge x_2 = 0$ — true
- $c \rightarrow P$
  true — true
- $(\texttt{Skip}; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $u_5 \leq x_1 \leq u_3$ — $u_5 \leq u_3$
- $(b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $u_5 \leq x_1 \leq u_3$ — $u_5 \leq u_3$
- $c \rightarrow P$
  $u_5 \leq u_3$ — $u_5 \leq u_3$
- $\texttt{Stop}\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $u_5 \leq x_1 \leq u_3$ — $u_5 \leq u_3$
- $(a \rightarrow \texttt{Wait}[u_5]; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $u_5 \leq u_3 \wedge x_1 = 0$ — $u_5 \leq u_3$
- $(\texttt{Wait}[u_5]_{x_2}; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $0 \leq x_1 \leq u_3 \wedge u_5 \leq u_3 \wedge x_2 = 0$ — $u_5 \leq u_3$



Outline

Expressiveness of PSTCSP

- Timed CSP equivalent to closed timed ϵ-automata [Ouaknine and Worrell, 2003]
  - Stricly less expressive than Timed ϵ-Automata
  - Incomparable with classical Timed Automata

- Corollary: Parametric Stateful Timed CSP is as expressive as Parametric Closed Timed ϵ-automata
  - Incomparable with classical Parametric Timed Automata (PTAs)

- Expressive enough
  - Most well-known protocols can be easily modeled using PSTCSP

Decidability of Membership for PSTCSP

- Membership question:
  Is a parameter valuation consistent with a process?

- Decidable (and easy)
  1. Instantiate the process with the parameter valuation
  2. Apply techniques for (non-parametric) Stateful Timed CSP [Sun et al., 2009]

Definition of Emptiness in PSTCSP

- Emptiness question:
  "Does there exist a parameter valuation consistent with a process?"
- Unclear definition of consistency in ((P)ST)CSP
  - For Timed Automata: acceptance of at least a timed word
  - But no notion of acceptance in CSP
- Suggestion for the definition of consistency
  - "Does there exist a timed word such that a process derives to another given process?"
  - More specifically: halting problem
    "Does there exist a timed word such that a process derives to Stop?"

Undecidability of Emptiness for PSTCSP

Theorem

The problem of deciding whether a PSTCSP model is empty is undecidable.

Two possible proofs:

- Encoding of a 2-counter machine
- Equivalence to a subset of PTAs, for which the emptiness problem is also undecidable

Undecidability of Parameter Synthesis

Corollary

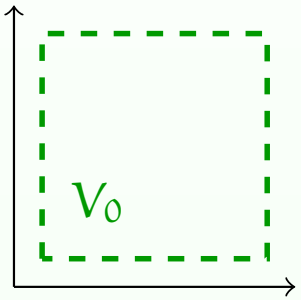
Parameter synthesis is undecidable in general for PSTCSP.

Outline

Algorithms for Parameter Synthesis

- Parameter synthesis: guarantees that the system will behave well w.r.t. a given property

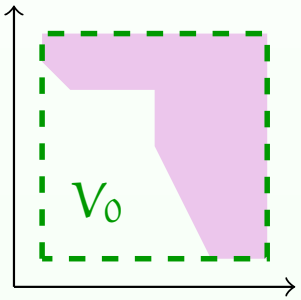
- The good parameters problem
  - "Given a bounded parameter domain V_0, find a set of parameter valuations of good behavior in V_0"



Algorithms for Parameter Synthesis

- Parameter synthesis: guarantees that the system will behave well w.r.t. a given property

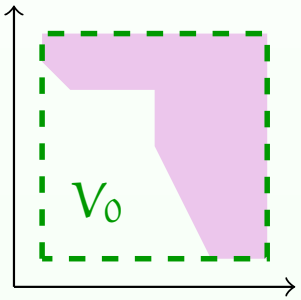
- The good parameters problem
  - "Given a bounded parameter domain V_0, find a set of parameter valuations of good behavior in V_0"



Algorithms for Parameter Synthesis

- Parameter synthesis: guarantees that the system will behave well w.r.t. a given property

- The good parameters problem
  - "Given a bounded parameter domain V_0, find a set of parameter valuations of good behavior in V_0"



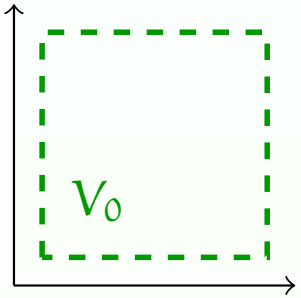
- Design of semi-algorithms
  - Termination not guaranteed because undecidable problem
  - Nevertheless, some methods terminate "more often" than others

Computation of the Reachability Graph

- Idea: compute all possible configurations
  - Algorithm *reachAll*
- No guarantee to terminate!

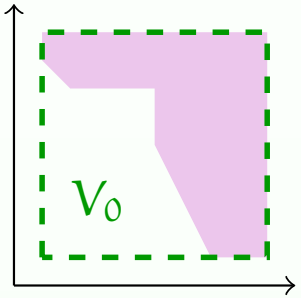
Inverse Method for PSTCSP

- The good parameters problem
  - "Given a bounded parameter domain V_0, find a set of parameter valuations of good behavior in V_0"



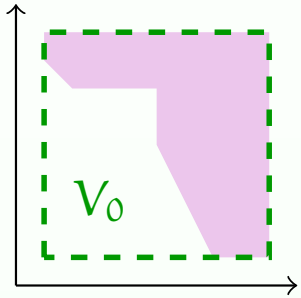
Inverse Method for PSTCSP

- The good parameters problem
  - "Given a bounded parameter domain V_0, find a set of parameter valuations of good behavior in V_0"

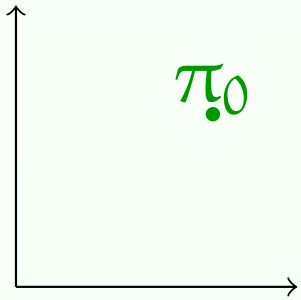


Inverse Method for PSTCSP

- The good parameters problem
  - "Given a bounded parameter domain V_0, find a set of parameter valuations of good behavior in V_0"

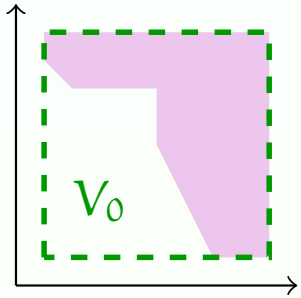


- The inverse problem
  - "Given a reference parameter valuation π_0, find other valuations around π_0 of same behavior"

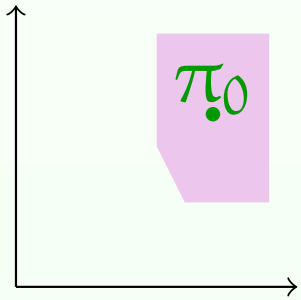


Inverse Method for PSTCSP

- The good parameters problem
  - "Given a bounded parameter domain V_0, find a set of parameter valuations of good behavior in V_0"



- The inverse problem
  - "Given a reference parameter valuation π_0, find other valuations around π_0 of same behavior"



Inverse Method for PSTCSP: Main Idea

- Idea of *IM*
  - Initially defined for Parametric Timed Automata [André et al., 2009]
  - On-the-fly computation of the reachable configurations (e.g., using breadth first search algorithm)
  - When the constraint associated to a configuration does not satisfy π_0, negate an inequality and add it to all configurations, so that this configuration is removed
  - Return the intersection of the constraints associated to all configurations

Inverse Method for PSTCSP: Example

Input

$\mathbf{P} \triangleq (\mathbf{a} \rightarrow \mathtt{Wait}[\mathbf{u_5}]; \mathbf{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[\mathbf{u_3}]\ \mathbf{c} \rightarrow \mathbf{P}$

$\pi_0 : \{\mathbf{u_3} = \mathbf{3} \wedge \mathbf{u_5} = \mathbf{5}\}$

Output

$\mathrm{K} = \mathtt{true}$

Inverse Method for PSTCSP: Example

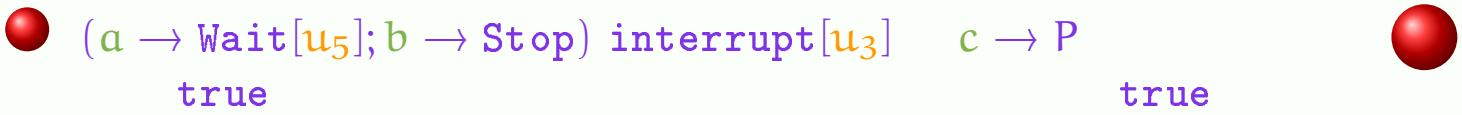
Input

$\mathbf{P} \triangleq (\mathtt{a} \rightarrow \mathtt{Wait}[u_5]; \mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]\ \mathtt{c} \rightarrow \mathbf{P}$

$\pi_0 : \{u_3 = 3 \wedge u_5 = 5\}$

Output

$\mathrm{K} = \mathtt{true}$



Inverse Method for PSTCSP: Example

Input

$\mathbf{P} \triangleq (\mathtt{a} \rightarrow \mathtt{Wait}[\mathtt{u_5}]; \mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[\mathtt{u_3}]\ \mathtt{c} \rightarrow \mathbf{P}$

$\pi_0 : \{\mathbf{u_3 = 3 \wedge u_5 = 5}\}$

Output

$K = \mathtt{true}$

$(\mathtt{a} \rightarrow \mathtt{Wait}[\mathtt{u_5}]; \mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[\mathtt{u_3}]_{x_1}\ \mathtt{c} \rightarrow \mathtt{P}$

$x_1 = 0$ $\qquad\qquad$ true

Inverse Method for PSTCSP: Example

Input

$\mathbf{P} \triangleq (\mathtt{a} \rightarrow \mathtt{Wait}[\mathbf{u_5}]; \mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[\mathbf{u_3}]\ \mathtt{c} \rightarrow \mathbf{P}$

$\pi_0 : \{\mathbf{u_3} = \mathbf{3} \wedge \mathbf{u_5} = \mathbf{5}\}$

Output

$\mathrm{K} = \mathtt{true}$

$(\mathtt{a} \rightarrow \mathtt{Wait}[u_5]; \mathtt{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ \mathtt{c} \rightarrow \mathrm{P}$

$x_1 = 0$

$\pi_0 \models \mathtt{true}$

Inverse Method for PSTCSP: Example

Input

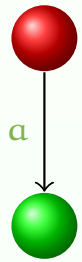
$\mathbf{P} \triangleq (\mathbf{a} \rightarrow \texttt{Wait}[\mathbf{u_5}]; \mathbf{b} \rightarrow \texttt{Stop})\ \texttt{interrupt}[\mathbf{u_3}]\ \mathbf{c} \rightarrow \mathbf{P}$

$\pi_0 : \{\mathbf{u_3} = \mathbf{3} \wedge \mathbf{u_5} = \mathbf{5}\}$

Output

$K = \texttt{true}$

- $(a \rightarrow \texttt{Wait}[u_5]; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $x_1 = 0$ $\qquad \pi_0 \models \texttt{true}$
- $(\texttt{Wait}[u_5]\ ; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $0 \leq x_1 \leq u_3$ $\qquad \texttt{true}$



Inverse Method for PSTCSP: Example

Input

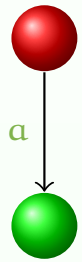
$\mathbf{P} \triangleq (\mathbf{a} \rightarrow \texttt{Wait}[\mathbf{u_5}]; \mathbf{b} \rightarrow \texttt{Stop})\ \texttt{interrupt}[\mathbf{u_3}]\ \mathbf{c} \rightarrow \mathbf{P}$

$\pi_0 : \{\mathbf{u_3} = \mathbf{3} \wedge \mathbf{u_5} = \mathbf{5}\}$

Output

$K = \texttt{true}$

- $(a \rightarrow \texttt{Wait}[u_5]; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $x_1 = 0$ $\quad \pi_0 \models \texttt{true}$
- $(\texttt{Wait}[u_5]_{x_2}; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $0 \leq x_1 \leq u_3 \wedge x_2 = 0$ $\quad \texttt{true}$



Inverse Method for PSTCSP: Example

Input

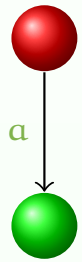
$\mathbf{P} \triangleq (\mathbf{a} \rightarrow \texttt{Wait}[\mathbf{u_5}]; \mathbf{b} \rightarrow \texttt{Stop})\ \texttt{interrupt}[\mathbf{u_3}]\ \mathbf{c} \rightarrow \mathbf{P}$

$\pi_0 : \{\mathbf{u_3} = \mathbf{3} \wedge \mathbf{u_5} = \mathbf{5}\}$

Output

$K = \texttt{true}$

- $(a \rightarrow \texttt{Wait}[u_5]; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $x_1 = 0$ $\quad \pi_0 \models \texttt{true}$
- $(\texttt{Wait}[u_5]_{x_2}; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $0 \leq x_1 \leq u_3 \wedge x_2 = 0$ $\quad \pi_0 \models \texttt{true}$



Inverse Method for PSTCSP: Example

Input

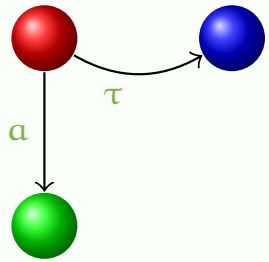
$\mathbf{P} \triangleq (\mathbf{a} \rightarrow \texttt{Wait}[\mathbf{u_5}]; \mathbf{b} \rightarrow \texttt{Stop})\ \texttt{interrupt}[\mathbf{u_3}]\ \mathbf{c} \rightarrow \mathbf{P}$

$\pi_0 : \{\mathbf{u_3} = \mathbf{3} \wedge \mathbf{u_5} = \mathbf{5}\}$

Output

$K = \texttt{true}$

- $(a \rightarrow \texttt{Wait}[u_5]; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $x_1 = 0$ $\quad \pi_0 \models \texttt{true}$
- $(\texttt{Wait}[u_5]_{x_2}; b \rightarrow \texttt{Stop})\ \texttt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $0 \leq x_1 \leq u_3 \wedge x_2 = 0$ $\quad \pi_0 \models \texttt{true}$
- $c \rightarrow P$
  $x_1 \geq 0 \wedge x_1 = u_3$ $\quad \texttt{true}$



Inverse Method for PSTCSP: Example

Input

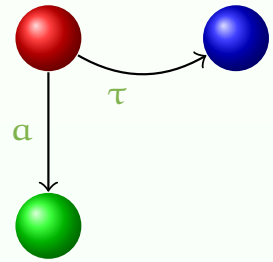
$\mathbf{P} \triangleq (\mathbf{a} \rightarrow \mathtt{Wait}[\mathbf{u_5}]; \mathbf{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[\mathbf{u_3}]\ \mathbf{c} \rightarrow \mathbf{P}$

$\pi_0 : \{\mathbf{u_3} = \mathbf{3} \wedge \mathbf{u_5} = \mathbf{5}\}$

Output

$K = \mathtt{true}$

- $(a \rightarrow \mathtt{Wait}[u_5]; b \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $x_1 = 0$ $\quad \pi_0 \models \mathtt{true}$
- $(\mathtt{Wait}[u_5]_{x_2}; b \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $0 \leq x_1 \leq u_3 \wedge x_2 = 0$ $\quad \pi_0 \models \mathtt{true}$
- $c \rightarrow P$
  $\mathtt{true}$ $\quad \mathtt{true}$



Inverse Method for PSTCSP: Example

Input

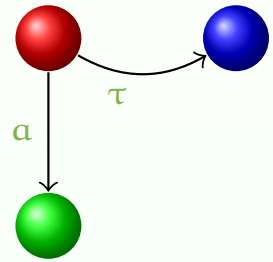
$\mathbf{P} \triangleq (\mathbf{a} \rightarrow \mathtt{Wait}[\mathbf{u_5}]; \mathbf{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[\mathbf{u_3}]\ \mathbf{c} \rightarrow \mathbf{P}$

$\pi_0 : \{\mathbf{u_3} = \mathbf{3} \wedge \mathbf{u_5} = \mathbf{5}\}$

Output

$K = \mathtt{true}$

- $(a \rightarrow \mathtt{Wait}[u_5]; b \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $x_1 = 0$ $\quad \pi_0 \models \mathtt{true}$
- $(\mathtt{Wait}[u_5]_{x_2}; b \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $0 \leq x_1 \leq u_3 \wedge x_2 = 0$ $\quad \pi_0 \models \mathtt{true}$
- $c \rightarrow P$
  $\mathtt{true}$ $\quad \pi_0 \models \mathtt{true}$



Inverse Method for PSTCSP: Example

Input

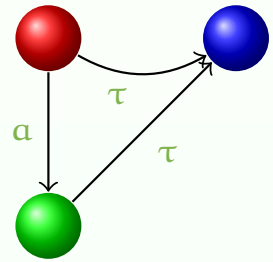
$\mathbf{P} \triangleq (\mathbf{a} \rightarrow \mathtt{Wait}[\mathbf{u_5}]; \mathbf{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[\mathbf{u_3}]\ \mathbf{c} \rightarrow \mathbf{P}$

$\pi_0 : \{\mathbf{u_3} = \mathbf{3} \wedge \mathbf{u_5} = \mathbf{5}\}$

Output

$K = \mathtt{true}$

- $(a \rightarrow \mathtt{Wait}[u_5]; b \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $x_1 = 0$ $\quad \pi_0 \models \mathtt{true}$
- $(\mathtt{Wait}[u_5]_{x_2}; b \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $0 \leq x_1 \leq u_3 \wedge x_2 = 0$ $\quad \pi_0 \models \mathtt{true}$
- $c \rightarrow P$
  $\mathtt{true}$ $\quad \pi_0 \models \mathtt{true}$



Inverse Method for PSTCSP: Example

Input

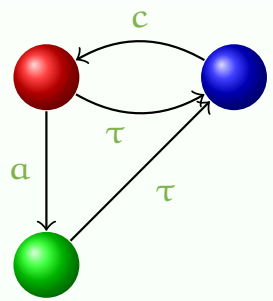
$\mathbf{P} \triangleq (\mathbf{a} \rightarrow \mathtt{Wait}[\mathbf{u_5}]; \mathbf{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[\mathbf{u_3}]\ \mathbf{c} \rightarrow \mathbf{P}$

$\pi_0 : \{\mathbf{u_3} = \mathbf{3} \wedge \mathbf{u_5} = \mathbf{5}\}$

Output

$K = \mathtt{true}$

- $(a \rightarrow \mathtt{Wait}[u_5]; b \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $x_1 = 0$ $\quad \pi_0 \models \mathtt{true}$
- $(\mathtt{Wait}[u_5]_{x_2}; b \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $0 \leq x_1 \leq u_3 \wedge x_2 = 0$ $\quad \pi_0 \models \mathtt{true}$
- $c \rightarrow P$
  $\mathtt{true}$ $\quad \pi_0 \models \mathtt{true}$



Inverse Method for PSTCSP: Example

Input

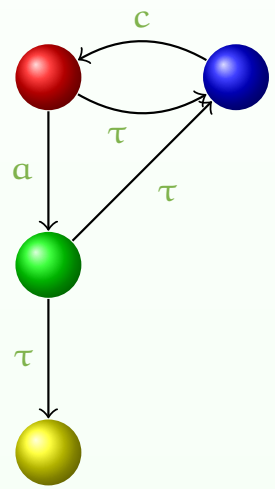
$\mathbf{P} \triangleq (\mathbf{a} \rightarrow \mathtt{Wait}[\mathbf{u_5}]; \mathbf{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[\mathbf{u_3}]\ \mathbf{c} \rightarrow \mathbf{P}$

$\pi_0 : \{\mathbf{u_3} = \mathbf{3} \wedge \mathbf{u_5} = \mathbf{5}\}$

Output

$K = \mathtt{true}$

- $(a \rightarrow \mathtt{Wait}[u_5]; b \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $x_1 = 0$ $\quad \pi_0 \models \mathtt{true}$
- $(\mathtt{Wait}[u_5]_{x_2}; b \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $0 \leq x_1 \leq u_3 \wedge x_2 = 0$ $\quad \pi_0 \models \mathtt{true}$
- $c \rightarrow P$
  $\mathtt{true}$ $\quad \pi_0 \models \mathtt{true}$
- $(\mathtt{Skip}; b \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $u_5 \leq x_1 \leq u_3$ $\quad u_5 \leq u_3$



Inverse Method for PSTCSP: Example

Input

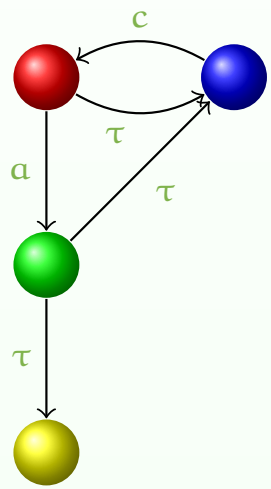
$\mathbf{P} \triangleq (\mathbf{a} \rightarrow \mathtt{Wait}[\mathbf{u_5}]; \mathbf{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[\mathbf{u_3}]\ \mathbf{c} \rightarrow \mathbf{P}$

$\pi_0 : \{\mathbf{u_3} = \mathbf{3} \wedge \mathbf{u_5} = \mathbf{5}\}$

Output

$K = \mathtt{true}$

- $(a \rightarrow \mathtt{Wait}[u_5]; b \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $x_1 = 0$ $\quad \pi_0 \models \mathtt{true}$
- $(\mathtt{Wait}[u_5]_{x_2}; b \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $0 \leq x_1 \leq u_3 \wedge x_2 = 0$ $\quad \pi_0 \models \mathtt{true}$
- $c \rightarrow P$
  $\mathtt{true}$ $\quad \pi_0 \models \mathtt{true}$
- $(\mathtt{Skip}; b \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $u_5 \leq x_1 \leq u_3$ $\quad \pi_0 \not\models u_5 \leq u_3$



Inverse Method for PSTCSP: Example

Input

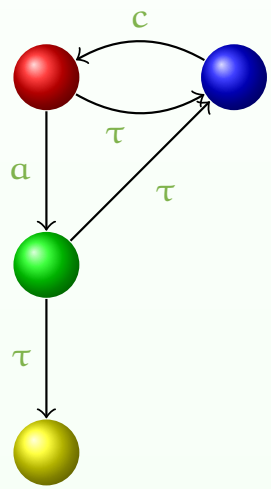
$\mathbf{P} \triangleq (\mathbf{a} \rightarrow \mathtt{Wait}[\mathbf{u_5}]; \mathbf{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[\mathbf{u_3}]\ \mathbf{c} \rightarrow \mathbf{P}$

$\pi_0 : \{\mathbf{u_3} = \mathbf{3} \wedge \mathbf{u_5} = \mathbf{5}\}$

Output

$K = u_5 > u_3$

- $(a \rightarrow \mathtt{Wait}[u_5]; b \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $x_1 = 0$ $\quad \pi_0 \models \mathtt{true}$
- $(\mathtt{Wait}[u_5]_{x_2}; b \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $0 \leq x_1 \leq u_3 \wedge x_2 = 0$ $\quad \pi_0 \models \mathtt{true}$
- $c \rightarrow P$
  $\mathtt{true}$ $\quad \pi_0 \models \mathtt{true}$
- $(\mathtt{Skip}; b \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $u_5 \leq x_1 \leq u_3$ $\quad \pi_0 \not\models u_5 \leq u_3$



Inverse Method for PSTCSP: Example

Input

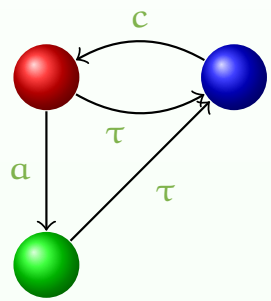
$\mathbf{P} \triangleq (\mathbf{a} \rightarrow \mathtt{Wait}[\mathbf{u_5}]; \mathbf{b} \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[\mathbf{u_3}]\ \mathbf{c} \rightarrow \mathbf{P}$

$\pi_0 : \{\mathbf{u_3} = \mathbf{3} \wedge \mathbf{u_5} = \mathbf{5}\}$

Output

$K = u_5 > u_3$

- $(a \rightarrow \mathtt{Wait}[u_5]; b \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $x_1 = 0$ $\quad \pi_0 \models \mathtt{true}$
- $(\mathtt{Wait}[u_5]_{x_2}; b \rightarrow \mathtt{Stop})\ \mathtt{interrupt}[u_3]_{x_1}\ c \rightarrow P$
  $0 \leq x_1 \leq u_3 \wedge x_2 = 0$ $\quad \pi_0 \models \mathtt{true}$
- $c \rightarrow P$
  $\mathtt{true}$ $\quad \pi_0 \models \mathtt{true}$



Inverse Method for PSTCSP: Properties

- Preserves properties on traces (LTL formulae)
  - From the equality of trace sets
  - Advantage: quantify robustness of the system
- Termination
  - Better termination than other methods
  - Not guaranteed for PTAs (proved)
  - Not guaranteed for PSTCSP
    (...but no counter-example found)
- Completeness
  - "Given π, if a process under π behaves like under π_0, then π belongs to the constraint synthesized by the method"
  - Not guaranteed for PSTCSP

Outline

Implementation of the Algorithms

- Implementation in PSyHCoS
  - Parameter Synthesis for Hierarchical Concurrent Systems
- Computation of the reachability graph
  - ☺ Interesting for small examples
    - ⇝ Manual synthesis of parameters from the graph
  - ☹ Often leads to an infinite state space
    - ⇝ Does not terminate (no synthesis possible)
- Synthesis using the inverse method
  - ☺ Partial exploration of the state space only
  - ☺ Always terminate in practice

Encoding of a configuration

- Encoding
  - Process (ID)
  - Value for variables
  - List of clocks
  - Constraint: definition of a normal form
- Example
  - $(\mathtt{Wait}[u_3]_{x_3} || \mathtt{Wait}[u_5]_{x_3} || \mathtt{Wait}[u_5]_{x_2}, x_3 \leq x_2)$
  - Encoding:
    - Process: $\mathtt{Wait}[u_3] || \mathtt{Wait}[u_5] || \mathtt{Wait}[u_5]$
    - List of clocks: $\{x_3, x_3, x_2\}$
    - Constraint: $x_3 \leq x_2$
- Justification for the list of clocks
  - Distinguishes between $(\mathtt{Wait}[u_3]_{x_3} || \mathtt{Wait}[u_5]_{x_3} || \mathtt{Wait}[u_5]_{x_2}, x_3 \leq x_2)$ and $(\mathtt{Wait}[u_3]_{x_2} || \mathtt{Wait}[u_5]_{x_3} || \mathtt{Wait}[u_5]_{x_2}, x_3 \leq x_2)$

Encoding of a configuration: optimization

- Actual equivalence between
  $(\texttt{Wait}[u_3]_{x_1} \| \texttt{Wait}[u_5]_{x_2}, x_1 \leq x_2)$ and
  $(\texttt{Wait}[u_3]_{x_2} \| \texttt{Wait}[u_5]_{x_1}, x_2 \leq x_1)$

Encoding of a configuration: optimization

- Actual equivalence between
  $(\mathtt{Wait}[u_3]_{x_1} || \mathtt{Wait}[u_5]_{x_2}, x_1 \leq x_2)$ and
  $(\mathtt{Wait}[u_3]_{x_2} || \mathtt{Wait}[u_5]_{x_1}, x_2 \leq x_1)$
- Idea $\rightsquigarrow$ rename clocks
  - Example: $(\mathtt{Wait}[u_3]_{x_3} || \mathtt{Wait}[u_5]_{x_3} || \mathtt{Wait}[u_5]_{x_2}, x_3 \leq x_2)$
    New encoding:
    - Process: $\mathtt{Wait}[u_3] || \mathtt{Wait}[u_5] || \mathtt{Wait}[u_5]$
    - List of clocks: $\{x_1, x_1, x_2\}$
    - Constraint: $x_1 \leq x_2$
- This method is time consuming
  - Numerous string and list sorts
  - But often leads to efficient state space reduction

Case studies

Case study	|U|	*reachAll* |S|	|T|	|X|	t	*reachAll+* |S|	|T|	|X|	t	*IM* |S|	|X|	t	*IM+* |S|	|X|	t
Bridge	4	-	-	-	M.O.	-	-	-	M.O.	2.8k	2	253	2.8k	2	455
Fischer_4	2	-	-	-	M.O.	-	-	-	M.O.	11k	4	41.9	2k	4	8.65
Fischer_5	2	-	-	-	M.O.	-	-	-	M.O.	133k	5	1176	13k	5	84.5
Fischer_6	2	-	-	-	M.O.	-	-	-	M.O.	-	-	M.O.	86k	6	1144
Jobshop	8	14k	20k	2	21.0	12k	17k	2	18.1	1112	2	17.1	877	2	22.8
RCS_5	4	5.6k	7.2k	4	10.5	5.6k	7.2k	4	9.54	5.6k	4	7.83	5.6k	4	16.7
RCS_6	4	34k	43k	4	91.7	34k	43k	4	54.5	34k	4	60.4	34k	4	91.3
TrAHV	6	7.2k	13k	6	14.2	7.2k	13k	6	15.8	227	6	0.555	227	6	0.655

- *reachAll*: computation of the reachability graph
- *IM*: inverse method
- *reachAll+* (resp. *IM+*): version with optimized encoding

Outline

Conclusion

- Parametric Stateful Timed CSP
  - Extension of (Timed) CSP
  - Powerful and intuitive language for specification of hierarchical concurrent systems
- Algorithms for parameter synthesis
  - Full reachability method: does not often terminate in practice
  - Inverse method: allows efficient parameter synthesis
    - Quantify the robustness to the system
- State space reduction
  - Normal form for configurations using clock renaming

Future Work

- Theoretical questions
  - Equivalence of timed constructs
  - Termination of the inverse method for PSTCSP

- More complex parameter synthesis
  - Synthesis w.r.t. a predicate on the variables
  - Synthesis w.r.t. refinement (parametric refinement checking)
  - Parametric model checking (LTL, CTL, TCTL properties)

References I

Alur, R. and Dill, D. L. (1994).
A theory of timed automata.
TCS, 126(2):183–235.

André, É., Chatain, T., Encrenaz, E., and Fribourg, L. (2009).
An inverse method for parametric timed automata.
International Journal of Foundations of Computer Science, 20(5):819–836.

Hoare, C. (1978).
Communicating sequential processes.
Commun. ACM, 21:666–677.

Merlin, P. M. (1974).
A study of the recoverability of computing systems.
PhD thesis, University of California, Irvine.

Ouaknine, J. and Worrell, J. (2003).
Timed CSP = closed timed ϵ-automata.
Nordic J. of Computing, 10:99–133.

Schneider, S. (2000).
Concurrent and Real-time Systems.
John Wiley and Sons.

References II

Sun, J., Liu, Y., Dong, J., and Zhang, X. (2009).
Verifying stateful timed CSP using implicit clocks and zone abstraction.
In *ICFEM'09*, volume 5885 of *LNCS*, pages 581–600. Springer.