Verification of Timed Systems

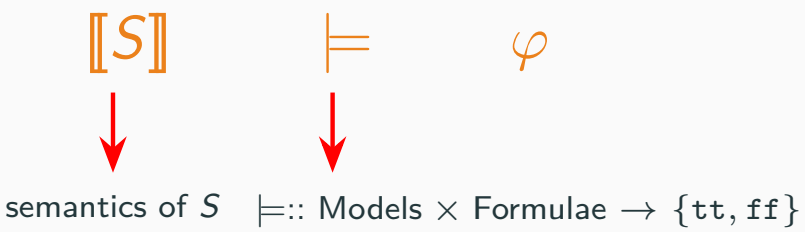
Renato Neves

Universidade do Minho

HASLab
HIGH-ASSURANCE
SOFTWARE LABORATORY

The Satisfaction Problem

Given a system S and a property φ show that



The choice of which logical language to use for writing φ depends on the underlying computational paradigm

A Logical Language for Timed Systems

Variant of Computation Tree Logic with two types of formulae

description of state and path properties

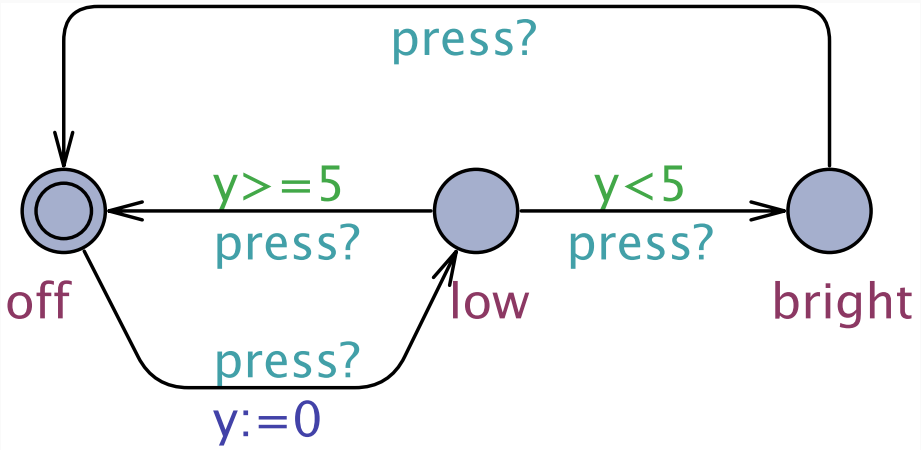
State formulae

Grammar

$\Psi ::= \ell \mid c \mid \texttt{deadlock} \mid \texttt{not } \Psi \mid \Psi \texttt{ or } \Psi \mid \Psi \texttt{ and } \Psi$

We can thus express current locations ℓ, clock constraints $c \in \mathcal{C}(C)$, and the presence of deadlocks

Back to the lamp



Exercise

Write formulae for the following statements

1. The lamp is `low`
2. Not `off` and $y > 25$
3. If it is `low` or `bright` then $y \leq 3600$

Path Formulae

Grammar

$$\Pi ::= A\Box\,\Psi \mid A\Diamond\,\Psi \mid E\Box\,\Psi \mid E\Diamond\,\Psi \mid \Phi \rightsquigarrow \Psi$$

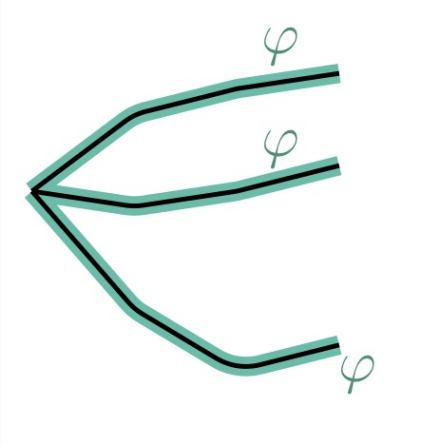
where

- A, E quantify (universally and existentially, resp.) over paths
- $\Box$, $\Diamond$ quantify (universally and existentially, resp.) over states in a path

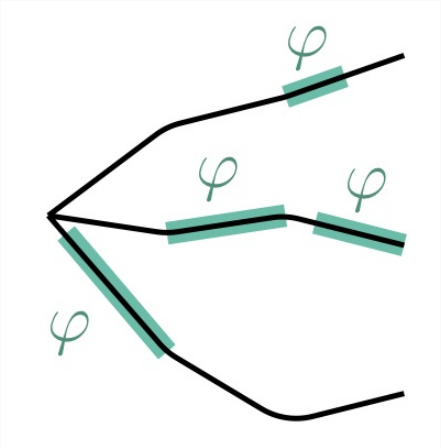
Paths can be seen as possible executions

Path Formulae pt. II

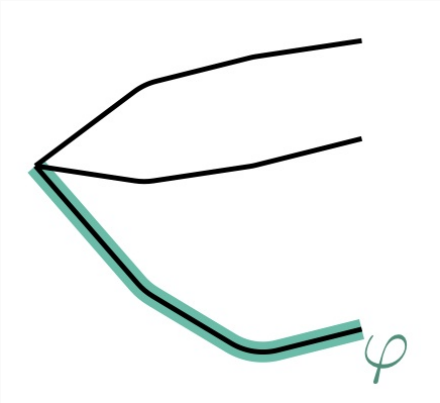
$A\Box\varphi$



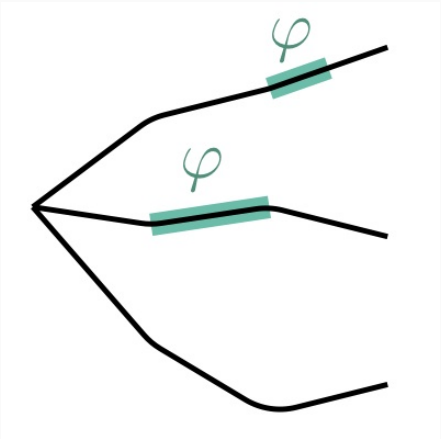
$A\Diamond\varphi$



$E\Box\varphi$



$E\Diamond\varphi$



Safety Properties

$A\Box\varphi$ and $E\Box\varphi$

Something bad will never happen

Examples:

- A nuclear reactor's temperature will never exceed a certain threshold
- We will never reach deadlock
- There is at least one execution in which we never reach deadlock

Reachability Properties

$E\Diamond\varphi$

Something good can happen

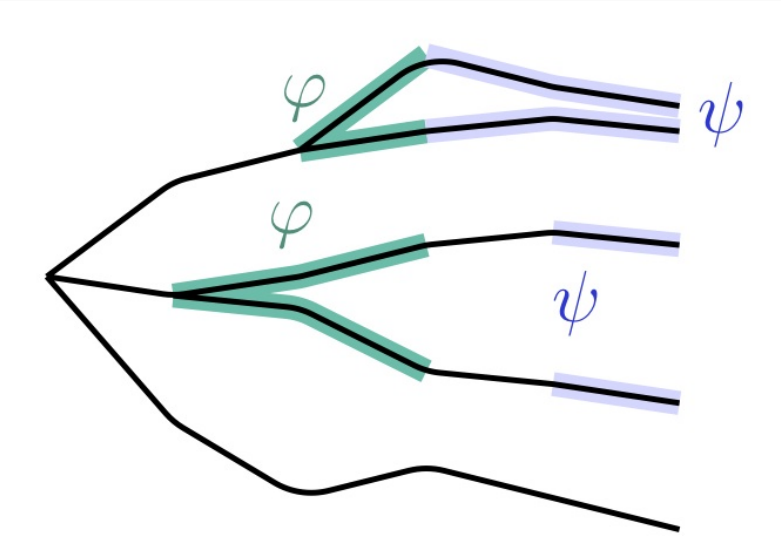
Examples:

- All adventurers reach the other side.
- All adventurers reach the other side in ≤ 17 minutes.
- ...

Path Formulae pt. III

For all paths if φ holds at some point then ψ will also hold later on

$$\varphi \rightsquigarrow \psi$$



Liveness Properties

$A \Diamond \phi$ and $\phi \rightsquigarrow \psi$

Something good will eventually happen or

if something happens then something good will eventually happen

Examples:

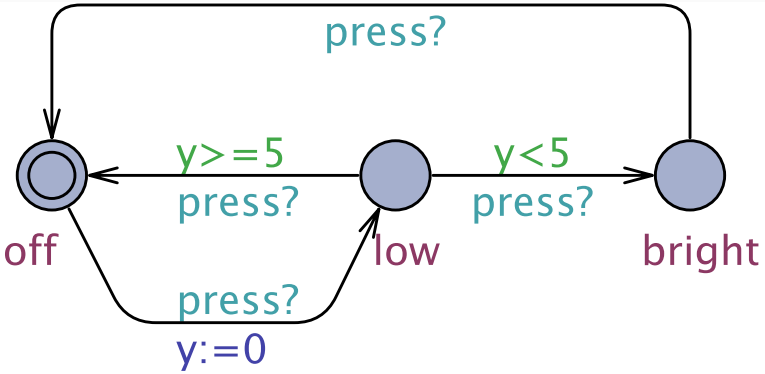
- Always when pressing the on button the television will eventually turn on
- If the philosopher requests a fork she will eventually get it
- If the plane asks to land it will eventually land

Exercises

Write the sentences below in CTL

1. The system never enters in deadlock
2. The location ℓ is reachable
3. In all executions we reach location ℓ
4. If we reach location ℓ we will inevitably reach location s
5. There exists at least one execution where variable `i` is always below or equal 10
6. The two philosophers never eat at the same time

Back to the lamp



Exercise

1. The lamp can become bright;
2. The lamp will eventually become bright;
3. The lamp can never be on for more than 3600s;
4. It is possible to never turn on the lamp;
5. Whenever the light is bright, the clock y is non-zero;
6. Whenever the light is bright it will eventually become off.