Semantics and Verification 2005

Lecture 9

- labelled transition systems with time
- timed automata
- timed and untimed bisimilarity
- timed and untimed language equivalence

Need for Introducing Time Features

- **Timeout in Alternating Bit protocol:**
  - In CCS timeouts were modelled using nondeterminism.
  - Enough to prove that the protocol is safe.
  - Maybe too abstract for certain questions (What is the average time to deliver the message?).
- **Many real-life systems depend on timing:**
  - Real-time controllers (production lines, computers in cars, railway crossings).
  - Embedded systems (mobile phones, remote controllers, digital watch).
  - ...

Labelled Transition Systems with Time

Timed (labelled) transition system (TLTS)

TLTS is a triple $(Proc, Act, \{\xrightarrow{a} \mid a \in Act\})$ where

- $Proc$ is a set of states (or processes),
- $Act = N \cup \mathbb{R}^{\geq 0}$ is a set of **actions** (consisting of **labels** and **time-elapsing steps**), and
- for every $a \in Act$, $\xrightarrow{a} \subseteq Proc \times Proc$ is a binary relation on states called the transition relation.

We write

- $s \xrightarrow{a} s'$ if $a \in N$ and $(s, s') \in \xrightarrow{a}$, and
- $s \xrightarrow{d} s'$ if $d \in \mathbb{R}^{\geq 0}$ and $(s, s') \in \xrightarrow{d}$.

How to Describe Timed Transition Systems?

Syntax unknown entity	$\longrightarrow$	Semantics known entity
CCS	$\longrightarrow$	Labelled Transition Systems
???	$\longrightarrow$	Timed Transition Systems

Timed Automata [Alur, Dill'90]

Finite-state automata equipped with clocks.

Definition of TA: Clock Constraints

Let $C = \{x, y, \ldots\}$ be a finite set of clocks.

Set $\mathcal{B}(C)$ of clock constraints over C

$\mathcal{B}(C)$ is defined by the following abstract syntax

$$g, g_1, g_2 ::= x \sim n \mid x - y \sim n \mid g_1 \wedge g_2$$

where $x, y \in C$ are clocks, $n \in \mathbb{N}$ and $\sim \in \{\leq, <, =, >, \geq\}$.

Example: $x \leq 3 \wedge y > 0 \wedge y - x = 2$

Clock Valuation

Clock valuation

Clock valuation v is a function $v : C \to \mathbb{R}^{\geq 0}$.

Let v be a clock valuation. Then

- $v + d$ is a clock valuation for any $d \in \mathbb{R}^{\geq 0}$ and it is defined by

$$(v + d)(x) = v(x) + d \text{ for all } x \in C$$

- $v[r]$ is a clock valuation for any $r \subseteq C$ and it is defined by

$$v[r](x) \begin{cases} 0 & \text{if } x \in r \\ v(x) & \text{otherwise.} \end{cases}$$

Evaluation of Clock Constraints

Evaluation of clock constraints ($v \models g$)

$$
\begin{array}{ll}
v \models x < n & \text{iff } v(x) < n \\
v \models x \leq n & \text{iff } v(x) \leq n \\
v \models x = n & \text{iff } v(x) = n \\
\vdots & \\
v \models x - y < n & \text{iff } v(x) - v(y) < n \\
v \models x - y \leq n & \text{iff } v(x) - v(y) \leq n \\
\vdots & \\
v \models g_1 \wedge g_2 & \text{iff } v \models g_1 \text{ and } v \models g_2
\end{array}
$$

Syntax of Timed Automata

Definition

A **timed automaton** over a set of clocks C and a set of labels N is a tuple

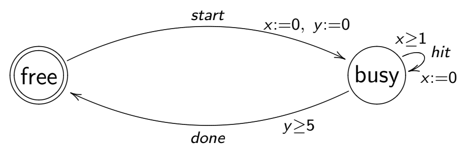
$$(L, \ell_0, E, I)$$

where

- L is a finite set of **locations**
- $\ell_0 \in L$ is the **initial location**
- $E \subseteq L \times \mathcal{B}(C) \times N \times 2^C \times L$ is the set of **edges**
- $I : L \to \mathcal{B}(C)$ assigns **invariants** to locations.

We usually write $\ell \xrightarrow{g,a,r} \ell'$ whenever $(\ell, g, a, r, \ell') \in E$.

Example: Hammer



Semantics of Timed Automata

Let $A = (L, \ell_0, E, I)$ be a timed automaton.

Timed transition system generated by A

$T(A) = (Proc, Act, \{\xrightarrow{a} \mid a \in Act\})$ where

- $Proc = L \times (C \to \mathbb{R}^{\geq 0})$, i.e. states are of the form (ℓ, v) where ℓ is a location and v a valuation
- $Act = N \cup \mathbb{R}^{\geq 0}$
- $\longrightarrow$ is defined as follows:

$(\ell, v) \xrightarrow{a} (\ell', v')$ if there is $(\ell \xrightarrow{g,a,r} \ell') \in E$ s.t. $v \models g$ and $v' = v[r]$

$(\ell, v) \xrightarrow{d} (\ell, v + d)$ for all $d \in \mathbb{R}^{\geq 0}$ s.t. $v \models I(\ell)$ and $v + d \models I(\ell)$

Timed Bisimilarity

Let A_1 and A_2 be timed automata.

Timed Bisimilarity

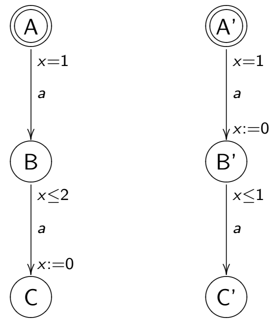
We say that A_1 and A_2 are **timed bisimilar** iff the transition systems $T(A_1)$ and $T(A_2)$ generated by A_1 and A_2 are strongly bisimilar.

Remark: both

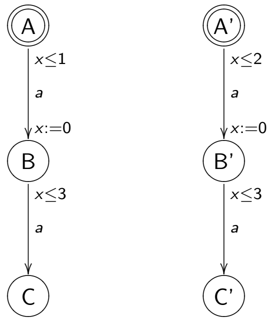
- $\xrightarrow{a}$ for $a \in N$ and
- $\xrightarrow{d}$ for $d \in \mathbb{R}^{\geq 0}$

are considered as normal (**visible**) transitions.

Example of Timed Bisimilar Automata



Example of Timed Non-Bisimilar Automata



Untimed Bisimilarity

Let A_1 and A_2 be timed automata. Let ϵ be a new (fresh) action.

Untimed Bisimilarity

We say that A_1 and A_2 are **untimed bisimilar** iff the transition systems $T(A_1)$ and $T(A_2)$ generated by A_1 and A_2 where **every transition of the form** $\xrightarrow{d}$ **for** $d \in \mathbb{R}^{\geq 0}$ **is replaced with** $\xrightarrow{\epsilon}$ are strongly bisimilar.

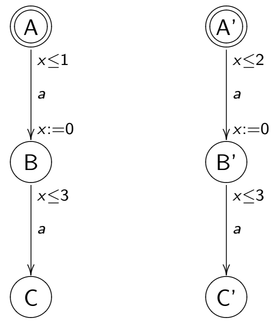
Remark:

- $\xrightarrow{a}$ for $a \in N$ is treated as a visible transition, while
- $\xrightarrow{d}$ for $d \in \mathbb{R}^{\geq 0}$ are all labelled by a single visible action $\xrightarrow{\epsilon}$.

Corollary

Any two timed bisimilar automata are also untimed bisimilar.

Timed Non-Bisimilar but Untimed Bisimilar Automata



Decidability of Timed and Untimed Bisimilarity

Theorem [Cerans'92]

Timed bisimilarity for timed automata is decidable in EXPTIME (deterministic exponential time).

Theorem [Larsen, Wang'93]

Untimed bisimilarity for timed automata is decidable in EXPTIME (deterministic exponential time).

Timed Traces

Let $A = (L, \ell_0, E, I)$ be a timed automaton over a set of clocks C and a set of labels N.

Timed Traces

A sequence $(t_1, a_1)(t_2, a_2)(t_3, a_3)\ldots$ where $t_i \in \mathbb{R}^{\geq 0}$ and $a_i \in N$ is called a **timed trace of** A iff there is a transition sequence

$$(\ell_0, v_0) \xrightarrow{d_1} \cdot \xrightarrow{a_1} \cdot \xrightarrow{d_2} \cdot \xrightarrow{a_2} \cdot \xrightarrow{d_3} \cdot \xrightarrow{a_3} \ldots$$

in A such that $v_0(x) = 0$ for all $x \in C$ and

$$t_i = t_{i-1} + d_i \qquad \text{where } t_0 = 0.$$

Intuition: t_i is the absolute time (**time-stamp**) when a_i happened since the start of the automaton A.

Timed and Untimed Language Equivalence

The set of all timed traces of an automaton A is denoted by $L(A)$ and called the **timed language of** A.

Theorem [Alur, Courcoubetis, Dill, Henzinger'94]

Timed language equivalence (the problem whether $L(A_1) = L(A_2)$ for given timed automata A_1 and A_2) is undecidable.

We say that $a_1 a_2 a_3 \ldots$ is an **untimed trace of** A iff there exist $t_1, t_2, t_3, \ldots \in \mathbb{R}^{\geq 0}$ such that $(t_1, a_1)(t_2, a_2)(t_3, a_3)\ldots$ is a timed trace of A.

Theorem [Alur, Dill'94]

Untimed language equivalence for timed automata is decidable.