A Clock-Optimal Hierarchical Monitoring Automaton for MITL

Deepak D'Souza and Raj Mohan M

Computer Science and Automation
Indian Institute of Science, Bangalore.

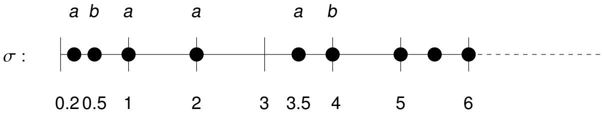
Contribution

A formula automaton construction for Metric Interval Temporal Logic (MITL):

- Uses Hierarchical Timed Buchi Automata
- More efficient in use of clocks than earlier constructions
- Optimal use of clocks

Metric Temporal Logic

- Models are timed words:



- Interpreted in continuous time.
- Syntax is given by:

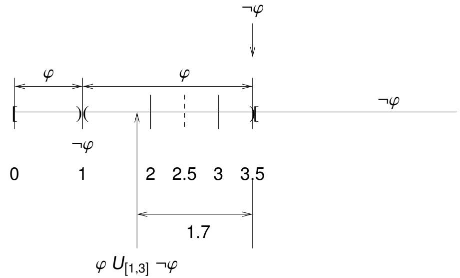
$$\varphi ::= a \mid \varphi_1 U_I \varphi_2 \mid \varphi_1 S_I \varphi_2 \mid \textit{boolean combinations}.$$

where

- $a \in \Sigma$.
- I is an interval like $[2,3]$, $(1,2.4]$, etc.

Semantics of U_I

Consider truth of a formula φ along the time word as shown below:

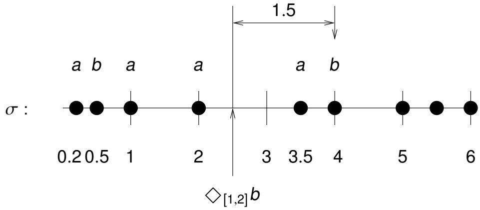


The formula $\varphi U_{[1,3]} \neg\varphi$ is true at 1.8.

Semantics of MTL Contd

Derived operator:

- $\Diamond_I \psi = \top U_I \psi$.



$\Diamond_{[1,2]} b$ is true at 1.5.

Metric Interval Temporal Logic

- Introduced by Alur, Feder and Henzinger [JACM 1996]
- Fragment of MTL in which the intervals are restricted to non-singular intervals.
- Formulas such as

$$\psi_1 U_{[2,2]} \psi_2$$

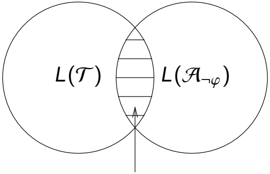
  are not allowed in MITL.

Formula Automaton for MITL

- Key to solving model checking and satisfiability problems for MITL.
- Formula automaton for φ accepts exactly the set of models of φ.
- Given a system $\mathcal{T}$ and a formula φ the model checking problem can be rephrased as whether

$$L(\mathcal{T}) \cap L(\mathcal{A}_{\neg\varphi}) = \emptyset,$$

where $\mathcal{A}_{\neg\varphi}$ is a formula automaton for $\neg\varphi$.



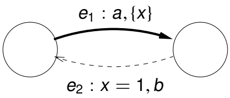
model checking problem: is $L(\mathcal{T}) \cap L(\mathcal{A}_{\neg\varphi}) = \emptyset$?

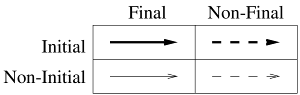
Hierarchical Timed Büchi Automaton

- We give an inductive monitoring automaton construction for MITL in terms of *Hierarchical Timed Büchi Automaton* (HTBA).
- An HTBA is a list $[C_n, \ldots, C_1]$ of automata where each of the C_i's is an *edge timed Büchi automaton*.

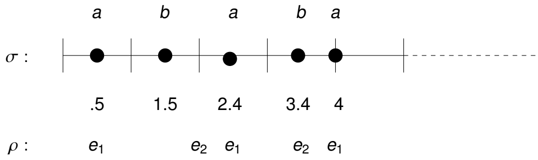
Edge Timed Büchi Automaton

An edge timed Büchi automaton is similar to a timed Büchi automaton but initial edges and final edges.



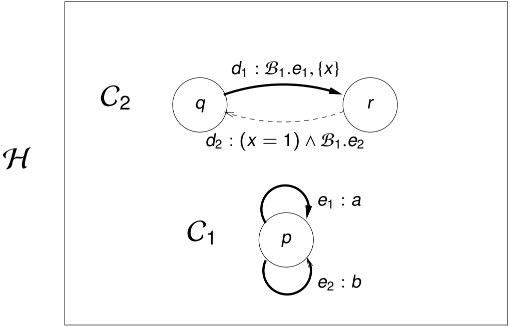


An example timed word σ and the run ρ of $\mathcal{A}$ over σ.



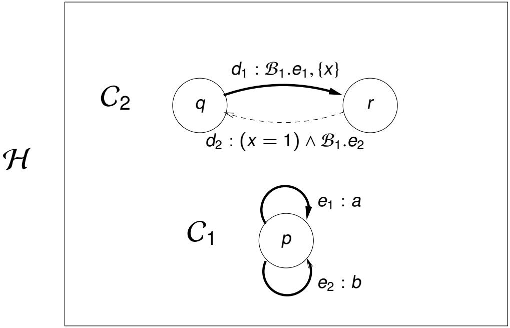
Hierarchical Timed Büchi Automaton

An HTBA $\mathcal{H} = [C_2, C_1]$.

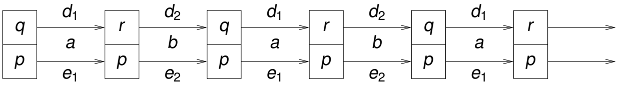


- In general an HTBA is a list $[C_n, \ldots, C_1]$ of automata.
- Automaton C_i can only refer to edges, clocks and states of the automata $C_{i-1}, \ldots, C_1$, hence the list is hierarchical.

Run of HTBA



The run of $\mathcal{H}$ over $(a, .5)(b, 1.5)(a, 2.4)(b, 3.4)(a, 4)\cdots$ is



Monitoring Automaton

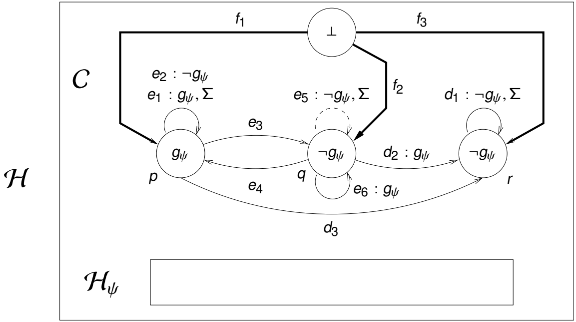
- A monitoring automaton for an MITL formula is an automaton which monitors the truth of the formula along its run over every timed word.
- An important tool for verification as one can build a formula automaton from it.

Properties of a Monitoring Automaton:

- A monitoring automaton is *universal*, i. e. it accepts all the timed words.
- A monitoring automaton is *unambiguous*, i. e. for every infinite timed word it has a unique accepting run over it.

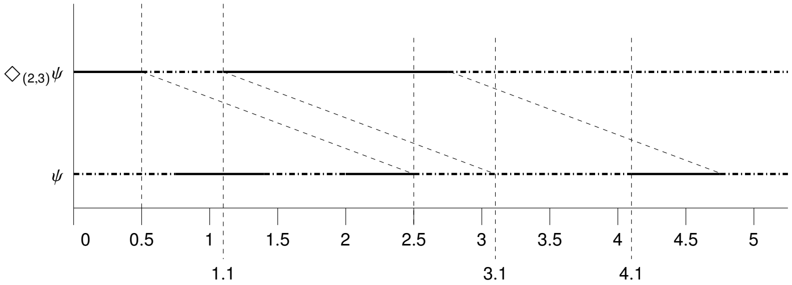
Construction: Monitoring HTBA for $\Diamond\psi$

Let $(\mathcal{H}_\psi, g_\psi)$ be the monitoring automaton for ψ. Then $([\mathcal{C}, \mathcal{H}_\psi], \mathcal{C}.(f_1 \vee f_2 \vee \bigvee_{i=1}^{6} e_i) \vee \mathcal{C}.(p \vee q))$ is a monitoring automaton for $\Diamond\psi$.



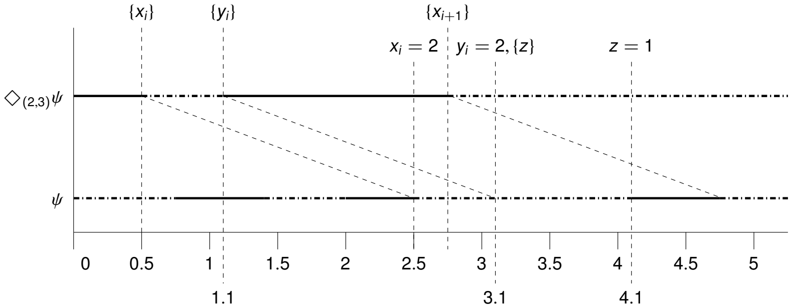
Construction for $\Diamond_I \psi$: Example $\Diamond_{(2,3)}\psi$

Relationship between the characteristic functions of ψ and $\Diamond_{(2,3)}\psi$ along a timed word.



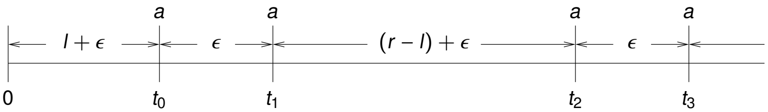
Construction (Sketch): Example $\Diamond_{(2,3)}\psi$

We use two automata for monitoring the formula $\Diamond_{(2,3)}\psi$: the first guesses the intervals in which the formula is false by resetting the clocks (x_i and y_i) and the second one verifies those guesses (using clock z and state information).



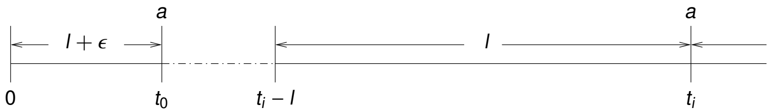
Clock Optimal for $\Diamond_I\psi$: Proof Sketch

- In the inductive step for monitoring automaton construction for $\Diamond_{(l,r)}\psi$ we use an optimal $(2 * \lceil l/(r-l) \rceil + 1)$ number of clocks.
- Consider the following timed word.
  1. $t_0 = l + \epsilon$.
  2. $\forall i \in \mathbb{N},\ t_{2i+1} - t_{2i} = \epsilon$.
  3. $\forall i \in \mathbb{N},\ t_{2i+2} - t_{2i+1} = r - l + \epsilon$.



Clock Optimality Contd

- At every time point $t \in (t_i - l, t_i)$ at least a clock is "tied" to the point $t_i - l$.



- No clock can be "tied" to two different points.
- There exists a point such that $2 * \lceil l/(r - l) \rceil + 1$ clocks are "tied".
- Our construction is clock-optimal.

Clock Optimality

- Our construction for the inductive step uses at most $2 * \lceil l/(r-l) \rceil + 1$ clocks.
- Previous constructions for monitoring TBA for the formulas of these forms use at least $2 * \lceil l/(r-l) \rceil + 2$ clocks.
- Similarly we also use an optimal number of clocks in the inductive step for monitoring automaton construction for $\diamondminus_I \psi$.

Thank You.