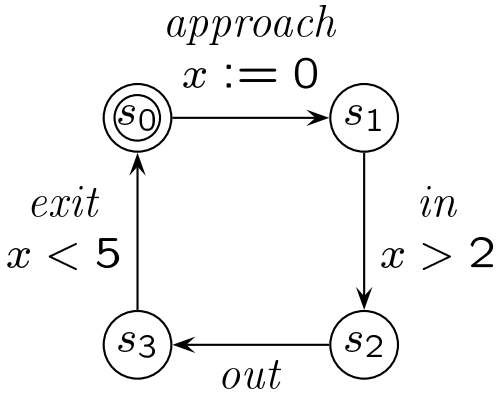
IT-højskolen
i København

Fully Symbolic Model Checking of Timed Systems using Difference Decision Diagrams

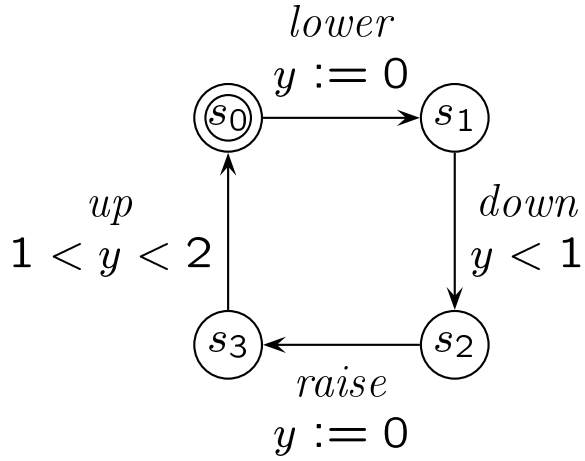
Jesper Møller, Jakob Lichtenberg,
Henrik R. Andersen & Henrik Hulgaard

The IT University in Copenhagen
Glentevej 67 • 2400 Copenhagen • Denmark

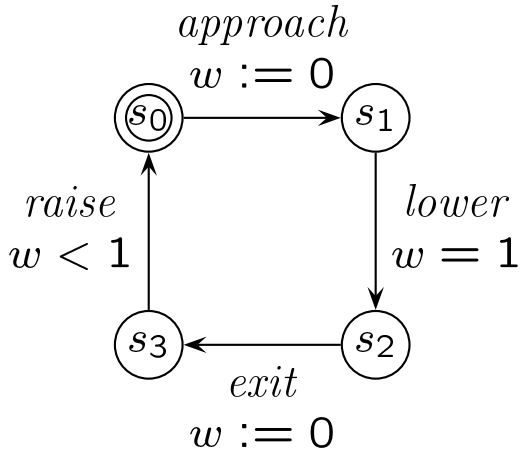
Example: Gate controller at a railroad crossing [Alur & Dill 91].



Train



Gate



Controller

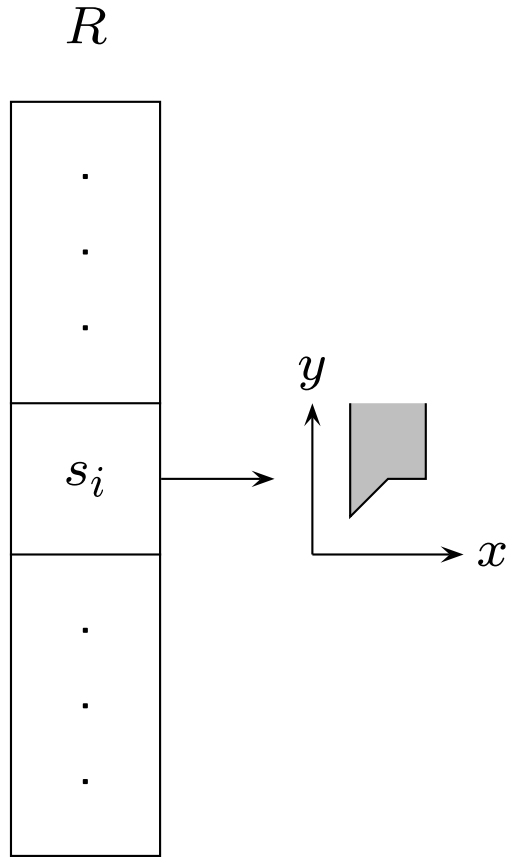
Safety When the train is inside the gate, the gate should be closed.

Liveness The gate should never be closed for more than 10 minutes.

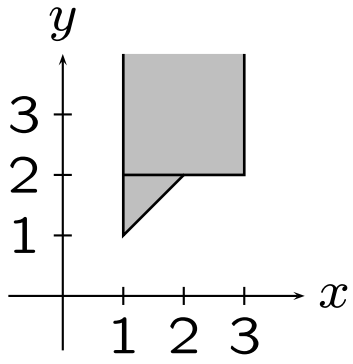
Current Approaches

IT-højskolen
i København

$Q \leftarrow \{(s_0, V_0)\}$
while $Q \neq \emptyset$ **do**
  Remove some (s, V) from Q
  $S \leftarrow \text{Next}(s, V)$
  for each $(s_i, V_i) \in S$ **do**
    if $V_i \not\subseteq R[s_i]$ **then**
      Add (s_i, V_i) to Q
      $R[s_i] \leftarrow R[s_i] \cup V_i$



DBM-based representation [Uppaal]



$$\begin{array}{c} \\ 0 \\ x \\ y \end{array} \begin{array}{c} \begin{array}{ccc} 0 & x & y \end{array} \\ \begin{bmatrix} 0 & 3 & \infty \\ -1 & 0 & \infty \\ -2 & 1 & 0 \end{bmatrix} \end{array} \qquad \begin{array}{c} \\ 0 \\ x \\ y \end{array} \begin{array}{c} \begin{array}{ccc} 0 & x & y \end{array} \\ \begin{bmatrix} 0 & 2 & 2 \\ -1 & 0 & 1 \\ -1 & 0 & 0 \end{bmatrix} \end{array}$$

Disadvantages:

1. The number of DBMs for representing $R[s_i]$ can become very large.
2. There is no sharing of DBMs between different states.
3. Each discrete state is enumerated explicitly.

A Symbolic Approach

IT-højskolen
i København

Represent a set of states as a formula ϕ.

$\phi \leftarrow \phi_0$
$R \leftarrow \phi$
while $\phi \not\equiv \mathit{false}$ **do**
  $\phi \leftarrow \mathsf{Next}(\phi) \wedge \neg R$
  $R \leftarrow R \vee \phi$

$$R \;=\; \Big((s_0 \vee s_1) \wedge 0 \leq x - y < 5\Big) \vee \cdots$$

We need : 1. A logic to express formulas in.
2. Next(ϕ).
3. A data structure for representing formulas.

Outline

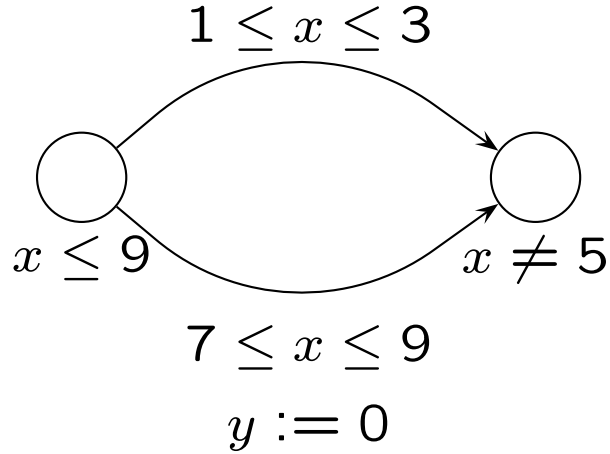
IT-højskolen
i København

- Timed guarded commands
- Symbolic reachability analysis
- Difference decision diagrams
- Experimental results

Timed Guarded Commands

IT-højskolen
i København

$$
\begin{aligned}
G &= (\{b\}, \{x, y\}, T, I)\,, \\
T &= \left\{ \begin{array}{ll} b \wedge (1 \leq x \leq 3) \rightarrow b & := \mathsf{false} \\ b \wedge (7 \leq x \leq 9) \rightarrow b, y & := \mathsf{false}, 0 \end{array} \right\}, \\
I &= \Big(b \Rightarrow (x \leq 9)\Big) \wedge \Big(\neg b \Rightarrow (x \neq 5)\Big)\,.
\end{aligned}
$$



Transitional Semantics

IT-højskolen
i København

A program state: $s = [x \mapsto 8.0,\ y \mapsto 0.0,\ b \mapsto \mathit{false}]$.

- **Discrete transition**

  Firing $x < 5.0 \ \rightarrow \ b, x := \mathit{true}, 0.0$:

  $$s' = [x \mapsto 0.0,\ y \mapsto 0.0,\ b \mapsto \mathit{true}]$$

- **Timed transition**

  Advancing time by 2.5:

  $$s' = [x \mapsto 10.5,\ y \mapsto 2.5,\ b \mapsto \mathit{false}]$$

The Logic

The logic to express formulas in :

$$\phi \ ::= \ x - y \leq d \mid \neg\phi \mid \phi_1 \wedge \phi_2 \mid \exists x.\phi \, .$$

We introduce the variable z representing "zero" or "current time".

Replace $x \leq d$ by $x - z \leq d$. Replace $x := d$ by $x := z + d$.

Example:

$$x \leq 5 \ \rightarrow \ y := 1 \qquad \text{becomes} \qquad x - z \leq 5 \ \rightarrow \ y := z + 1$$

Discrete Transitions

IT-højskolen
i København

Firing $g \to \vec{v} := \vec{d}$:

$$\frac{s \models g \quad s[\vec{v} := \vec{d}] \models I}{s \to s[\vec{v} := \vec{d}]}$$

$$\mathsf{Next}_{\mathsf{discrete}}(\phi,\ g \to \vec{v} := \vec{d}) \ = \ (\phi \wedge g)[\vec{v} := \vec{d}] \wedge I$$

Advancing time using the z-variable

IT-højskolen i København

Advancing all clocks by δ:

$$\phi[\vec{c} := \vec{c} + \delta] \;=\; \phi[z := z - \delta] \;=\; \Big(\exists z.(\phi \wedge z' = z - \delta)\Big)[z/z']$$

Timed Transitions

IT-højskolen
i København

Advance time by δ :

$$\frac{\delta \geq 0 \quad \forall \delta'.0 \leq \delta' \leq \delta : s[\vec{c} := \vec{c} + \delta'] \models I}{s \xrightarrow{\delta} s[\vec{c} := \vec{c} + \delta]}$$

Predicate stating whether z' is a legal zero-point :

$$P_{\mathsf{next}} \;=\; z' \leq z \;\wedge\; \forall z''.(z' \leq z'' \leq z \Rightarrow I[z''/z])$$

$$\mathsf{Next}_{\mathsf{timed}}(\phi, \delta) \;=\; \Big(\exists z.(\phi \;\wedge\; z' = z - \delta \;\wedge\; P_{\mathsf{next}})\Big)[z/z']$$

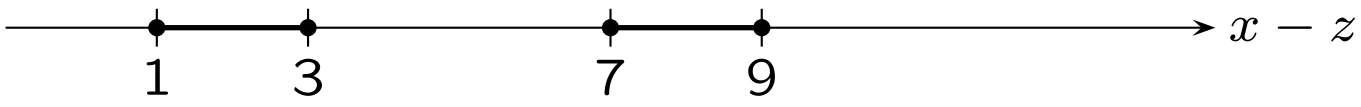
$$\mathsf{Next}_{\mathsf{timed}}(\phi) \;=\; \bigvee_{\delta \in \mathbb{R}} \mathsf{Next}_{\mathsf{timed}}(\phi, \delta) \;=\; \Big(\exists z.(\phi \wedge P_{\mathsf{next}})\Big)[z/z']$$

Example

IT-højskolen i København

Consider the formula

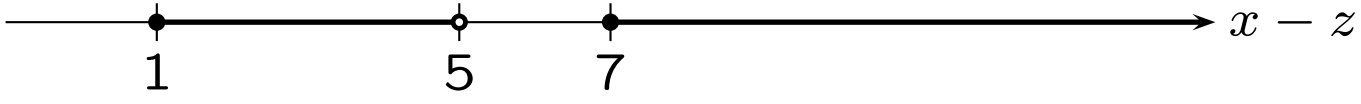
$$\phi \;=\; (1 \leq x - z \leq 3) \vee (7 \leq x - z \leq 9)$$



and the state-invariant $I \;=\; x - z \neq 5$.

Advancing time from ϕ:

$$\mathsf{Next}_{\mathsf{timed}}(\phi) \;=\; (1 \leq x - z < 5) \vee (7 \leq x - z)$$



The 3 Ingredients

- ✓ A logic
- ✓ Next(ϕ)
- ☛ A data structure

Difference Decision Diagrams

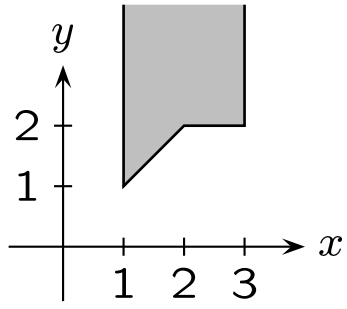
IT-højskolen i København

Implicit representation of:

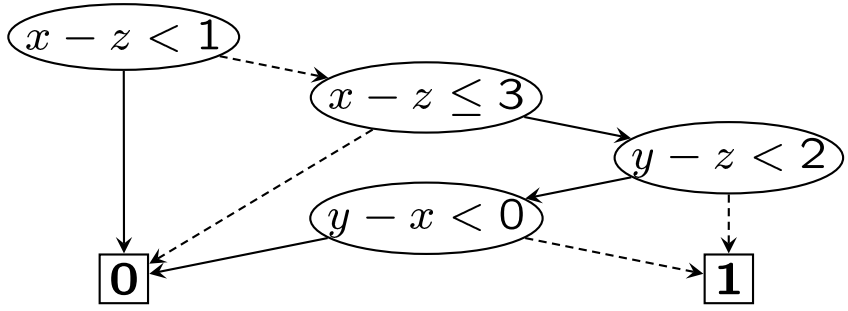
$$\phi \ ::= \ x - y \leq d \mid \neg\phi \mid \phi_1 \wedge \phi_2 \mid \exists x.\phi\,.$$

Example

$$\phi \ = \ 1 \leq x - z \leq 3 \ \wedge \ (y - z \geq 2 \ \vee \ y - x \geq 0)$$

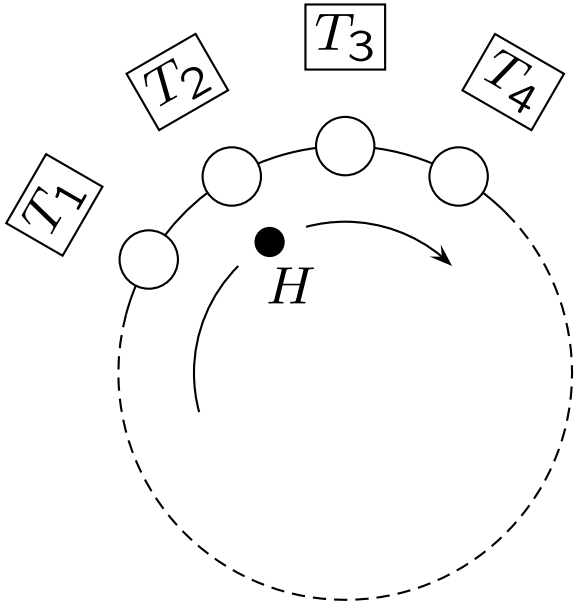


(x, y)-plot for $z = 0$



Difference decision diagram

Milner's Scheduler [Milner 89]



$$
\begin{array}{lcll}
c_i \wedge \neg t_i & \rightarrow & H, T_i, t_i, c_i, h_i & := 0, 0, \mathsf{T}, \mathsf{F}, \mathsf{T} \\
h_i \wedge H^l \leq H & \rightarrow & c_{(i \bmod N)+1}, h_i & := \mathsf{T}, \mathsf{F} \\
t_i \wedge T^l \leq T_i & \rightarrow & t_i & := \mathsf{F}
\end{array}
$$

$$I = \bigwedge_{i=1}^{N} (h_i \Rightarrow H \leq H^u) \wedge (t_i \Rightarrow T_i \leq T^u)$$

Experimental Results

IT-højskolen i København

N	Kronos	Uppaal	DDD
4	0.2	0.1	0.1
5	0.7	0.2	0.1
6	22.6	0.6	0.1
7	339.2	2.3	0.1
8	–	9.0	0.2
9	–	35.0	0.2
10	–	138.4	0.2
11	–	529.8	0.2
12	–	2560.7	0.3
16	–	–	0.5
32	–	–	2.2
64	–	–	15.9
128	–	–	123.3
256	–	–	1104.8

(a) 1 clock.

N	Kronos	Uppaal	DDD
4	0.4	0.2	0.2
5	2.4	1.7	0.3
6	24.2	17.6	0.5
7	346.6	201.7	0.5
8	–	2460.2	0.6
16	–	–	1.5
32	–	–	5.7
64	–	–	31.7
128	–	–	217.3

(b) $N + 1$ clocks.

Conclusion

IT-højskolen i København

- Symbolic model checking of timed systems requires a data structure and a decision procedure for the logic :

$$\phi \ ::= \ x - y \leq d \mid \neg\phi \mid \phi_1 \wedge \phi_2 \mid \exists x.\phi \, .$$

- Advancing time amounts to existential quantification of the z-variable.

- TCTL formulas can be verified by letting time go backwards.