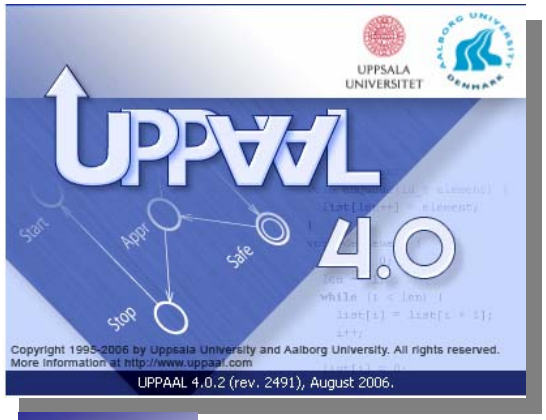
Playing Games with Timed Interfaces --

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:

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

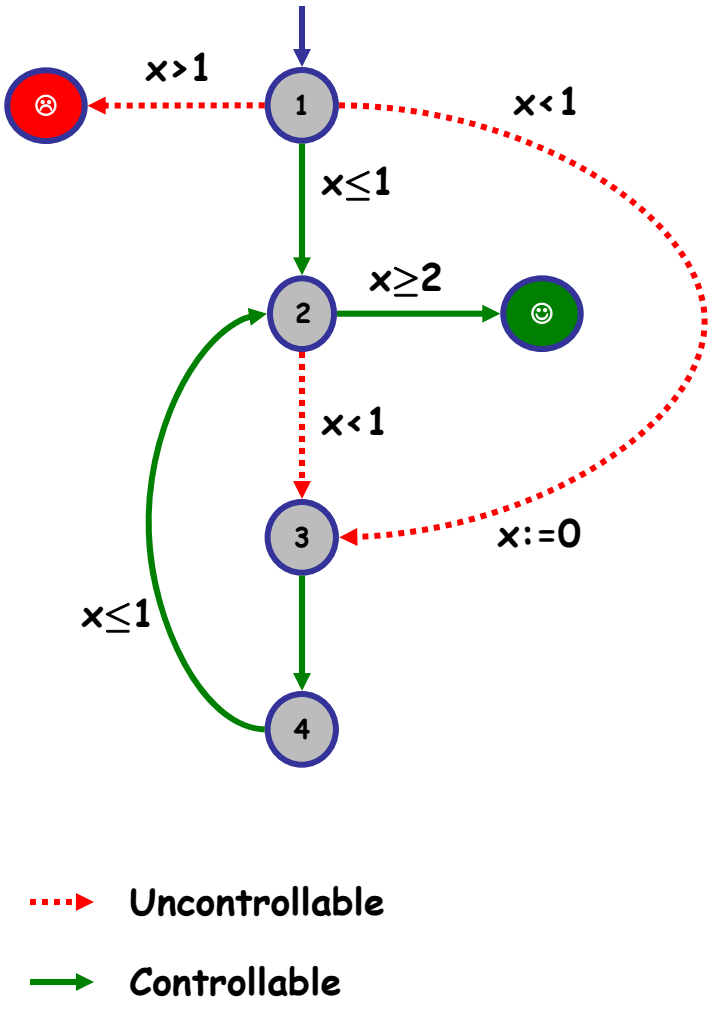
Winning Run:

$States(\rho) \cap G \neq \emptyset$

$States(\rho) \cap G = \emptyset$

Winning Strategy:

$Runs(F) \subseteq WinRuns$



Timed Games

Reachability / Safety Games

Strategy:

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

Winning Run:

$States(\rho) \cap G \neq \emptyset$

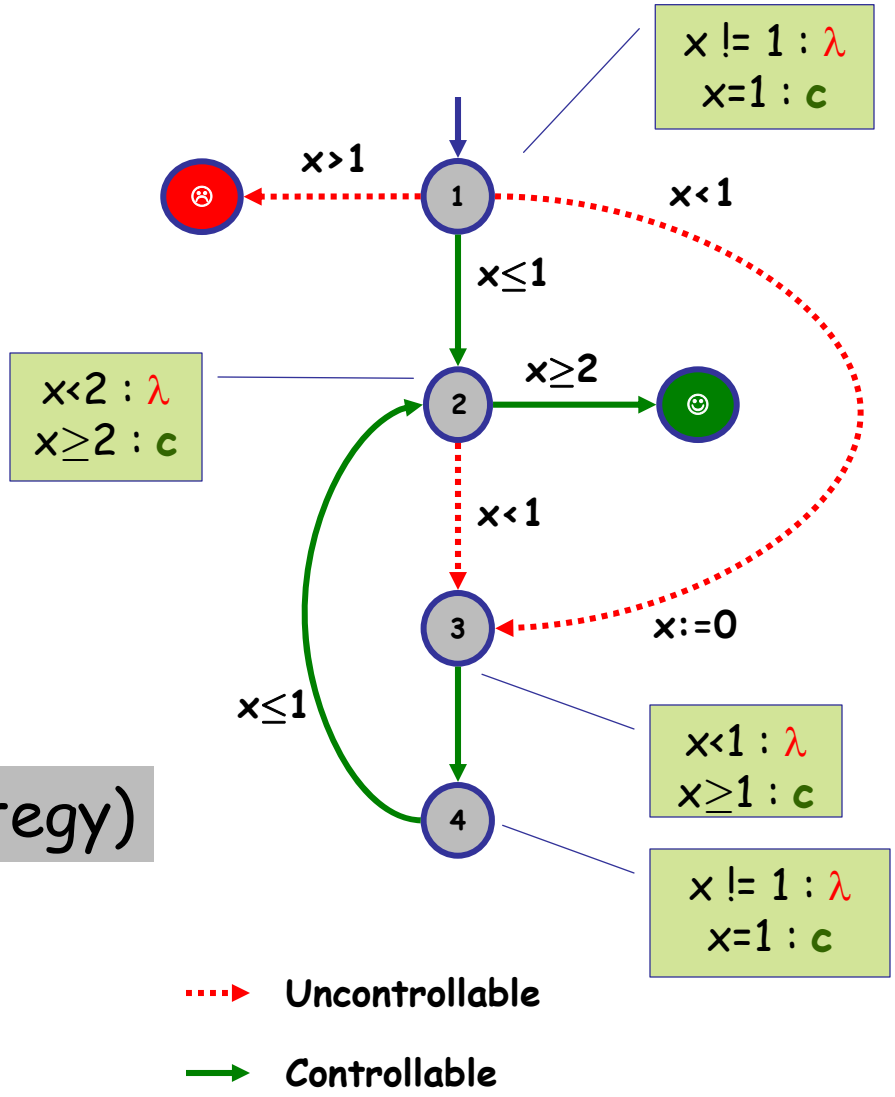
$States(\rho) \cap G = \emptyset$

Winning Strategy:

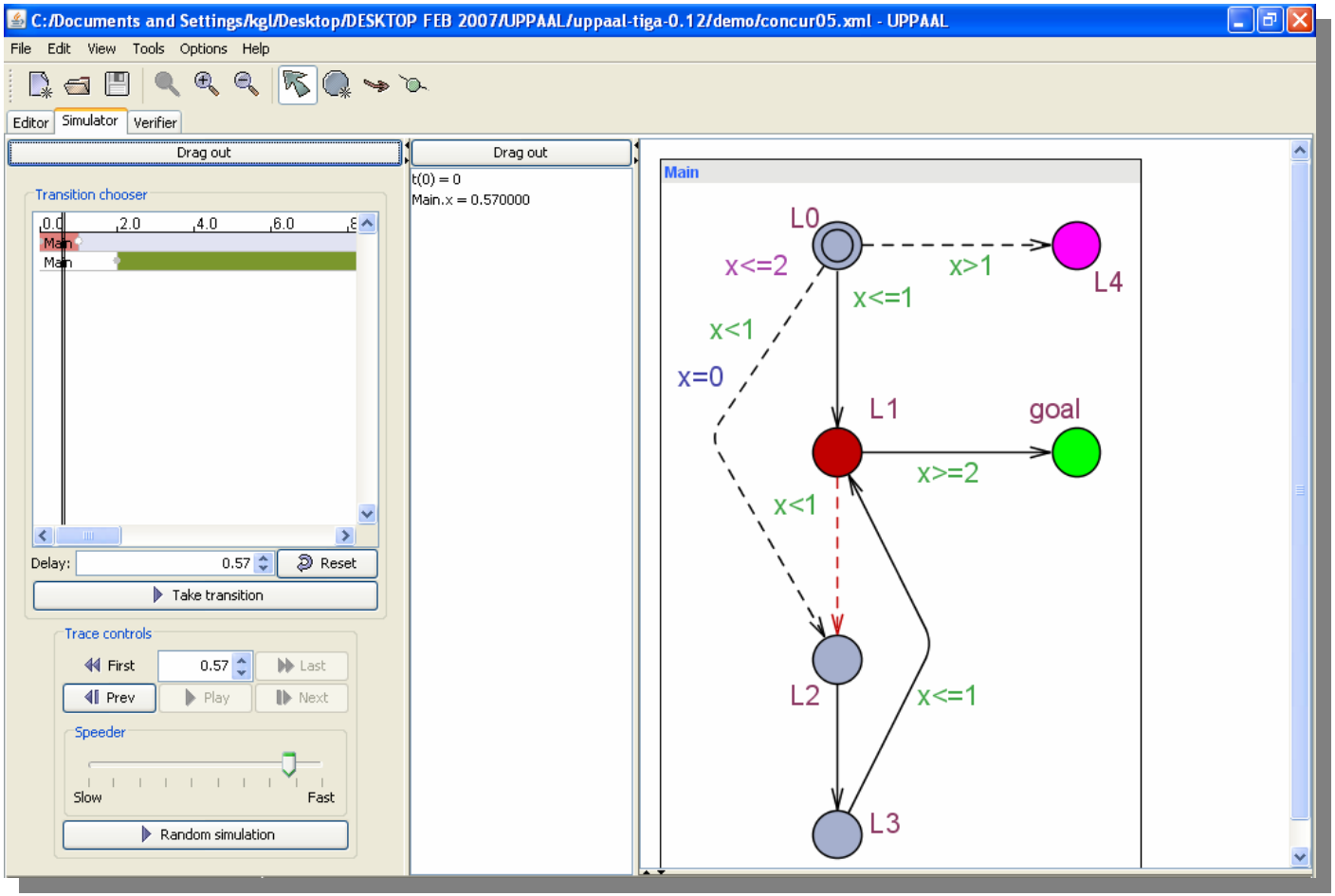
$Runs(F) \subseteq WinRuns$

Winning (memoryless) strategy)

control: A<> ☺



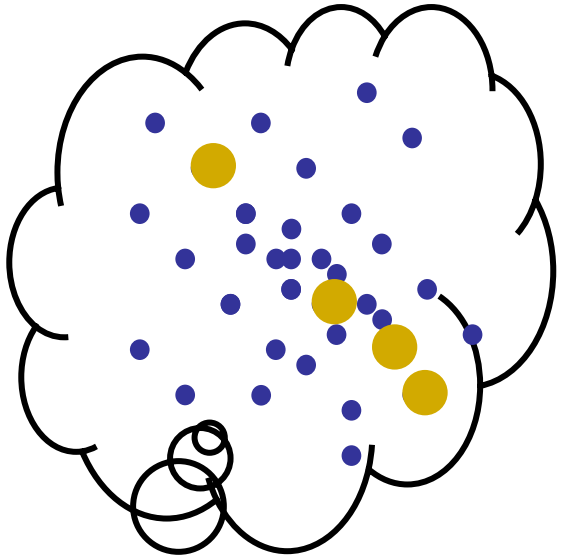
UPPAAL Tiga

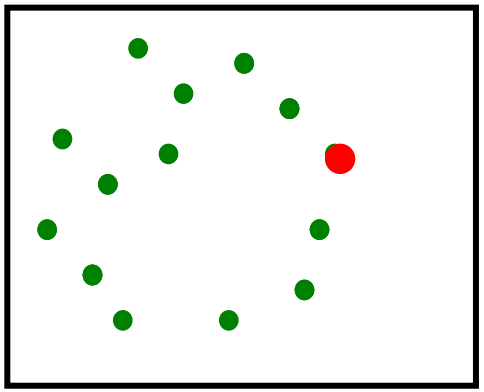


CCONCUR05, CAV07, FORMATS07

Specification Theory

Imp: set of implementations





Spec: set of specifications

Specification Formalism

$$SPF = (Imp, Spec, sat)$$

where

$$sat \subseteq Imp \times Spec$$

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

Refinement :

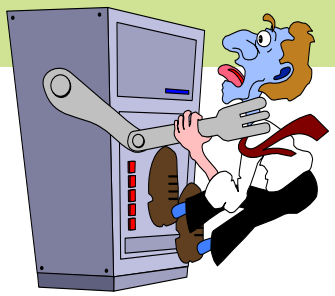
$$S \lhd T \text{ iff } |S| \subseteq |T|$$

Consistency :

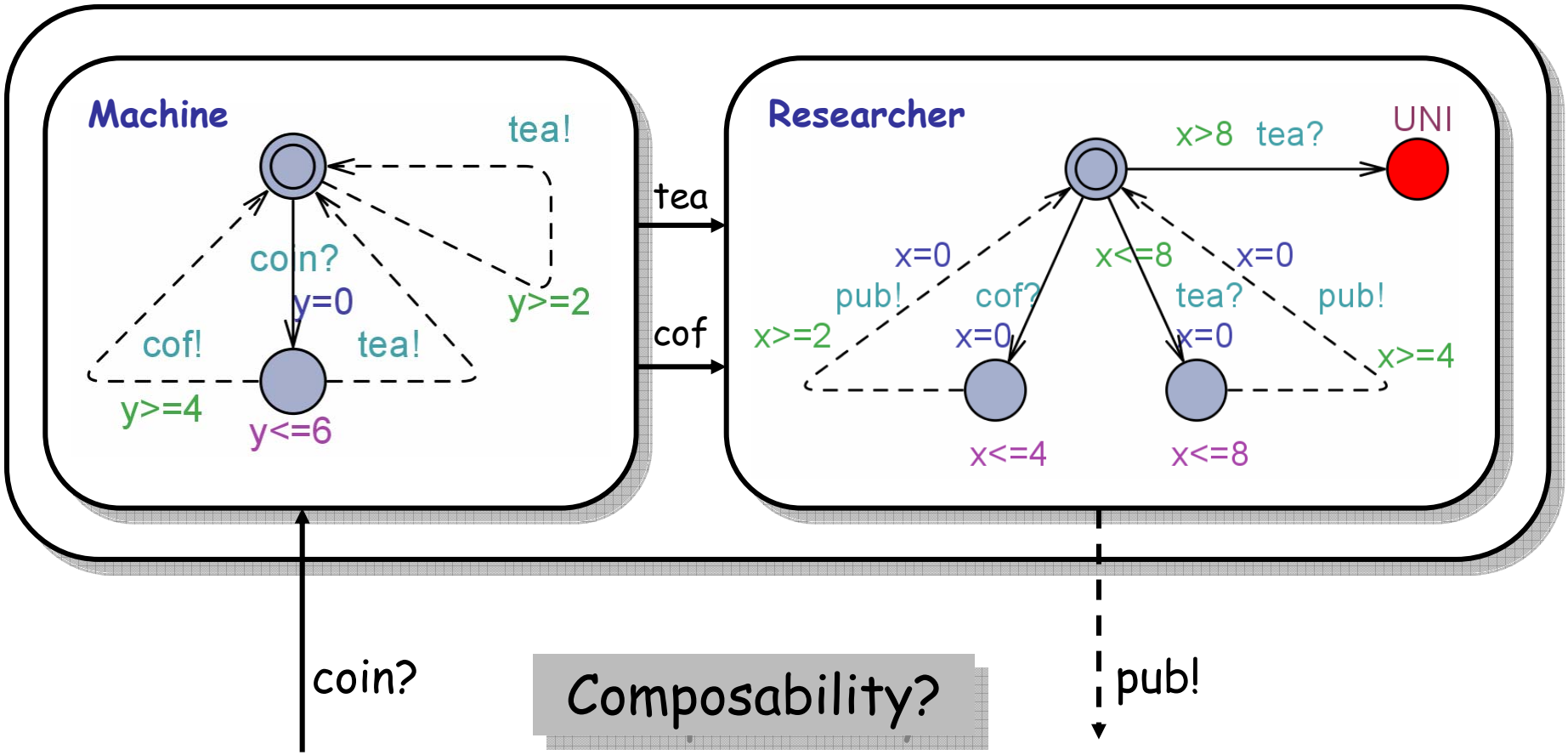
$$|S| \neq \emptyset$$

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

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



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



Alfaro,Henzinger, Stoelinga EMSOFT02

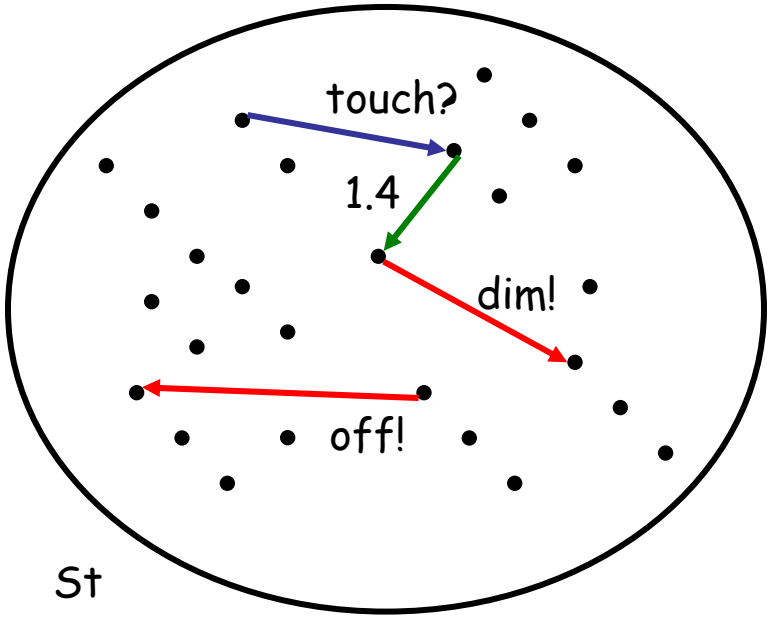
Timed I/O Transition Systems

TIOTS:

$(St, Act, \rightarrow)$

where $\rightarrow : St \times (Act \cup \Re) \times St$

and $Act = \Sigma_i \cup \Sigma_o$



Time determinism ($d \in \Re$)

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

Input enabledness

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

Time divergence

$$\text{whenever } s \xrightarrow{d_0} \xrightarrow{a_0} \xrightarrow{d_1} \xrightarrow{a_1} \cdots$$

$$\text{then } \sum_{i \geq 0} d_i = \infty$$

Determinism ($a \in Act \cup \Re$)

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

Output urgency

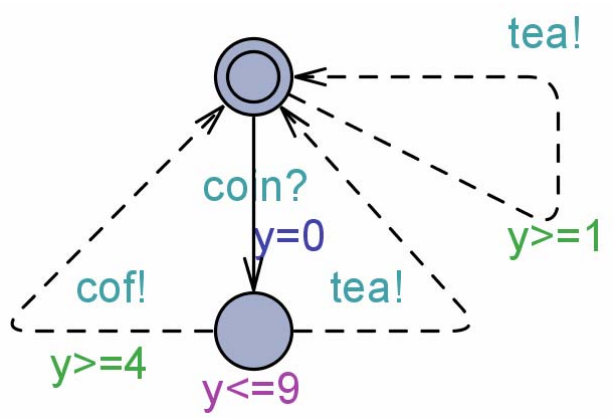
$$\text{whenever } s \xrightarrow{o}$$

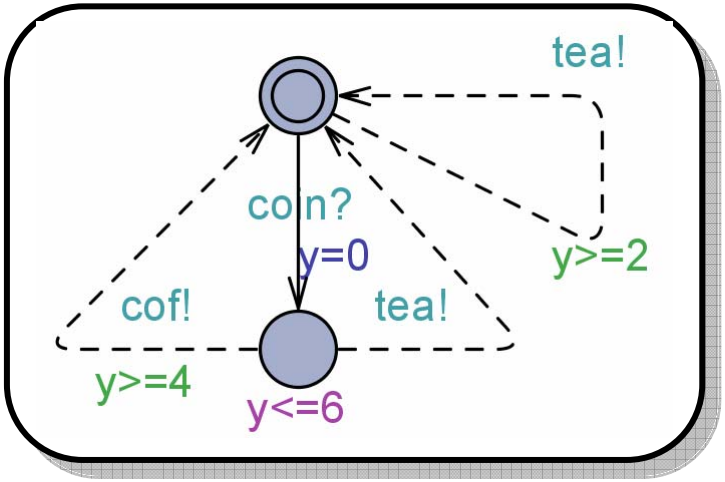
$$\text{then } s \xrightarrow{d} \text{ implies } d = 0$$

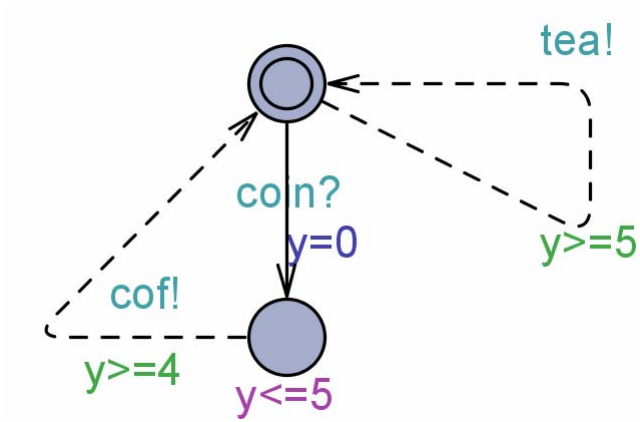
Isolated outputs

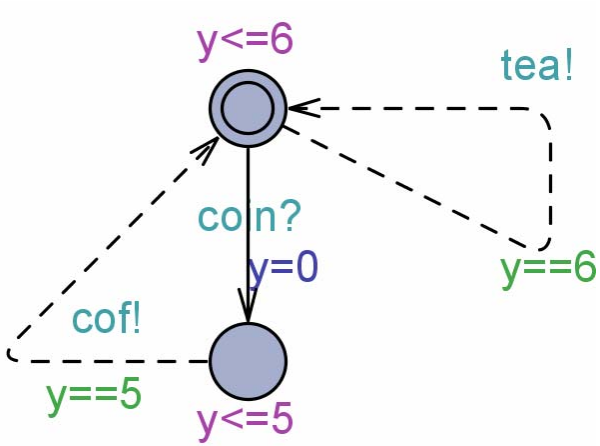
$$\text{If } s \xrightarrow{o} \text{ and } s \xrightarrow{o'} \text{ then } o = o'$$

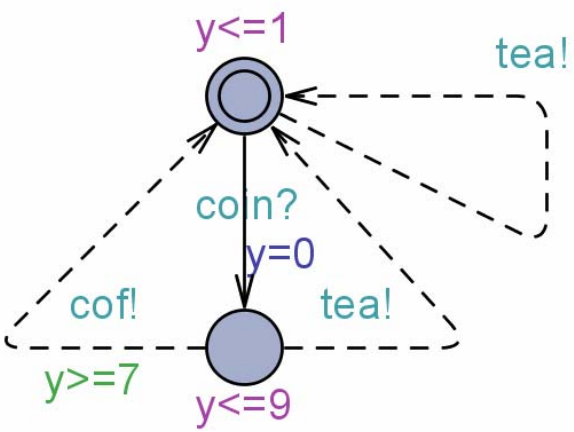
Refinements, Implementations, Consistency











Timed Refinement = Timed Alternating Simulation

Let S and T be TIOGA.

S ≤ 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

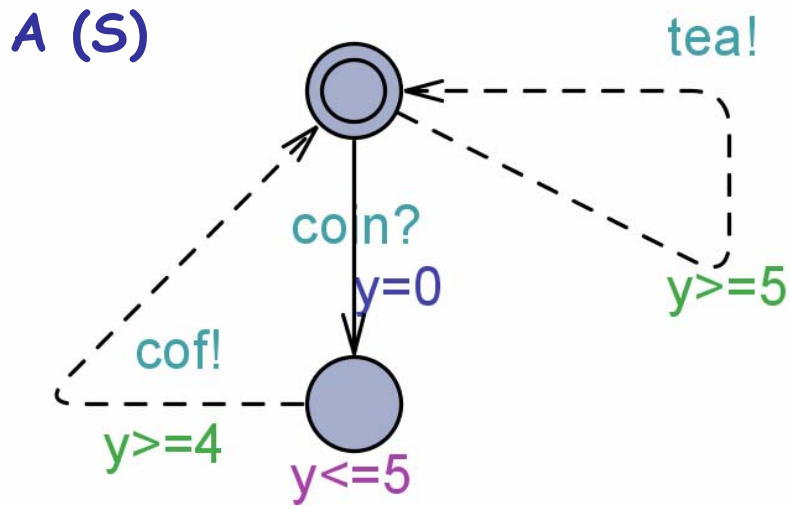
then $S \leq T \Leftrightarrow TTr(S) \subseteq TTr(T)$

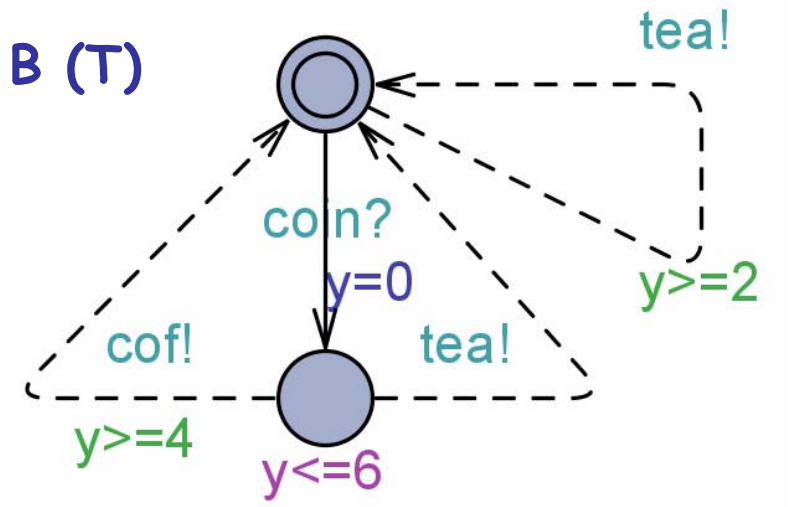
Theorem

$S \leq T \Rightarrow$

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

Refinement (example)





Let S and T be TIOGA.

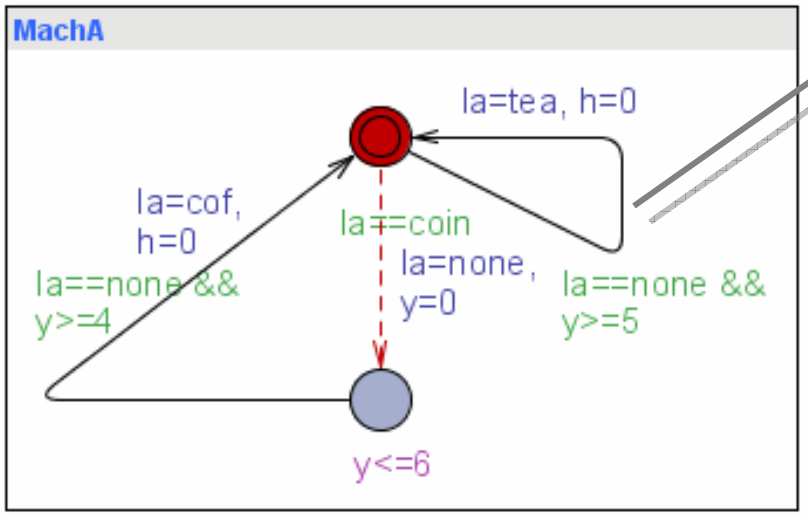
$S \prec T$ iff

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 $S' \leq T'$

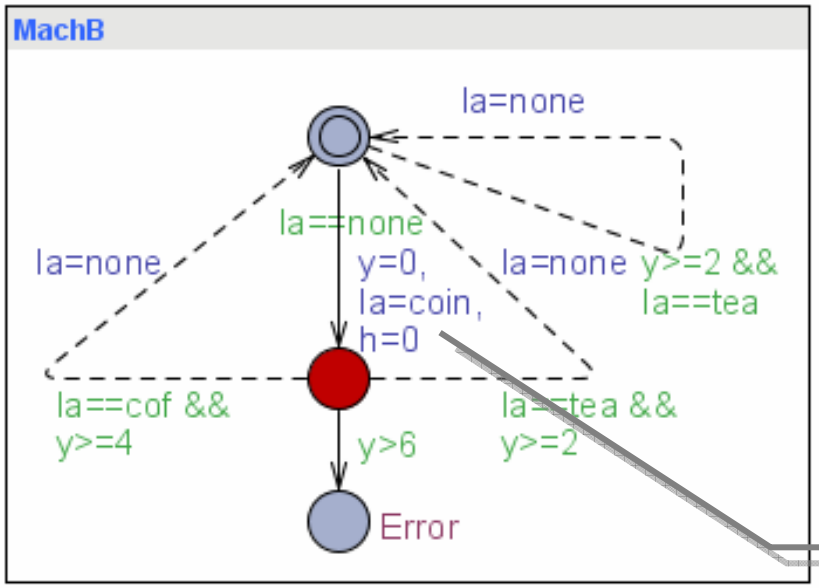
iii. $S \xrightarrow{d} S'$ then $T \xrightarrow{d} T'$ with $S' \leq T'$

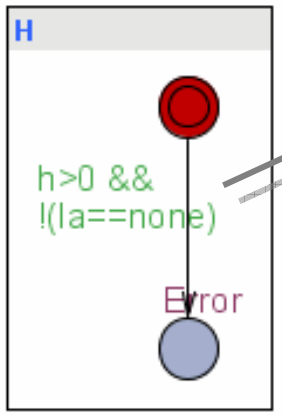
Refinement Checking as a Game



Challenging on outputs and delays

not $A \leq B$
iff
MachA | MachB | H sat
control: A<> Error

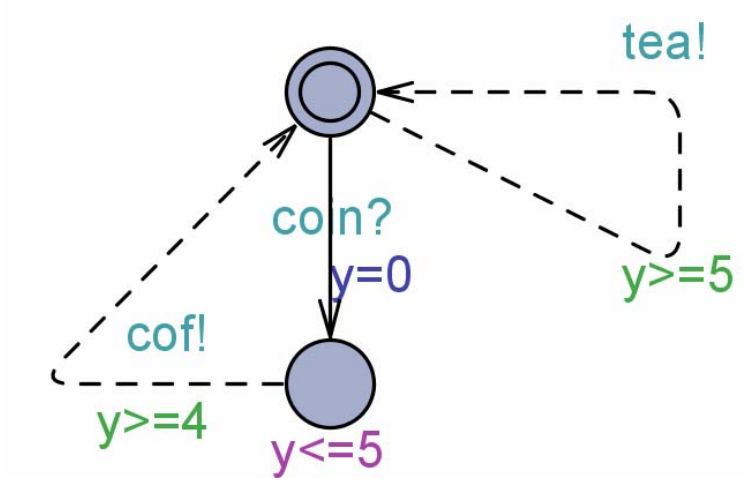




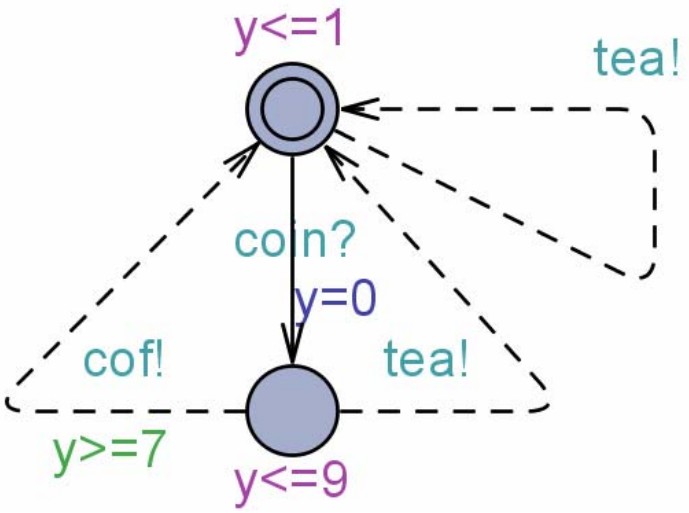
Checking that responses are made immediately

Challenging on inputs

Consistency



S



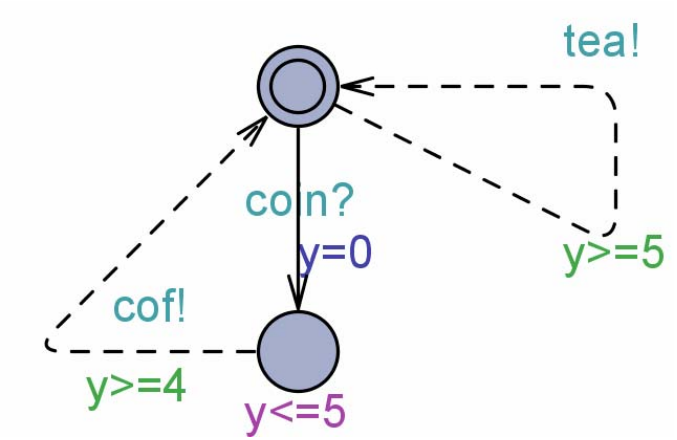
T

Consistency :

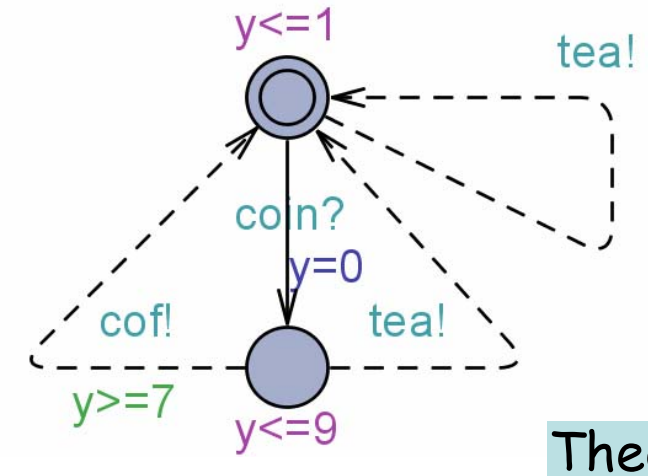
Does there exist I such that

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

Consistency



S



T

Theorem

CONS(S, T) iff

S and T are consistent.

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

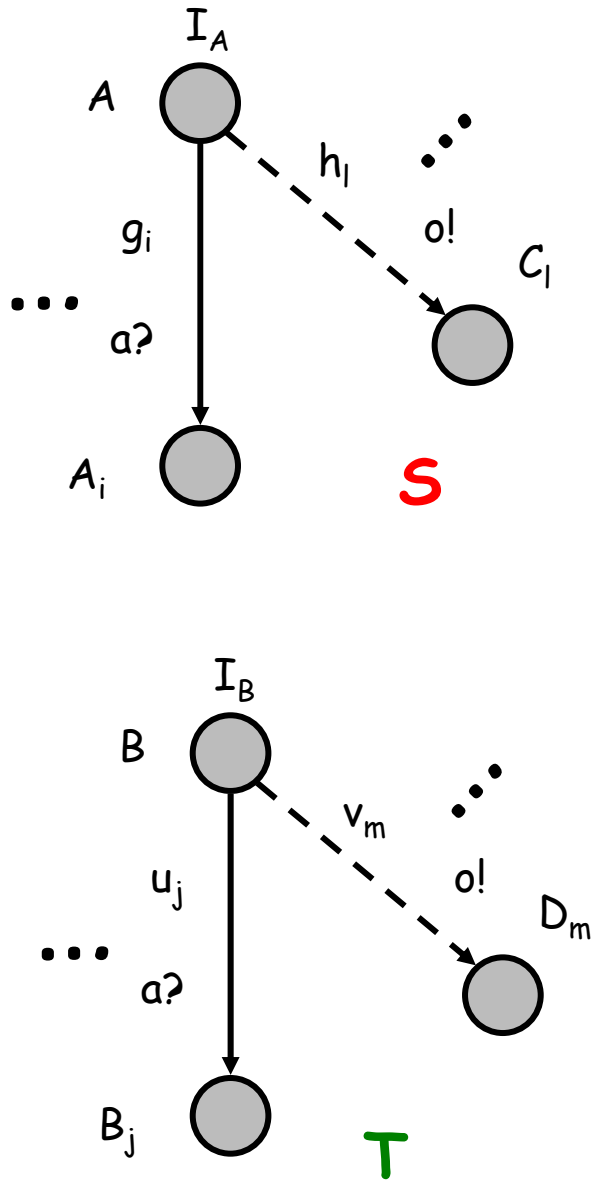
Define CONS as the largest relation such that whenever CONS(s,t) then

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

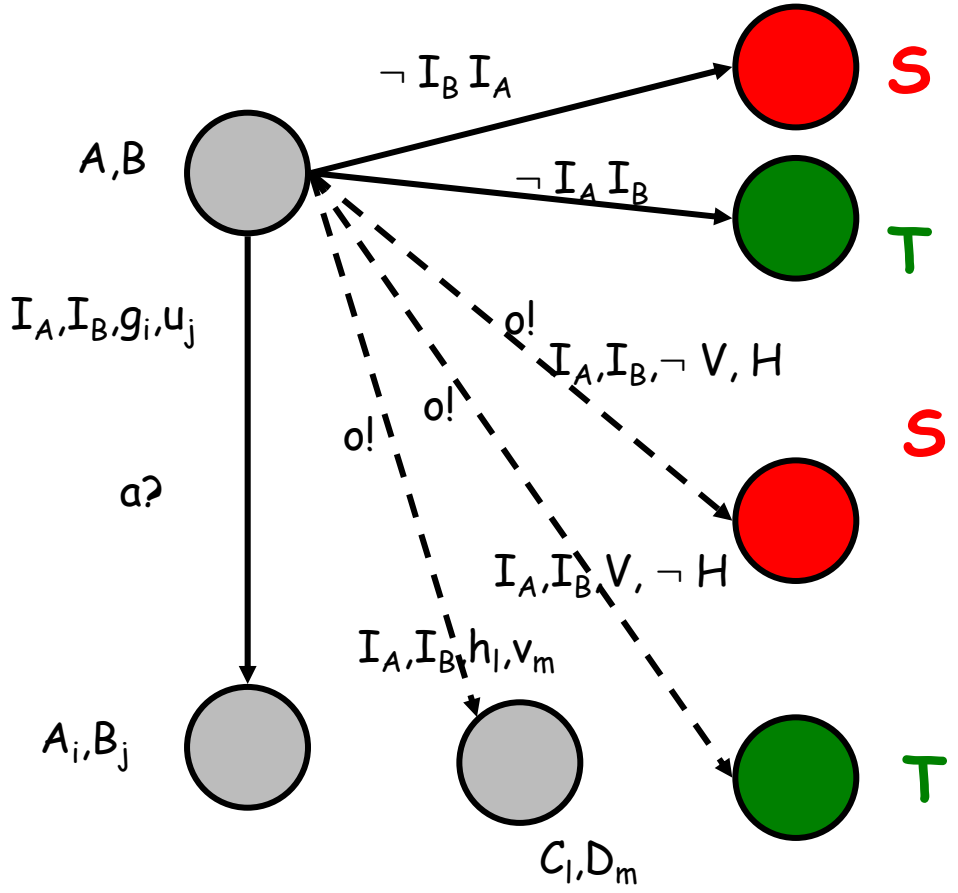
ii. $\left(\exists \sigma \in \Sigma_o \cup \Re.\, s \xrightarrow{\sigma} \vee t \xrightarrow{\sigma}\right) \Rightarrow$

$$\left(\exists \sigma \in \Sigma_o \cup \Re.\, s \xrightarrow{\sigma} s' \wedge t \xrightarrow{\sigma} t' \wedge CONS(s',t')\right)$$

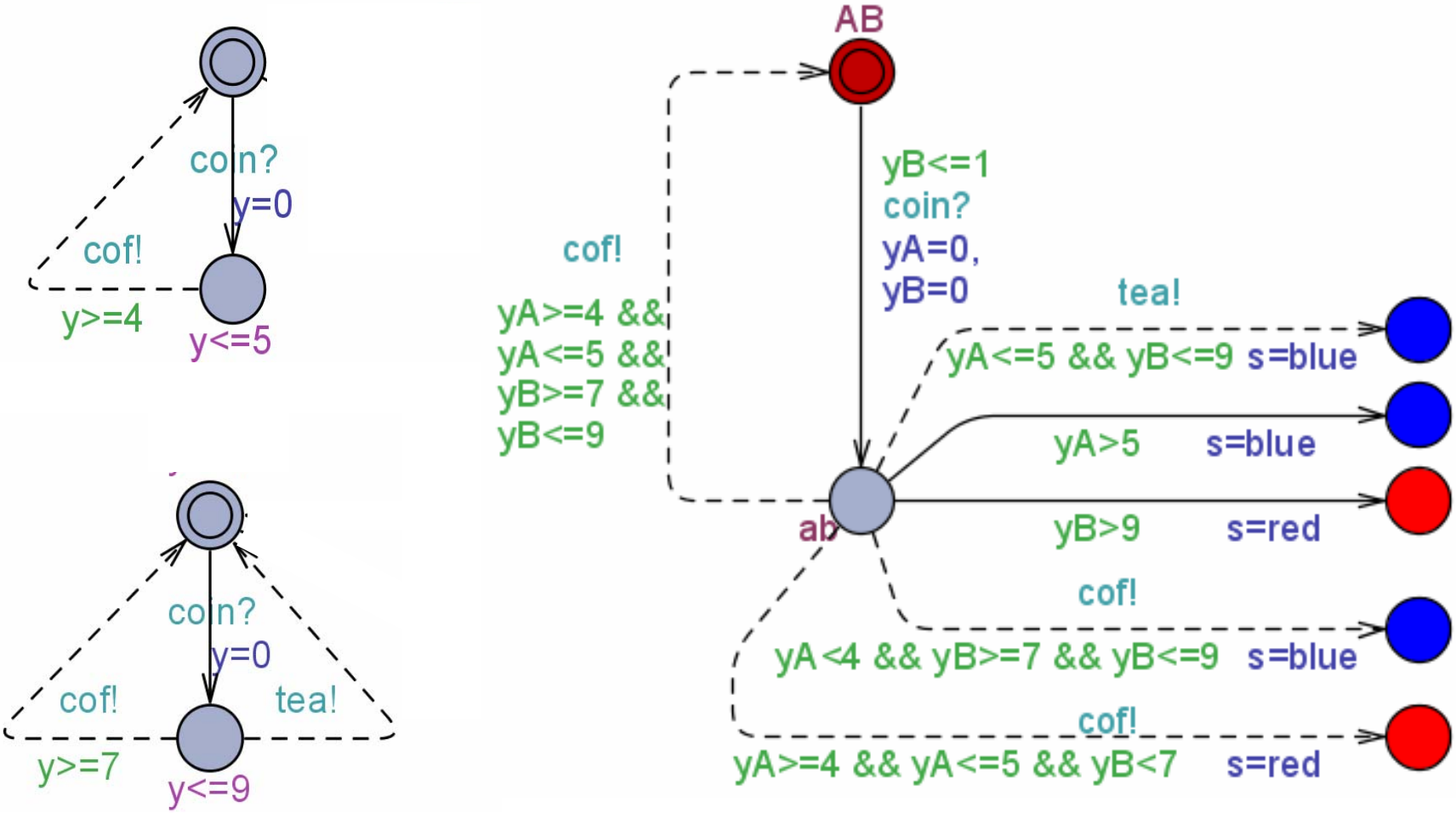
Consistency Checking as a Game



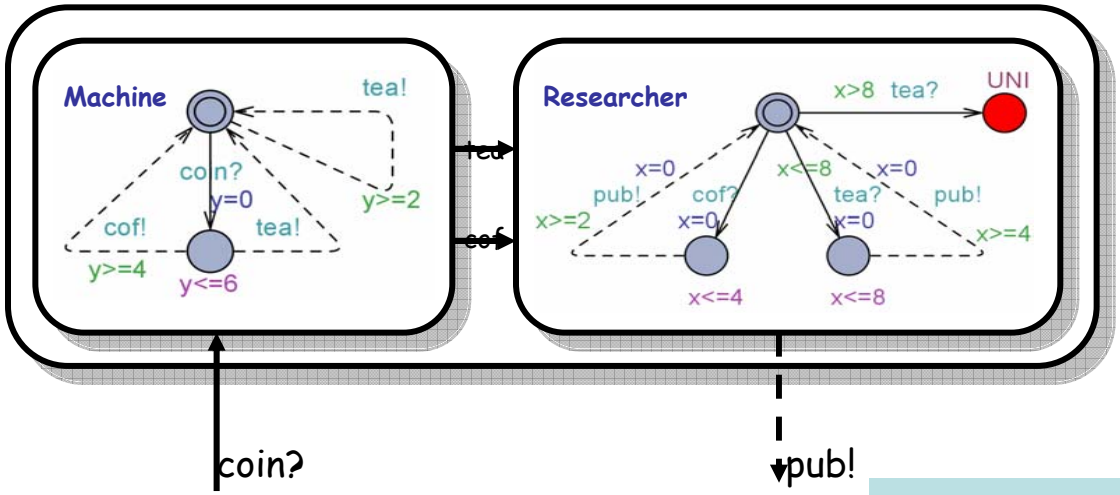
S and T are inconsistent
iff
SxT satisfies
control: A<> (T or S).



Consistency Checking - Example



Composition of Timed Interfaces



Classical rules for Composition of I/O transition systems

$$\frac{s_1 \xrightarrow{i?} s_1'}{s_1 | s_2 \xrightarrow{i?} s_1' | s_2} \; i \in \sum_i^1 - \sum_0^2$$

$$\frac{s_1 \xrightarrow{o!} s_1'}{s_1 | s_2 \xrightarrow{o!} s_1' | s_2} \; o \in \sum_o^1 - \sum_i^2$$

τ becomes uncontrollable

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

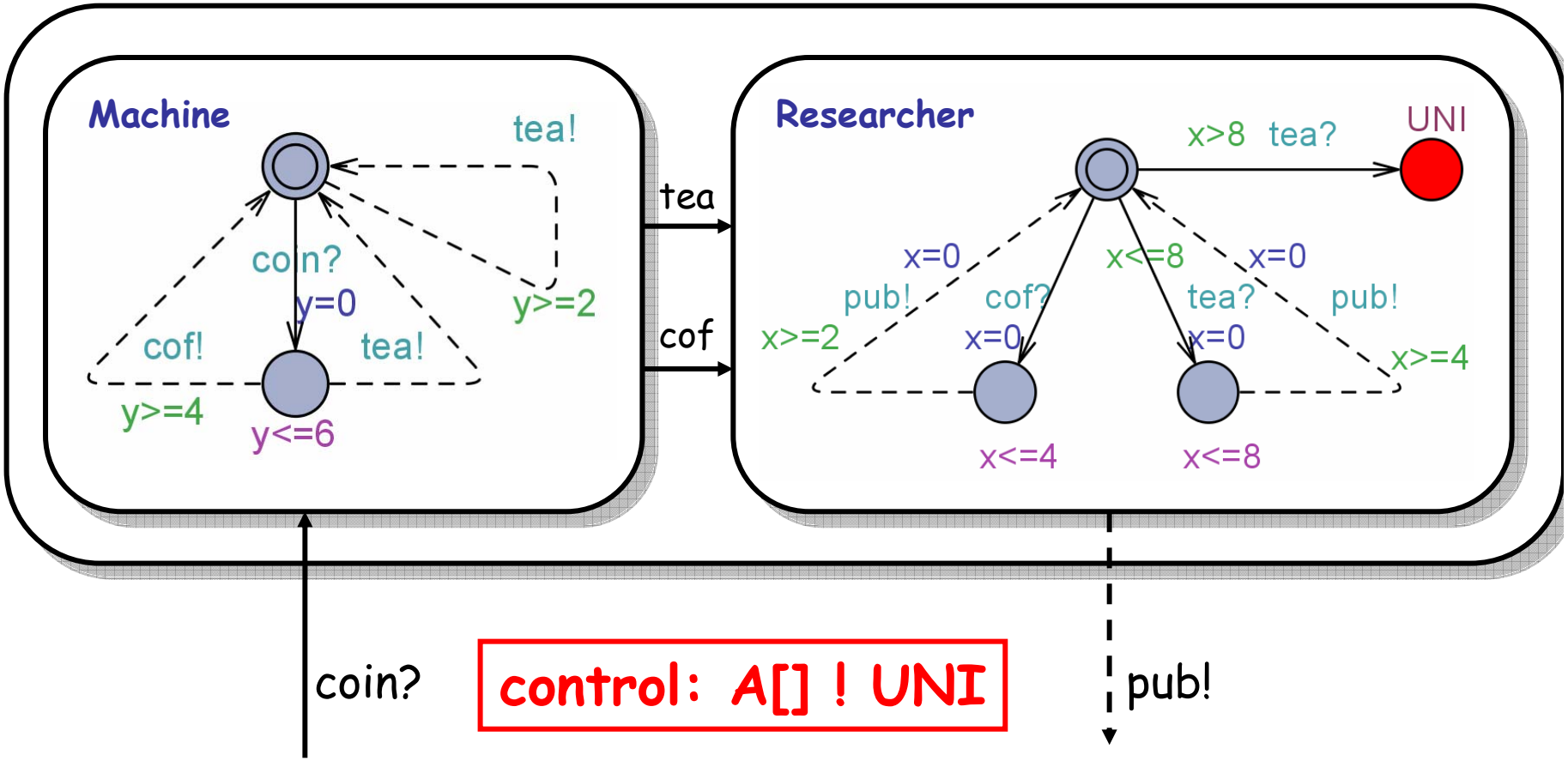
Theorem

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

then

$A_1 | A_2 \leq B_1 | B_2$

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 !