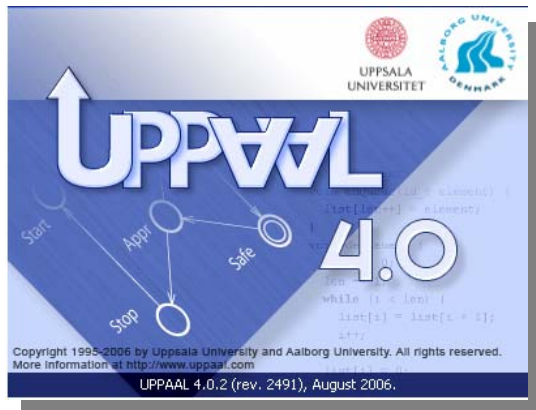


# Playing Games with Timed Interfaces

--

## Towards a Formal Design Methodology for Real-Time Systems



TIGA

Kim Guldstrand Larsen  
with

Thomas Chatain, Alexandre David,  
Ulrik Nyman, Andrzej Wasowski

# Overview

- Timed Games: Review
- Specification Theory
- Timed I/O Games
- Refinement Checking    as games    using TIGA
- Consistency Checking    as games    using TIGA
- Composability Checking    as games    using TIGA
- Future Challenges

# Timed Games

## Reachability / Safety Games

Strategy:

$$F : Q \rightarrow E_c \cup \lambda$$

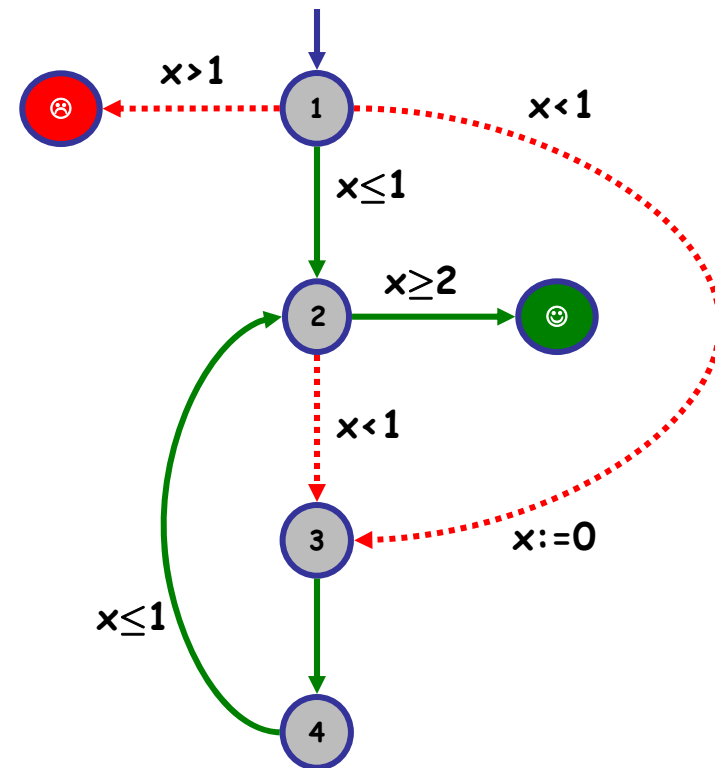
Winning Run:

$$\text{States}(\rho) \cap G \neq \emptyset$$

$$\text{States}(\rho) \cap G = \emptyset$$

Winning Strategy:

$$\text{Runs}(F) \subseteq \text{WinRuns}$$



.....> Uncontrollable

——> Controllable

# Timed Games

Strategy:

$$F : Q \rightarrow E_c \cup \lambda$$

Winning Run:

$$\text{States}(\rho) \cap G \neq \emptyset$$

$$\text{States}(\rho) \cap G = \emptyset$$

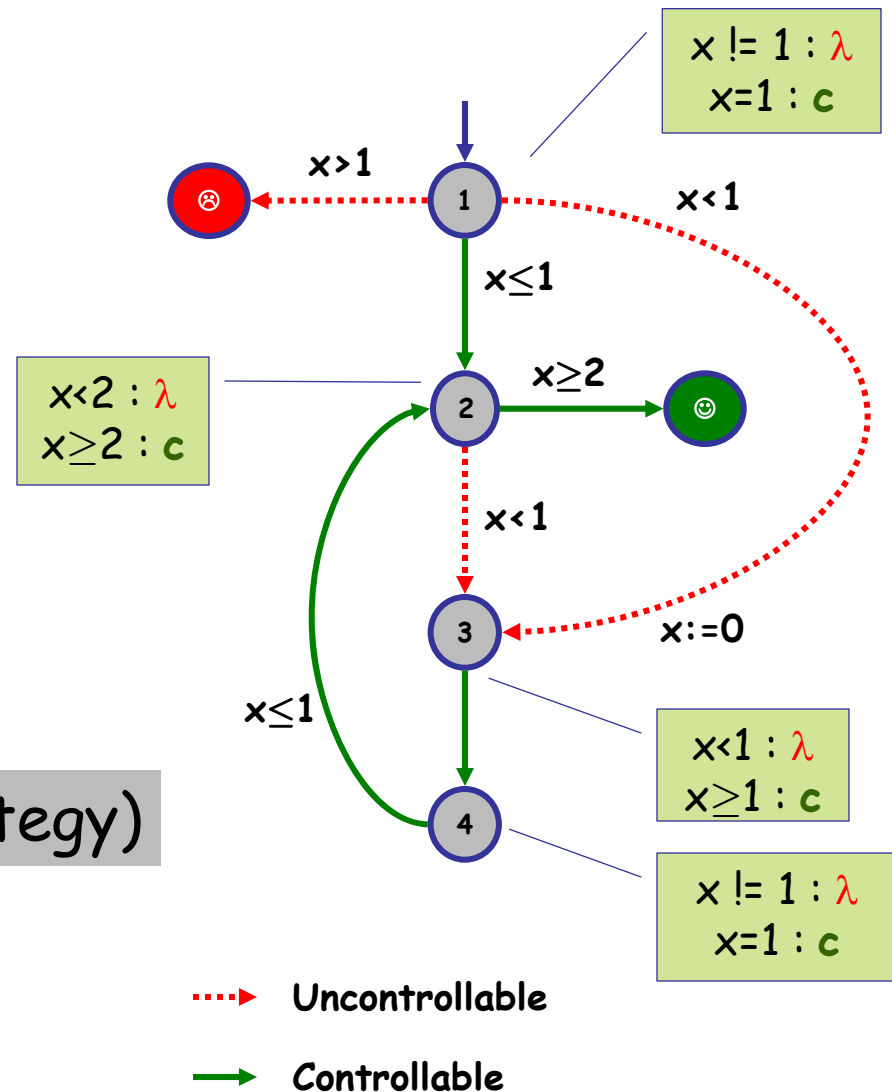
Winning Strategy:

$$\text{Runs}(F) \subseteq \text{WinRuns}$$

**Winning (memoryless) strategy)**

control:  $A \leftrightarrow \text{😊}$

Reachability / Safety Games



# UPPAAL Tiga

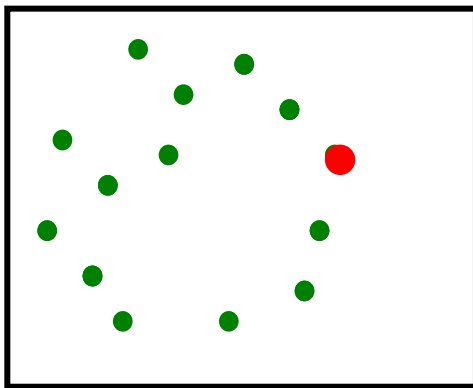
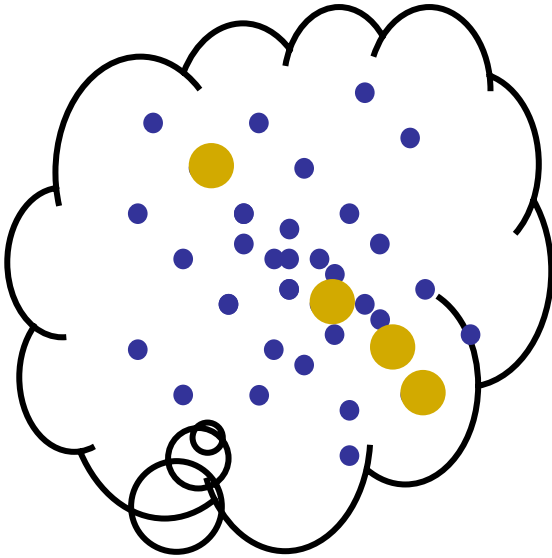
The screenshot displays the UPPAAL simulator interface. The main window title is "C:/Documents and Settings/kg/Desktop/DESKTOP FEB 2007/UPPAAL/uppaal-tiga-0.12/demo/concur05.xml - UPPAAL". The interface is divided into several panels:

- Transition chooser:** A panel on the left showing a list of transitions. The "Main" transition is selected. Below the list, there is a "Delay:" field set to 0.57 and a "Reset" button. A "Take transition" button is also present.
- Trace controls:** A panel below the transition chooser with buttons for "First", "Prev", "Play", "Next", and "Last". A "Speeder" slider is set to a middle position between "Slow" and "Fast". A "Random simulation" button is at the bottom.
- Main diagram:** A state transition diagram with five states: L0 (blue), L1 (red), L2 (blue), L3 (blue), and L4 (pink). A green state labeled "goal" is also present. Transitions are labeled with guard conditions:
  - L0 to L1:  $x \leq 1$  (green)
  - L0 to L4:  $x > 1$  (green)
  - L1 to goal:  $x \geq 2$  (green)
  - L1 to L2:  $x < 1$  (green)
  - L2 to L3:  $x \leq 1$  (green)
  - L3 to L1:  $x < 1$  (green)
  - L0 to L2:  $x = 0$  (green)
  - L0 to L1:  $x \leq 2$  (pink)
  - L1 to L0:  $x < 1$  (green)
- Drag out:** A panel on the right showing the current state of the simulation:  $t(0) = 0$  and  $\text{Main.x} = 0.570000$ .

CCONCUR05, CAV07, FORMATS07

# Specification Theory

Imp: set of implementations



Spec: set of specifications

Specification Formalism

$$\text{SPF} = (\text{Imp}, \text{Spec}, \text{sat})$$

where

$$\text{sat} \subseteq \text{Imp} \times \text{Spec}$$

$$|S| = \{ I : I \text{ sat } S \}$$

Refinement :

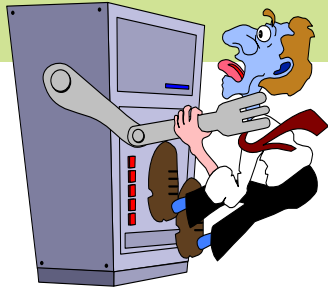
$$S \triangleleft T \text{ iff } |S| \subseteq |T|$$

Consistency :

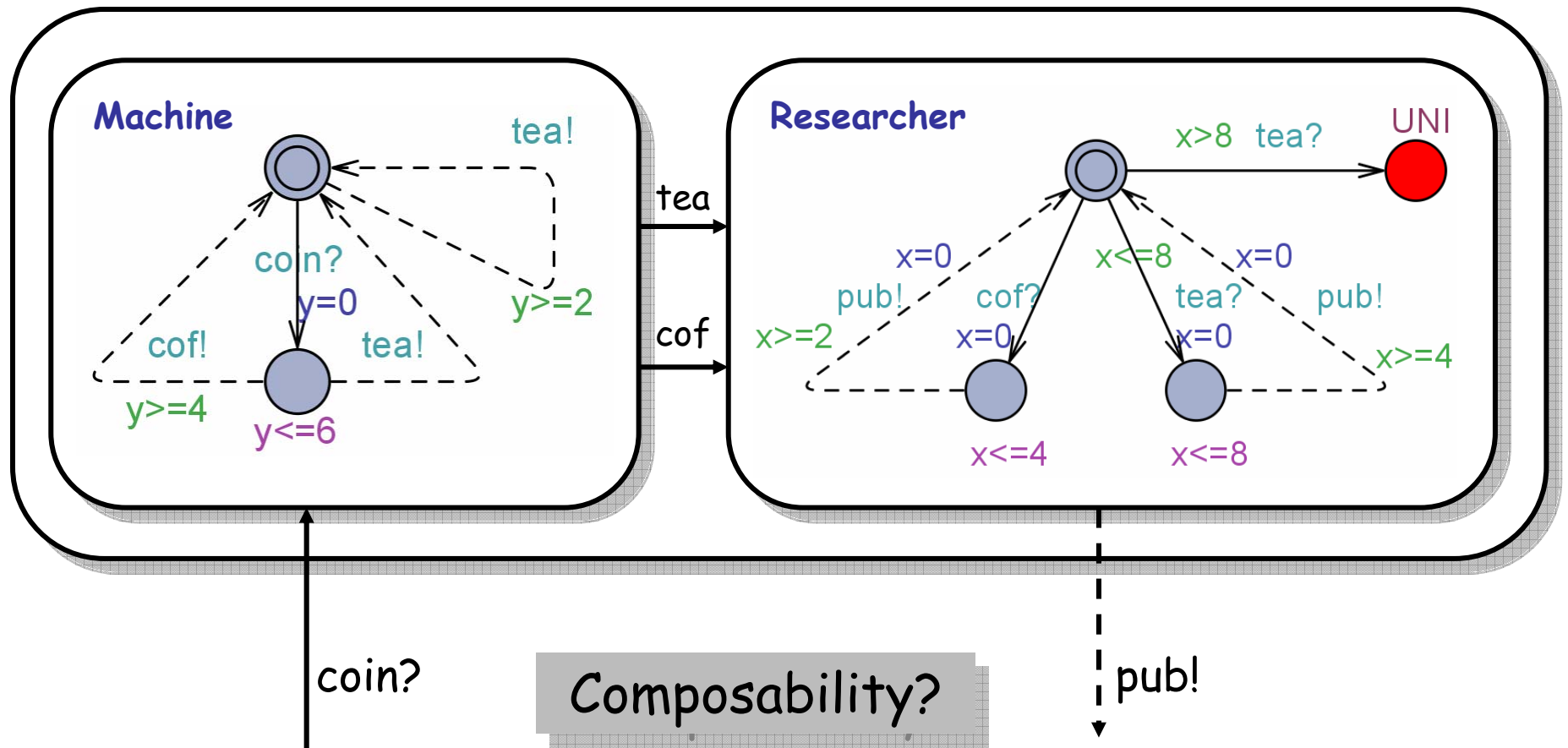
$$|S| \neq \emptyset$$

$$|S| \cap |T| \neq \emptyset$$

# Timed Interface Specifications = Timed I/O Games (Modal Transition Sys)



Input: controllable (required)  
Output: uncontrollable (allowed)



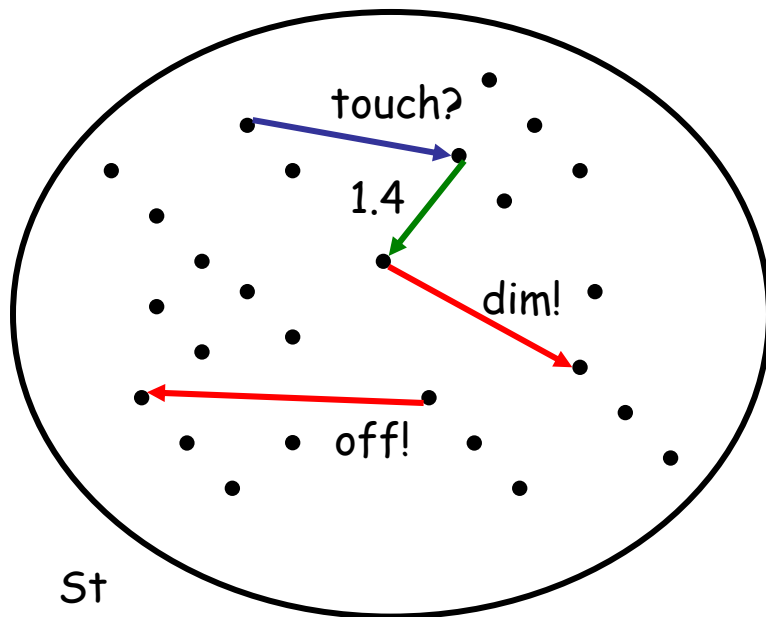
# Timed I/O Transition Systems

TIOTS:

$(St, Act, \rightarrow)$

where  $\rightarrow: St \times (Act \cup \mathbb{R}) \times St$

and  $Act = \Sigma_i \cup \Sigma_o$



Time determinism ( $d \in \mathbb{R}$ )

*if  $s \xrightarrow{d} s'$  and  $s \xrightarrow{d} s''$  then  $s' = s''$*

Input enabledness

*for all  $s$  and  $i \in \Sigma_i$ .  $s \xrightarrow{i}$*

Time divergence

*whenever  $s \xrightarrow{d_0} \xrightarrow{a_0} \xrightarrow{d_1} \xrightarrow{a_1} \dots$   
then  $\sum_{i \geq 0} d_i = \infty$*

Determinism ( $a \in Act \cup \mathbb{R}$ )

*if  $s \xrightarrow{a} s'$  and  $s \xrightarrow{a} s''$  then  $s' = s''$*

Output urgency

*whenever  $s \xrightarrow{o}$*

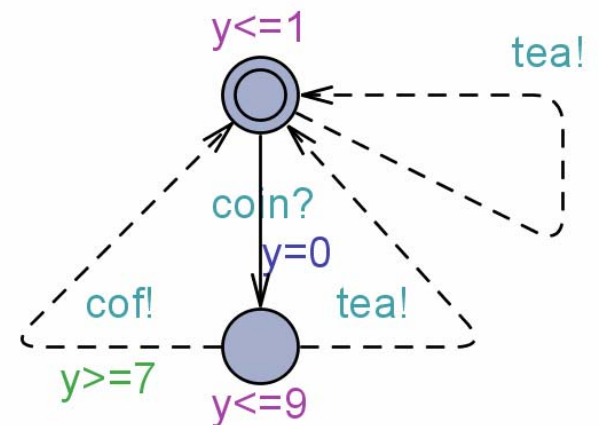
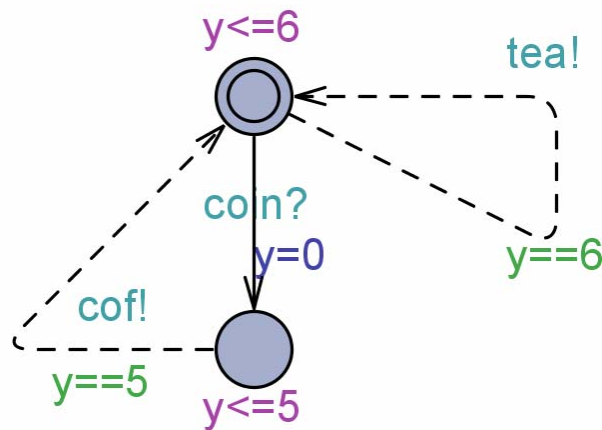
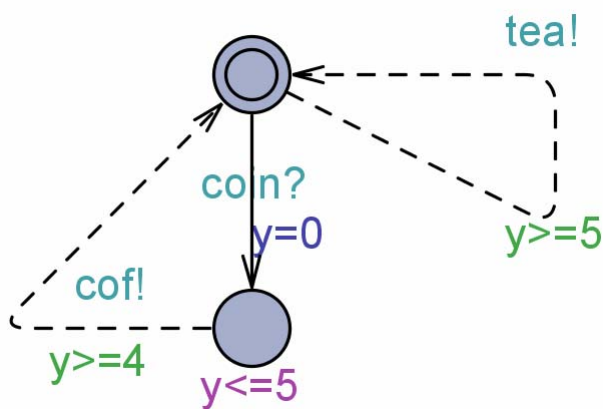
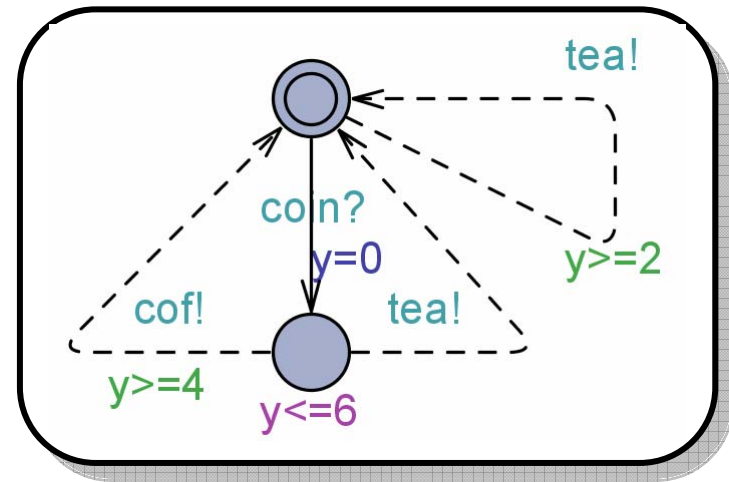
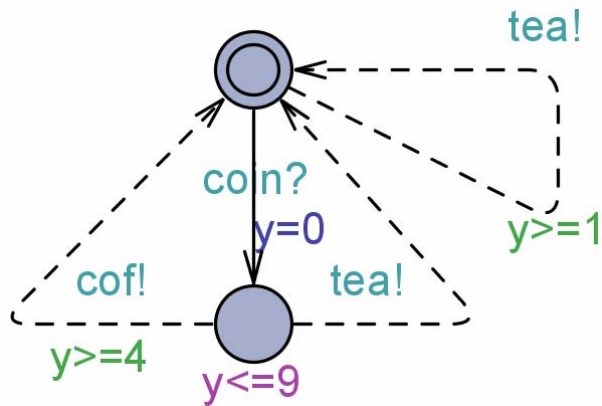
*then  $s \xrightarrow{d}$  implies  $d = 0$*

Isolated outputs

*If  $s \xrightarrow{o}$  and  $s \xrightarrow{o'}$  then  $o = o'$*



# Refinements, Implementations, Consistency



# Timed Refinement = Timed Alternating Simulation

Let  $S$  and  $T$  be TIOGA.

$S \leq T$  iff

- i.  $T \xrightarrow{i?} T'$  then  $S \xrightarrow{i?} S'$  with  $S' \leq T'$
- ii.  $S \xrightarrow{o!} S'$  then  $T \xrightarrow{o!} T'$  with  $S' \leq T'$
- iii.  $S \xrightarrow{d} S'$  then  $T \xrightarrow{d} T'$  with  $S' \leq T'$

Intuition:

$S$  leaves less choices than  $T$   
for an implementation.

Definition:

$$I \text{ sat } S \Leftrightarrow^{\Delta} I \leq S$$

Theorem

Whenever  $S \leq T$  then  $|S| \subseteq |T|$

Conjecture

Whenever  $|S| \subseteq |T|$  then  $S \leq T$

Theorem

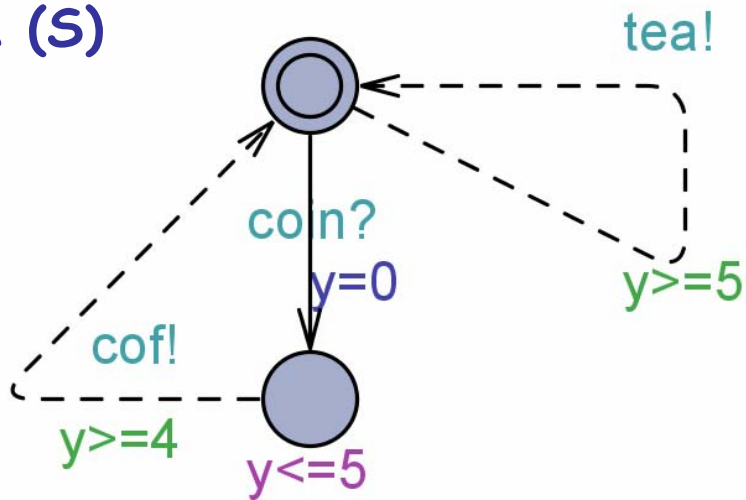
Whenever  $S$  and  $T$  are deterministic  
then  $S \leq T \Leftrightarrow \text{TTr}(S) \subseteq \text{TTr}(T)$

Theorem

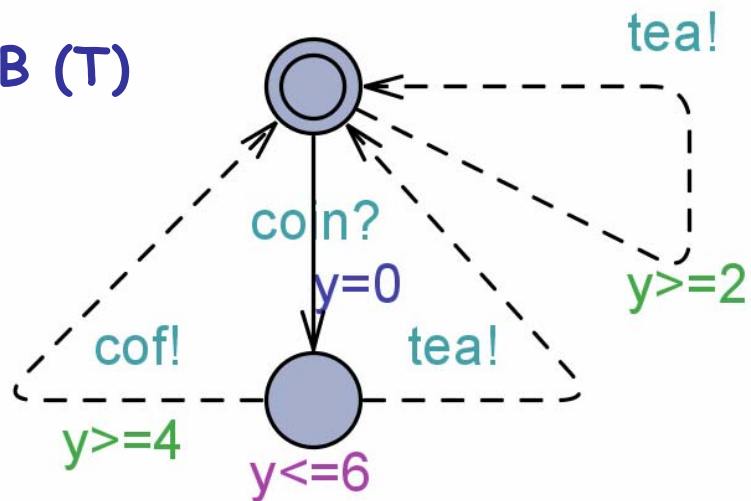
$S \leq T \Rightarrow$   
 $(\forall \Phi \in \text{ATCTL}. T \text{ cntr } \Phi \Rightarrow S \text{ cntr } \Phi)$

# Refinement (example)

A (S)



B (T)

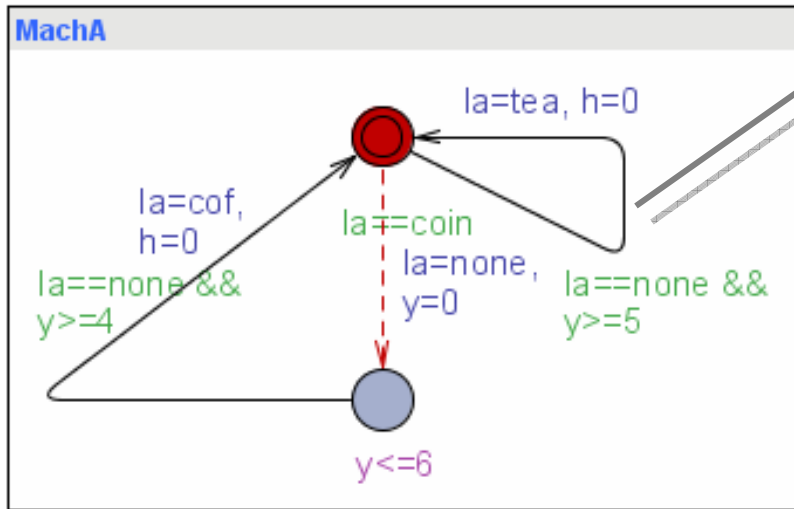


Let  $S$  and  $T$  be TIOGA.

$S \prec T$  iff

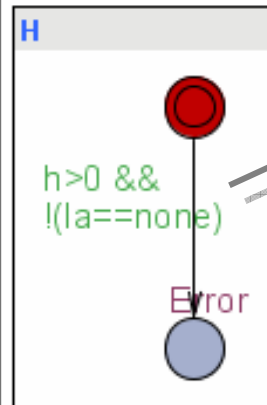
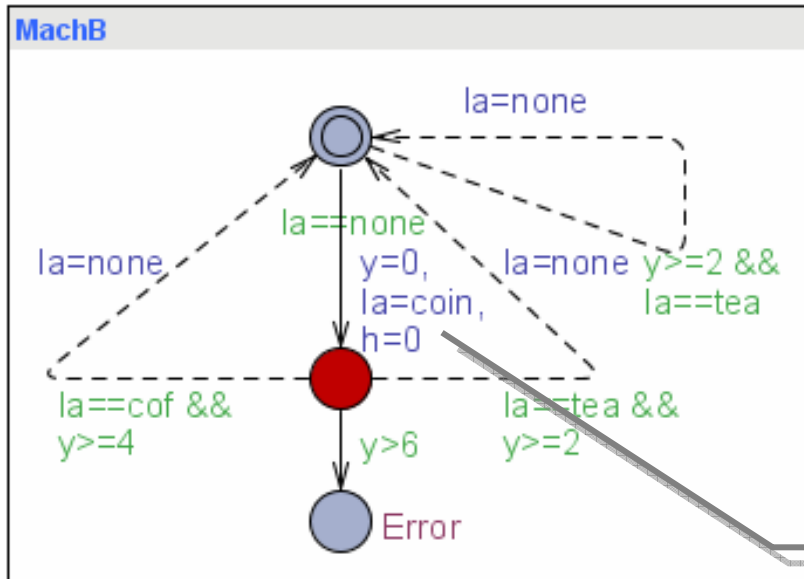
- i.  $T \xrightarrow{i?} T'$  then  $S \xrightarrow{i?} S'$  with  $S' \leq T'$
- ii.  $S \xrightarrow{o!} S'$  then  $T \xrightarrow{o!} T'$  with  $S' \leq T'$
- iii.  $S \xrightarrow{d} S'$  then  $T \xrightarrow{d} T'$  with  $S' \leq T'$

# Refinement Checking as a Game



Challenging on outputs and delays

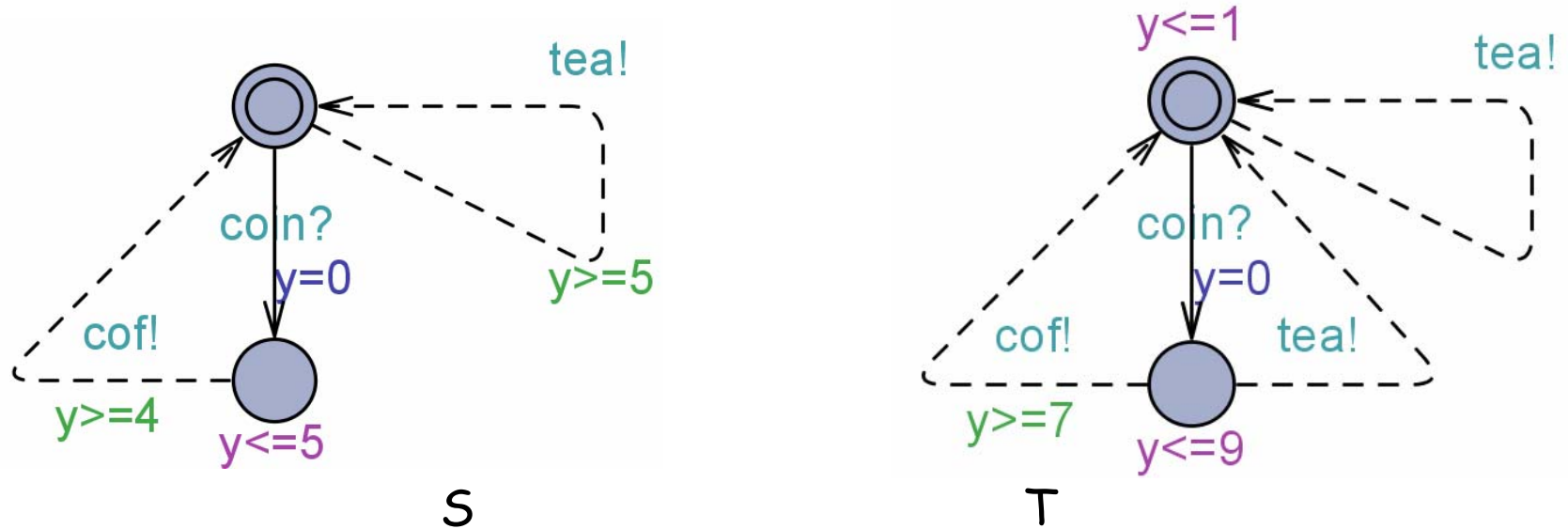
not  $A \leq B$   
 iff  
 $\text{MachA} \mid \text{MachB} \mid H \text{ sat}$   
 control:  $A \leftrightarrow \text{Error}$



Checking that responses are made immediately

Challenging on inputs

# Consistency

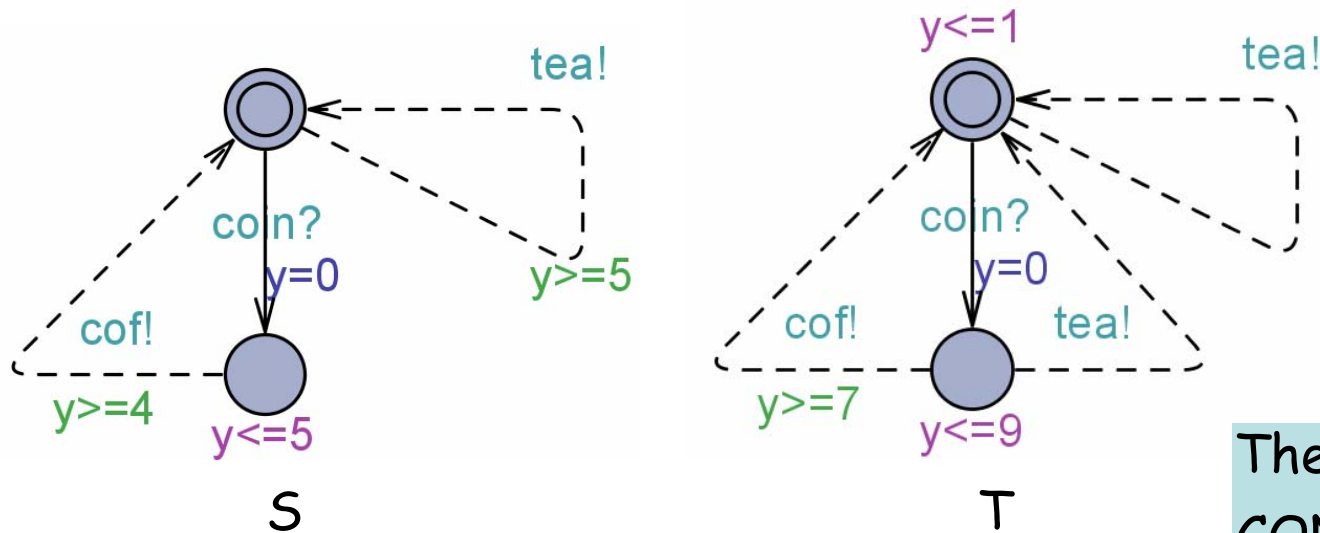


Consistency:

Does there exist  $I$  such that

$I \leq S$  and  $I \leq T$ ?

# Consistency



Theorem  
 $CONS(S, T)$  iff  
 S and T are consistent.

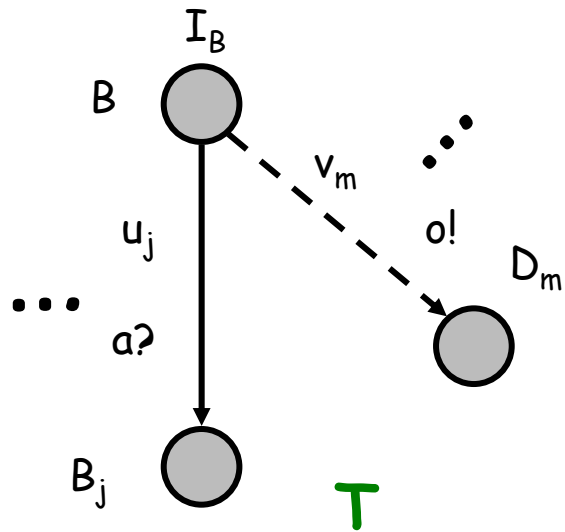
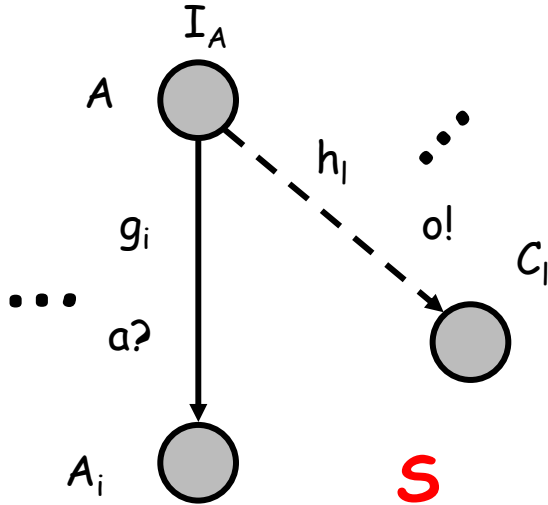
Let  $s$  be a state of  $S$  and  $t$  a state of  $T$ .

Define  $CONS$  as the largest relation such that whenever  $CONS(s, t)$  then

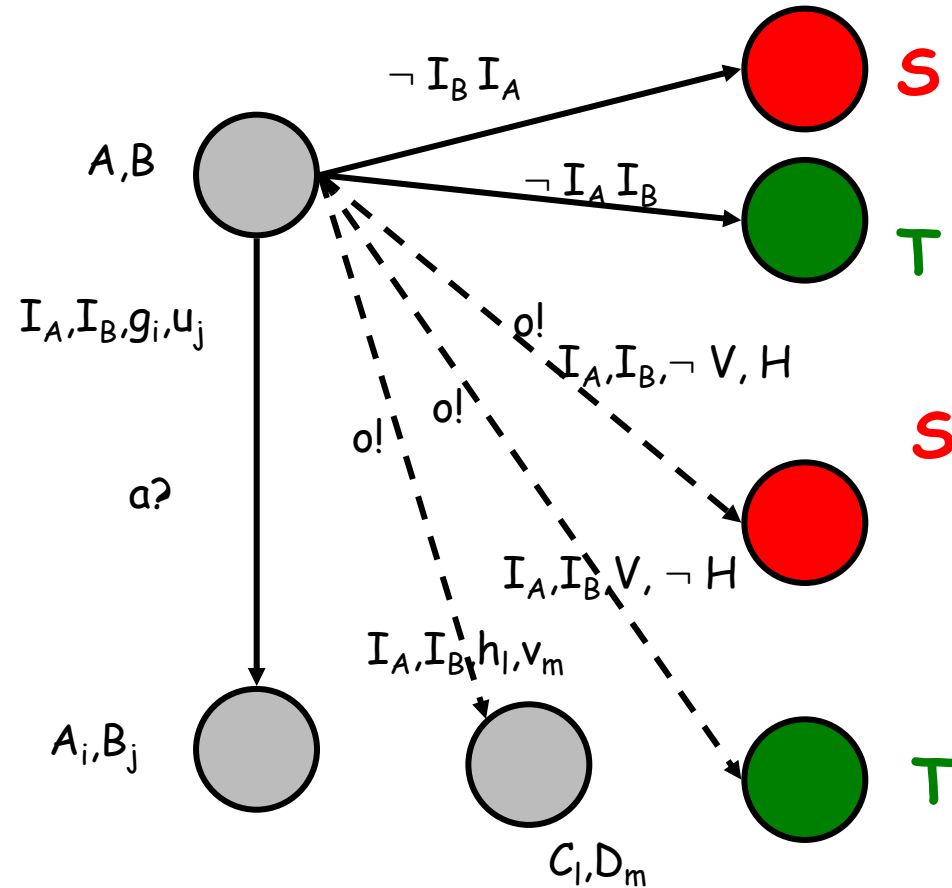
$$i. \forall i. (s \xrightarrow{i?} s' \wedge t \xrightarrow{i?} t') \Rightarrow CONS(s', t')$$

$$ii. (\exists \sigma \in \Sigma_0 \cup \mathcal{R}. s \xrightarrow{\sigma} v \wedge t \xrightarrow{\sigma} w) \Rightarrow \\ (\exists \sigma \in \Sigma_0 \cup \mathcal{R}. s \xrightarrow{\sigma} s' \wedge t \xrightarrow{\sigma} t' \wedge CONS(s', t'))$$

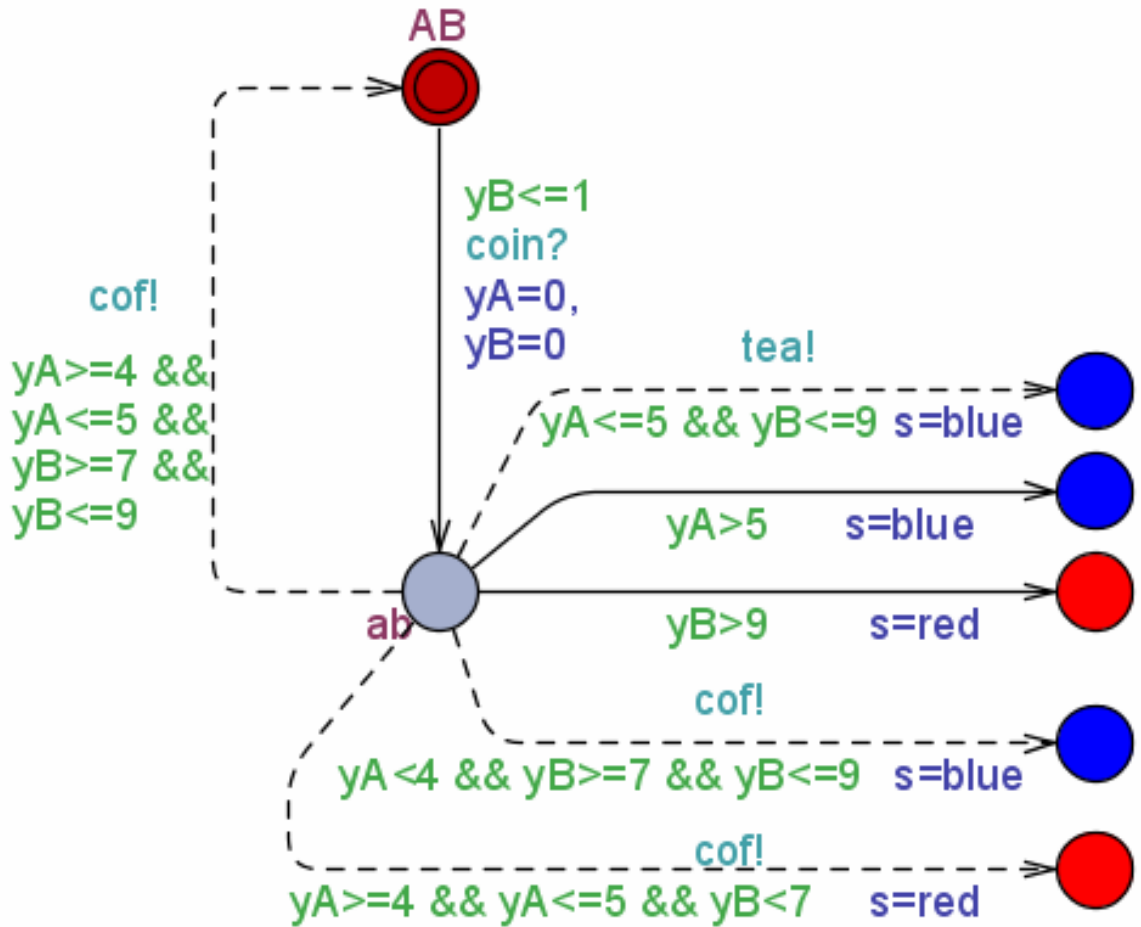
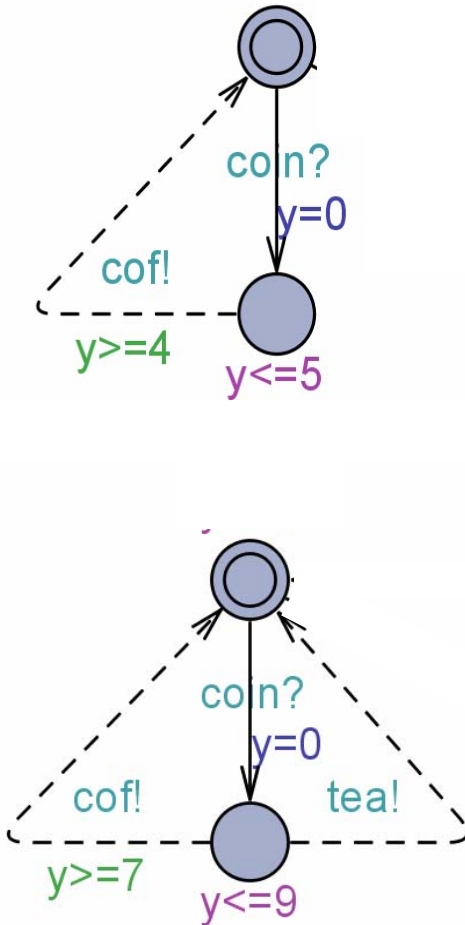
# Consistency Checking as a Game



S and T are inconsistent iff  
 $S \times T$  satisfies  
 control:  $A \ltimes (T \text{ or } S)$ .

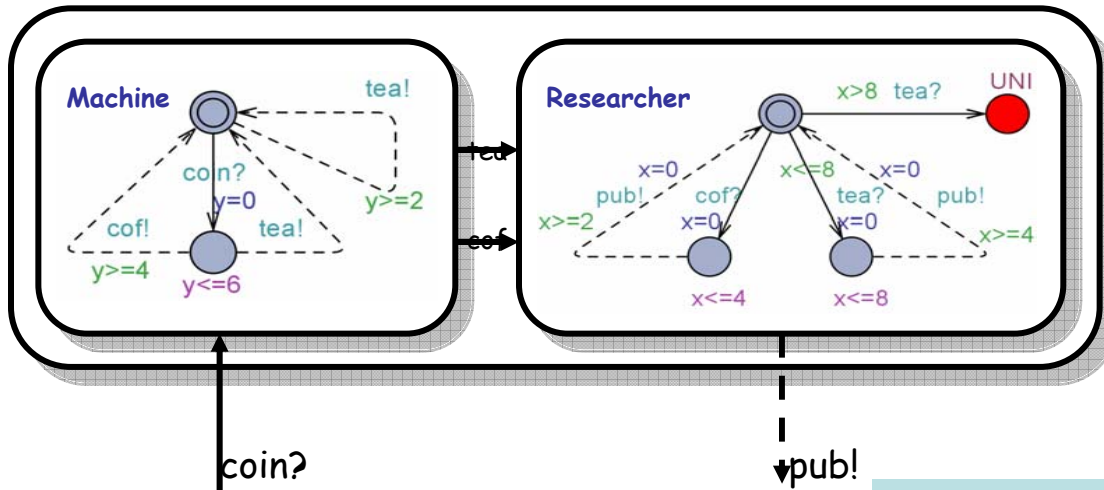


# Consistency Checking - Example





# Composition of Timed Interfaces



Classical rules for Composition of I/O transition systems

## Theorem

If  $A_1 \leq B_1$  and  $A_2 \leq B_2$

then

$$A_1 | A_2 \leq B_1 | B_2$$

*τ becomes uncontrollable*

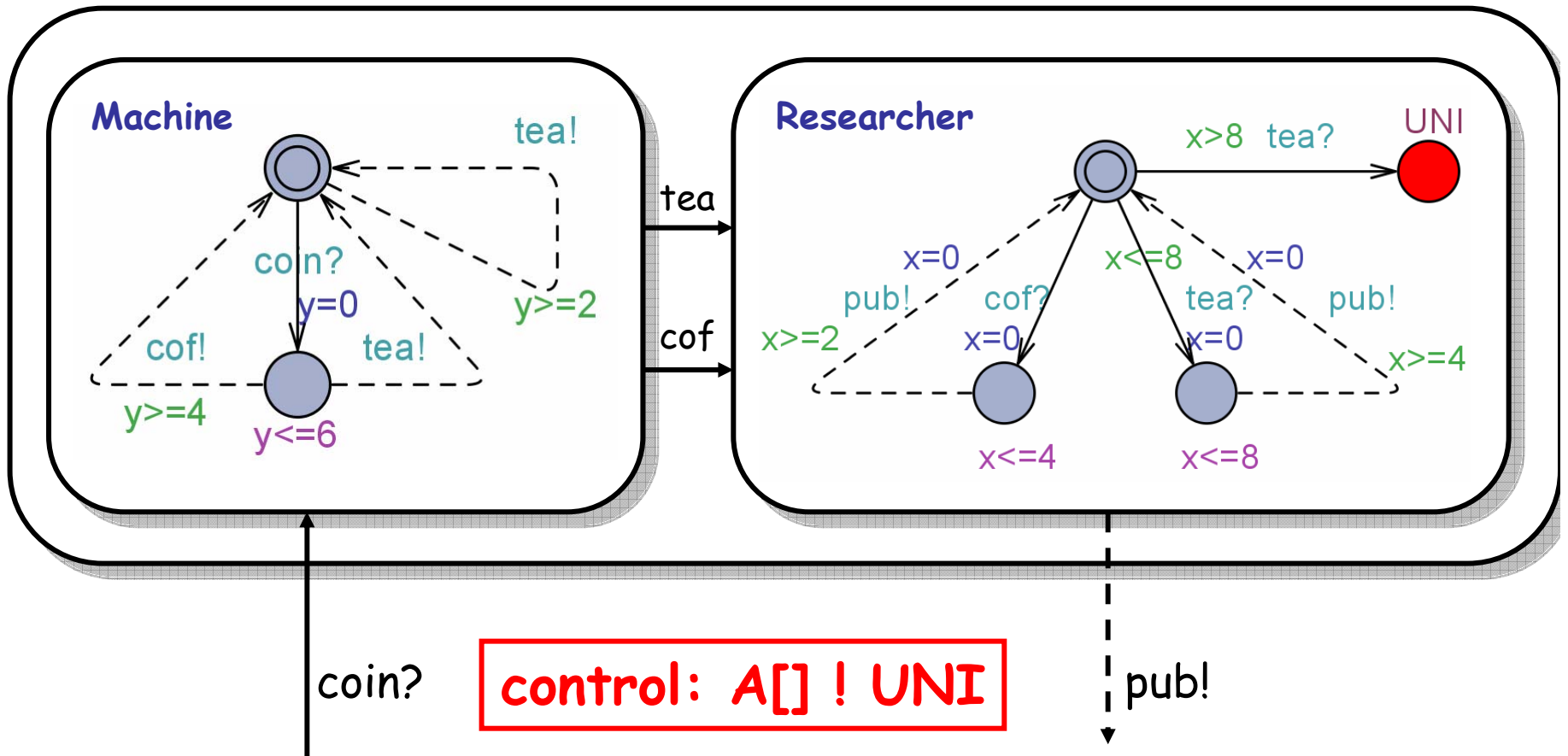
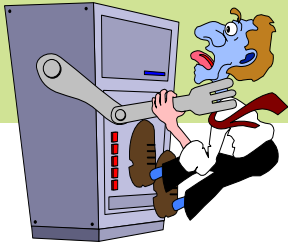
$$\frac{s_1 \xrightarrow{i?} s_1'}{s_1 | s_2 \xrightarrow{i?} s_1' | s_2} \quad i \in \Sigma_i^1 - \Sigma_0^2$$

$$\frac{s_1 \xrightarrow{o!} s_1'}{s_1 | s_2 \xrightarrow{o!} s_1' | s_2} \quad o \in \Sigma_o^1 - \Sigma_i^2$$

$$\frac{s_1 \xrightarrow{a!} s_1' \quad s_2 \xrightarrow{a?} s_2'}{s_1 | s_2 \xrightarrow{\tau!!} s_1' | s_2'} \quad a \in \Sigma_o^1 - \Sigma_i^2$$

# Composability of Timed Interfaces

## - as a Game



Can the OVERALL environment use to use the composition so that for any unexpected input is guaranteed not to occur?

# Future Challenges

- Independent Implementability:

If  $B_1$  and  $B_2$  are composable  
and  $A_1 \leq B_1$  and  $A_2 \leq B_2$   
then  $A_1$  and  $A_2$  are composable!

- Non-determinism?
- Unobservable actions?
- → Timed Games with Partial Observability !
- Applications !

**Thanks for your attention !**

