Time-critical reactive systems (I)

Luís S. Barbosa

HASLab - INESC TEC
Universidade do Minho
Braga, Portugal

24 April 2014

Motivation

Specifying an airbag saying that in a car crash the airbag eventually inflates

- in μ-calculus: $\nu Y \,.\, [crash](\mu X \,.\, [-airbag]X \wedge \langle - \rangle \mathrm{true}) \;\wedge\; [-]Y$
- in CTL: $\forall\Box(crash \Rightarrow \forall\Diamond airbag)$ or $\mathrm{AG}(crash \Rightarrow \mathrm{AF} airbag)$
- ...

maybe not enough, but:

in a car crash the airbag eventually inflates within 20ms

Correctness in time-critical systems not only depends on the logical result of the computation, but also on the time at which the results are produced

[Baier & Katoen, 2008]

Motivation

Specifying an airbag saying that in a car crash the airbag eventually inflates

- in μ-calculus: $\nu Y \,.\, [crash](\mu X \,.\, [-airbag]X \wedge \langle - \rangle \mathrm{true}) \;\wedge\; [-]Y$
- in CTL: $\forall\Box(crash \Rightarrow \forall\Diamond airbag)$ or $\mathrm{AG}(crash \Rightarrow \mathrm{AF}\, airbag)$
- ...

maybe not enough, but:

in a car crash the airbag eventually inflates within 20ms

> *Correctness in time-critical systems not only depends on the logical result of the computation, but also on the time at which the results are produced*
>
> [Baier & Katoen, 2008]

Examples of time-critical systems

Lip-synchronization protocol

Synchronizes the separate video and audio sources bounding on the amount of time mediating the presentation of a video frame and the corresponding audio frame. Humans tolerate less than 160 ms.

Bounded retransmission protocol

Controls communication of large files over infrared channel between a remote control unit and a video/audio equipment. Correctness depends crucially on

- transmission and synchronization delays
- time-out values for times at sender and receiver

And many others...

- medical instruments
- hybrid systems (eg for controlling industrial plants)
- ...

Timed transition systems

Timed LTS

$$A = \langle S, Act, \longrightarrow \subseteq S \times Act \times \boldsymbol{R}^+ \times S, \circlearrowleft \subseteq S \times \boldsymbol{R}^+, s_o \in S, T \subseteq S \rangle$$

$s \xrightarrow{a}_t s$ a transition through a occurs from s to s' at time t

$s \circlearrowleft_t$ it is possible to idle in state s until (and including) time t

subject to progress and density constraints

Timed transition systems

Progress

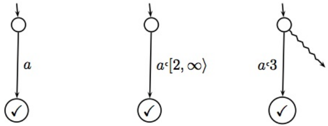
$$s \xrightarrow{a}_t s'' \xrightarrow{b}_{t'} s' \text{ or } s \xrightarrow{a}_t s'' \circlearrowleft_{t'} \quad \text{implies} \quad t < t'$$

Density

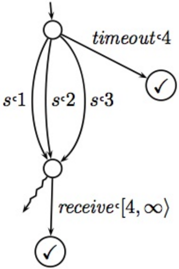
$$s \xrightarrow{a}_t s' \text{ or } s \circlearrowleft_t \quad \text{implies} \quad s \circlearrowleft_{t'} \text{ for all } 0 < t' \leq t$$

Pictures

The density constraint makes almost impossible drawing TLTS: need to cut off redundancy!



Example: modelling a timeout process



From LTS to TLTS

Timed bisimulation

Timed processes

Combinator

- $a@t$ (assume 0 as the beginning of time: $a@0 = \delta@0$)
- $p@t$ (first action of p must occur at time t)
- time deadlock: cf typically when the interaction of parallel processes have incompatible time constraints

Example

$$Clock(t : \mathbb{R}^+) \; = \; tick@(t+1).Clock(t+1)$$

Timed processes

Expressing time constraints

$$\sum_{t \in \mathbb{R}^+} a@t \,.\, \sum_{u \in \mathbb{R}^+} (u \leq t + 10) \rightarrow b@u$$

$$\sum_{t \in \mathbb{R}^+} a@t \,.\, \sum_{u \in \mathbb{R}^+} (u \leq t + 10) \rightarrow b@u \diamond \mathsf{timeout}@u$$

Extending the logic

Examples

$$[true^*.a@t]\langle b@4\rangle true$$

$$[true^*]\forall_{t\in R^+}[\mathrm{call}@t]\langle true^*\rangle\ \exists_{u\in R^+}(u \le t+10 \wedge \langle \mathrm{cararrive}\rangle \mathrm{true})$$

$$\forall_{t\in R^+}[true^*.\mathrm{on}@t]\ \mu_X\ ([\forall_{u\in R^+}\neg(u \le t+0.4 \cup \mathrm{light}@u)]X)$$

$$\forall_{t,u\in R^+}[true^*.\mathrm{standby}@t.true@u]\ u > t+5$$

Extending the logic

Examples

$$[true^*.a@t]\langle b@4\rangle true$$

$$[true^*]\forall_{t\in \mathbb{R}^+}[\mathrm{call}@t]\langle true^*\rangle\ \exists_{u\in \mathbb{R}^+}(u \leq t+10 \wedge \langle \mathrm{cararrive}\rangle \mathrm{true})$$

$$\forall_{t\in \mathbb{R}^+}[true^*.\mathrm{on}@t]\ \mu_X\ ([\forall_{u\in \mathbb{R}^+}\neg(u \leq t+0.4 \cup \mathrm{light}@u)]X)$$

$$\forall_{t,u\in \mathbb{R}^+}[true^*.\mathrm{standby}@t.true@u]\ u > t+5$$

Extending the logic

Examples

$$[true^*.a@t]\langle b@4\rangle true$$

$$[true^*]\forall_{t\in \boldsymbol{R}^+}[\mathrm{call}@t]\langle true^*\rangle\ \exists_{u\in \boldsymbol{R}^+}(u \leq t + 10 \wedge \langle \mathrm{cararrive}\rangle \mathrm{true})$$

$$\forall_{t\in \boldsymbol{R}^+}[true^*.\mathrm{on}@t]\ \mu_X\ ([\forall_{u\in \boldsymbol{R}^+}\neg(u \leq t + 0.4 \cup \mathrm{light}@u)]X)$$

$$\forall_{t,u\in \boldsymbol{R}^+}[true^*.\mathrm{standby}@t.true@u]\ u > t + 5$$

Extending the logic

Examples

$$[true^*.a@t]\langle b@4\rangle true$$

$$[true^*]\forall_{t\in R^+}[\text{call}@t]\langle true^*\rangle\ \exists_{u\in R^+}(u\leq t+10\wedge\langle\text{cararrive}\rangle\text{true})$$

$$\forall_{t\in R^+}[true^*.\text{on}@t]\ \mu_X\ ([\forall_{u\in R^+}\neg(u\leq t+0.4\cup\text{light}@u)]X)$$

$$\forall_{t,u\in R^+}[true^*.\text{standby}@t.true@u]\ u>t+5$$

Extending the logic: delays

$$\Delta = \forall_{t \in R^+} \Delta @t$$

and

$$\nabla @t = \neg \Delta @t$$

Examples

$$[true^*.\text{standby}] \Delta$$

$$\forall_{t \in R^+} [true^*.\text{standby}@t] \Delta @(t+6)$$

$$[true^*.\text{emergency}] \nabla @t$$

Extending the logic: delays

$$\Delta = \forall_{t \in R^+} \Delta @t$$

and

$$\nabla @t = \neg \Delta @t$$

Examples

$$[true^*.\text{standby}] \Delta$$

$$\forall_{t \in R^+} [true^*.\text{standby}@t] \Delta @(t+6)$$

$$[true^*.\text{emergency}] \nabla @t$$

Extending the logic: delays

$$\Delta = \forall_{t \in \mathbf{R}^+} \Delta @t$$

and

$$\nabla @t = \neg \Delta @t$$

Examples

$$[true^*.\mathrm{standby}] \Delta$$

$$\forall_{t \in \mathbf{R}^+} [true^*.\mathrm{standby}@t] \Delta @(t+6)$$

$$[true^*.\mathrm{emergency}] \nabla @t$$

Extending the logic: delays

$$\Delta = \forall_{t \in \boldsymbol{R}^+} \Delta @t$$

and

$$\nabla @t = \neg \Delta @t$$

Examples

$$[\mathit{true}^*.\text{standby}] \Delta$$

$$\forall_{t \in \boldsymbol{R}^+} [\mathit{true}^*.\text{standby}@t] \Delta @(t+6)$$

$$[\mathit{true}^*.\text{emergency}] \nabla @t$$

Dealing with time in system models

Extension of Process Algebras with time

- TCCS [Yi,90] which introduced a new prefix:

  $\epsilon(d).E$ delay d units of time and then behave as E

- TCSP [Reed& Roscoe, 88], ATP [Nicollin & Sifakis, 94], among many others

Emphasis on axiomatics, behavioural equivalences, expressivity

Dealing with time in system models

However, in general, expressive power is somehow limited and infinite-state LTS difficult to handle in practice

Example

TCCS is unable to express a system which has only one action *a* which can only occur at time point 5 with the effect of moving the system to its initial state.

This example has, however, a simple description in terms of time measured by a stopwatch:

1. Set the stopwatch to 0
2. When the stopwatch measures 5, action *a* can occur. If *a* occurs go to 1., if not idle forever.

Dealing with time in system models

However, in general, expressive power is somehow limited and infinite-state LTS difficult to handle in practice

Example

TCCS is unable to express a system which has only one action a which can only occur at time point 5 with the effect of moving the system to its initial state.

This example has, however, a simple description in terms of time measured by a stopwatch:

1. Set the stopwatch to 0
2. When the stopwatch measures 5, action a can occur. If a occurs go to 1., if not idle forever.

Dealing with time in system models

This suggests resorting to an automaton-based formalism with an explicit notion of clock (stopwatch) to control availability of transitions.

$\boxed{\text{Timed Automata [Alur \& Dill, 90]}}$

- emphasis on decidability of the model-checking problem and corresponding practically efficient algorithms

Associate tools

- UPPAAL [Behrmann, David, Larsen, 04]
- KRONOS [Bozga, 98]