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

$$S \qquad \models \qquad \varphi$$

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

$\boxed{\text{description of state and path properties}}$

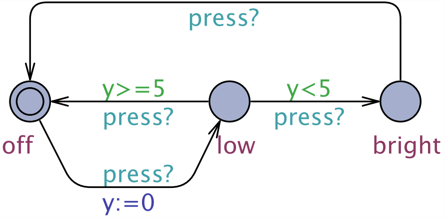
State formulae

Grammar

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

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

Back to the annoying lamp



Exercise

Write formulae for the following statements

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

Path Formulae

Grammar

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

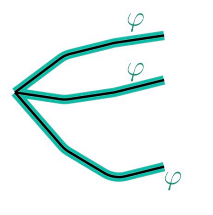
A, E quantify (universally / existentially) over paths

$\Box$, $\Diamond$ quantify (universally / existentially) over states in a path

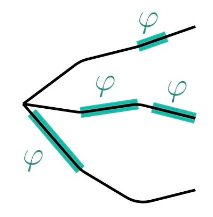
Paths are seen as possible system executions

Path Formulae in Pictures

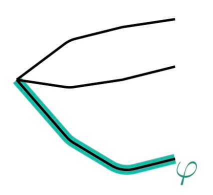
$A\Box\varphi$



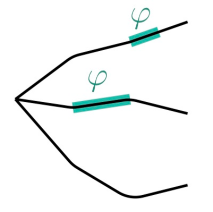
$A\Diamond\varphi$



$E\Box\varphi$



$E\Diamond\varphi$



Safety properties

$A\Box\,\varphi \qquad E\Box\,\varphi$

Something bad will never happen, *e.g.*

- Temperature will never exceed the prescribed threshold
- System never reaches a deadlock
- At least one execution with no deadlocks

Reachability properties

$E\Diamond\, \varphi$

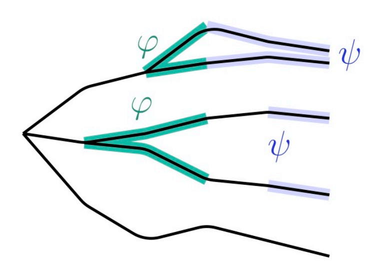
Something good can happen, *e.g.*

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

Path formulae

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

$$\phi \rightsquigarrow \psi \overset{\text{abv}}{=} A\Box(\phi \to A\Diamond\psi)$$



Liveness Properties

$A \Diamond \phi \qquad \phi \leadsto \psi$

If something happens then something good eventually happens

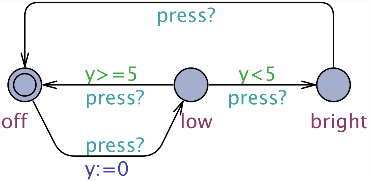
- When pressing ON the television will eventually turn on
- If the philosopher requests a fork she will get it
- If the plane asks to land it will eventually land

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 Annoying 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.

Table of Contents

Chapter’s Conclusion

Key Takeaways

Communicating systems as timed automata

Syntax

Semantics for rigorous analysis and verification

UPPAAL as an important tool of the cyber-physical engineer

Key takeaways

Time as the main physical process …

… others will appear in the next lectures

Barely scratched the surface …

… more about the theory of timed automata in the website