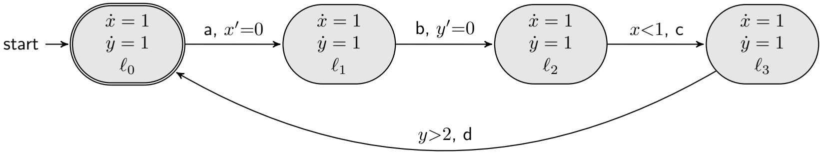
The Theory of Alur-Dill Timed Automata

Ashutosh Trivedi

Department of Computer Science and Engineering,
IIT Bombay

CS620: New Trends in IT: Modeling and Verification of Cyber-Physical Systems
(4 September 2013)

Timed Automata

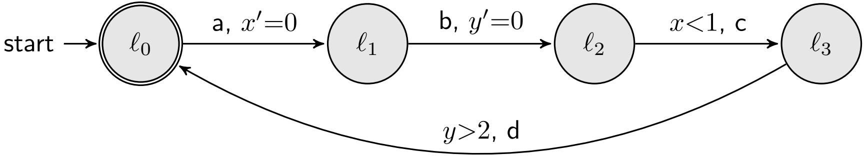


- Formalism introduced by Alur and Dill [AD94] to model real-time systems
- Hybrid automata with restricted dynamics for variables so that all variables grow with uniform rate, i.e.

$$\dot{x} = 1$$

  for all variables x is all modes.
- A number of verification problems of practical interest (reachability, model checking) are decidable
- Efficient symbolic algorithms are implemented in tools like UPPAAL [UPP], Kronos [Kro], and RED [RED]

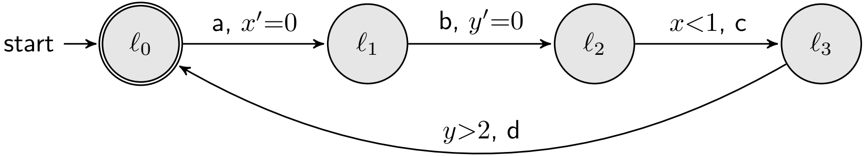
Timed Automata



A timed automaton is a tuple $\mathcal{T} = (L, L_0, \Sigma, C, \Delta, I, F)$ where:

- L is a finite set of locations,
- $L_0 \subseteq L$ is the set of initial locations,
- Σ is a finite set of actions,
- C is a finite set of clocks,
- $\Delta \subseteq L \times \mathrm{pred}(C) \times \Sigma \times \mathrm{pred}(C \cup C') \times L$ is the transition relation,
- $I : L \to \mathrm{pred}(C)$ is the invariant function, and
- $F \subseteq L$ is the set of final locations.

Clock Constraints and Resets



- Timed automata restrict predicates appearing as transition guards and as invariants to the set $\Phi(C)$ of clock constraints defined inductively as:

$$\delta := c \leq d \mid d \leq c \mid \neg\delta \mid \delta_1 \wedge \delta_2$$

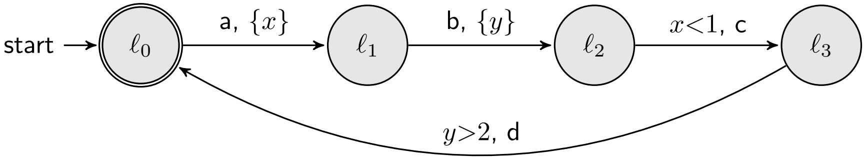
  where c is a clock in C and d is a constant in $\mathbb{Q}$.

- Timed automata also restrict variable update functions to be clock resets, i.e.

$$c' = 0 \wedge d' = 0$$

  Hence, we often represent variable updates via a subset $C' \subseteq C$ of clocks to be reset.

Timed Automata



A timed automaton is a tuple $\mathcal{T} = (L, L_0, \Sigma, C, \Delta, I, F)$ where:

- L is a finite set of locations,
- $L_0 \subseteq L$ is the set of initial locations,
- Σ is a finite set of actions,
- C is a finite set of clocks,
- $\Delta \subseteq L \times \Phi(C) \times \Sigma \times 2^C \times L$ is the transition relation,
- $I : L \to \Phi(C)$ is the invariant function, and
- $F \subseteq L$ is the set of final locations.

Also define deterministic variant.

Semantics of Timed Automata

- A clock valuation is a function $\nu : C \to \mathbb{R}_{\geq 0}$ that assigns values to the clocks.
- We can also write a valuation as a point in $\mathbb{R}_{\geq 0}^{|C|}$
- A clock constraint characterizes a convex subset of $\mathbb{R}_{\geq 0}^{|C|}$.
- For a clock constraints $G \in \Phi(C)$ we write $\nu \models G$ if ν satisfies G.

Semantics of Timed Automata

- A clock valuation is a function $\nu : C \to \mathbb{R}_{\geq 0}$ that assigns values to the clocks.
- We can also write a valuation as a point in $\mathbb{R}_{\geq 0}^{|C|}$
- A clock constraint characterizes a convex subset of $\mathbb{R}_{\geq 0}^{|C|}$.
- For a clock constraints $G \in \Phi(C)$ we write $\nu \models G$ if ν satisfies G.
- For a valuation $\nu \in \mathbb{R}_{\geq 0}^{|C|}$ and delay $t \in \mathbb{R}_{\geq 0}$ we define $(\nu{+}t)$ as a valuation such that

  $$(\nu{+}t)(c) \stackrel{\text{def}}{=} \nu(c) + t$$

  for all clocks $c \in C$.
- For a valuation $\nu \in \mathbb{R}_{\geq 0}^{|C|}$ and a reset set $C' \subseteq C$ we define $\nu[C'{:=}0]$ as a valuation such that

  $$\nu[C'{:=}0](c) \stackrel{\text{def}}{=} \begin{cases} \nu(c) & \text{if } c \notin C' \\ 0 & \text{otherwise} \end{cases}$$

  for all clocks $c \in C$.

Semantics of Timed Automata

A timed automaton is a tuple $\mathcal{T} = (L, L_0, \Sigma, C, \Delta, I, F)$ where:

- L is a finite set of locations,
- $L_0 \subseteq L$ is the set of initial locations,
- Σ is a finite set of actions,
- C is a finite set of clocks,
- $\Delta \subseteq L \times \Phi(C) \times \Sigma \times 2^C \times L$ is the transition relation,
- $I : L \to \Phi(C)$ is the invariant function, and
- $F \subseteq L$ is the set of final locations.

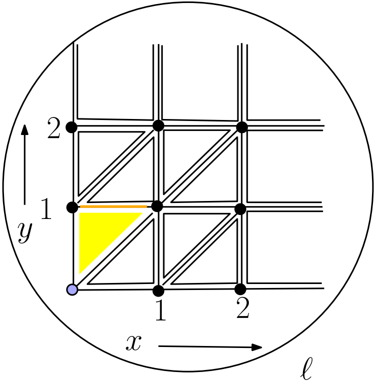
Semantics:

- Infinite state transition graph of configurations and timed moves
- Configuration $(\ell, \nu) \in L \times \mathbb{R}_{\geq 0}^{|C|}$
- Timed Moves $(t, a) \in \mathbb{R}_{\geq 0} \times \Sigma$
- Transition $(\ell, \nu) \xrightarrow{(t,a)} (\ell', \nu')$ exists iff there is $(\ell, G, a, C', \ell') \in \Delta$ s.t.
  - $\nu + t' \models I(\ell)$ for all $t' \in [0, t]$
  - $\nu + t \models G$, and
  - $\nu + t[C' := 0] = \nu'$ and $\nu' \models I(\ell')$.

Timed Automata as acceptors/generators of timed words

- Timed word $(a_0, t_0), (a_1, t_1), \ldots, (a_n, t_n) \in (\Sigma \times \mathbb{R}_{\geq 0})^n$ such that $t_i \geq t_{i-1}$ for all $i \geq 1$.
- Alternative representation (σ, τ)
- A run of a timed automata on a timed word
- Accepting word
- Language of a timed automaton
- Emptiness problem
- Examples

Emptiness Problem: Region Graph

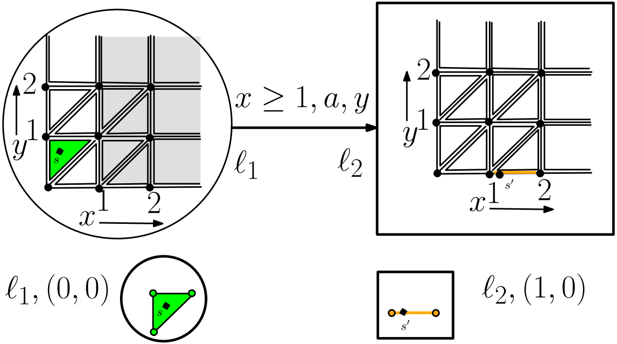


$x < 1, x > 0$
$y = 1$
THIN

$x < 1, x > 0$
$y < 1, y > 0$
$y - x > 0$
THICK

$x = 0, y = 0$
THIN

Emptiness Problem: Region Graph



R. Alur and D. Dill.
A theory of timed automata.
TCS, 126(2):183–235, 1994.

Kronos.
http://www-verimag.imag.fr/TEMPORISE/kronos/.

RED.
http://cc.ee.ntu.edu.tw/~farn/red/.

UPPAAL.
http://www.uppaal.com/.