Modeling and Analysis of Hybrid Systems

Algorithmic analysis for linear hybrid systems

Prof. Dr. Erika Ábrahám

Informatik 2 - Theory of Hybrid Systems
RWTH Aachen University

SS 2015

Literature

Alur et al.: The algorithmic analysis of hybrid systems

Theoretical Computer Science, 138(1):3–34, 1995

Linear terms, constraints and formulas

- A linear term e over a set Var of variables is of the form

  $$e ::= c \mid c \cdot x \mid e + e$$

  where $x \in Var$ is a variable and c stays for an integer (rational) constant.

  Example: $x_1 + 2x_2 + 5x_3$ is a linear term over $Var = \{x_1, x_2, x_3\}$.

- A linear constraint t over Var is an (in)equality

  $$t ::= e \sim 0$$

  with $\sim \in \{>, \geq, =, \leq, <\}$ and e a linear term over Var.

  Example: $x_1 + 2x_2 + (-2) \geq 0$ is a linear constraint over $Var = \{x_1, x_2\}$. We sometimes deviate from this normal form and write, e.g., $x_1 + 2x_2 \geq 2$.

Linear terms, constraints and formulas

- A conjunctive linear formula φ over Var is defined by the following grammar:

$$\varphi ::= t \mid \varphi \land \varphi \mid \exists x.\ \varphi$$

  with t a linear constraint over Var and $x \in Var$ a variable. Let Φ_X be the set of all conjunctive linear formulas with free (non-quantified) variables from $X \subseteq Var$.

  Example: $\exists t.\ \exists x_1.\ x_1 \geq 0 \land x_1' = x_1 + 2t \land t \geq 0$ is a conjunctive linear formula over $\{x_1, x_1', t\}$, with free (non-quantified) variables $\{x_1'\}$.
- A region over Var is a pair $(l, \varphi) \in Loc \times \Phi_{Var}$ of a location and a conjunctive linear formula with free variables from Var.

  Example: $(l, \exists t.\ \exists x_1.\ x_1 \geq 0 \land x_1' = x_1 + 2t \land t \geq 0)$ is a region over $\{x_1'\}$.
- We will use the intersection of two sets $P_1, P_2 \subseteq Loc \times \Phi_{Var}$ of regions, defined as

$$P_1 \hat{\cap} P_2 = \{(l, \varphi_1 \land \varphi_2) \mid (l, \varphi_1) \in P_1, (l, \varphi_2) \in P_2\}\ .$$

Substitution

- Assume a set Var of variables, a linear formula $\varphi \in \Phi_{Var}$ over Var, a variable $x \in Var$, and a linear term e over Var. The substitution $\varphi[e/x]$ replaces each free occurrence of x in φ by e.

  Example: $(x + 2y \leq 0)[5/y] = x + 2 \cdot 5 \leq 0$

  Example: $(\exists y.\ x + 2y \leq 0)[5/y] = x + 2y \leq 0$
- We also write $\varphi[e_1, \ldots, e_n/x_1, \ldots, x_n]$ instead of $\varphi[e_1/x_1] \ldots [e_n/x_n]$.
- For $Var = \{x_1, \ldots, x_n\}$ we will also use a primed variable set $Var' = \{x'_1, \ldots, x'_n\}$ and write short $\varphi[Var'/Var]$ for $\varphi[x'_1/x_1] \ldots [x'_n/x_n]$.

Linear terms, constraints and formulas

The semantics of linear terms, constraints and formulas over $Var = \{x_1, \ldots, x_n\}$ in the context of a valuation $\nu \in V_{Var}$ (i.e., $\nu : Var \to \mathbb{R}$) is as usual (we use the same notation for the syntax and the semantics of constants and operators):

$$
\begin{array}{lcl}
\nu(c) & \equiv & c \\
\nu(c \cdot x) & \equiv & c \cdot \nu(x) \\
\nu(e_1 + e_2) & \equiv & \nu(e_1) + \nu(e_2) \\
\nu(e \sim 0) & \equiv & \nu(e) \sim 0 \\
\nu(\varphi_1 \wedge \varphi_2) & \equiv & \nu(\varphi_1) \textit{ and } \nu(\varphi_2) \\
\nu(\exists x.\ \varphi) & \equiv & \textit{exists } v \in \mathbb{R} \textit{ such that } \nu(\varphi[v/x]) \textit{ holds}
\end{array}
$$

$[\![c]\!]_\nu = c$

Linear terms, constraints and formulas

The solution set $Sat(\varphi)$ of a linear formula φ over Var is the set of all valuations $\nu \in V_{Var}$ that make φ true:

$$Sat(\varphi) = \{\nu \in V_{Var} \mid \nu(\varphi) \text{ holds}\}$$

The solution set $Sat((l, \varphi))$ of a region $(l, \varphi) \in Loc \times \Phi_{Var}$ over Loc and Var is

$$Sat((l, \varphi)) = \{(l, \nu) \in Loc \times V_{Var} \mid \nu(\varphi) \text{ holds}\}$$

Two region sets $P_1, P_2 \subseteq Loc \times \Phi_{Var}$ are equivalent, written $P_1 \hat{=} P_2$, iff

$$\bigcup_{R \in P_1} Sat(R) = \bigcup_{R \in P_2} Sat(R) \ .$$

We define similarly the inclusion $P_1 \hat{\subseteq} P_2$ iff

$$\bigcup_{R \in P_1} Sat(R) \subseteq \bigcup_{R \in P_2} Sat(R) \ .$$

Linear hybrid automata I

A linear hybrid automaton is a hybrid automata $\mathcal{H} = (Loc, Var, Lab, Edge, Act, Inv, Init)$ with the following restrictions:

- Edges $e = (l, \mu_e, l')$ are represented as $(l, \varphi_e^{guard}, \varphi_e^{reset}, l')$ with $\varphi_e^{guard} \in \Phi_{Var}$ and $\varphi_e^{reset} \in \Phi_{Var \cup Var'}$, where the transition relation μ_e is given as:

  $$\mu_e = \{(\nu, \nu') \in V_{Var} \times V_{Var} \mid \nu \in Sat(\varphi_e^{guard}) \textit{ and } (\nu \oplus \nu') \in Sat(\varphi_e^{reset})\}$$

  where $(\nu \oplus \nu')(x) = \nu(x)$ for $x \in Var$ and $(\nu \oplus \nu')(x') = \nu'(x)$ for $x' \in Var'$.

- For each location $l \in Loc$, the activities are specified by a conjunctive linear formula of the form $\texttt{Act}_l = \bigwedge_{i=1}^{n} x_i + k_{l,i}^{lower} t \leq x_i' \wedge x_i' \leq x_i + k_{l,i}^{upper} t$, defining

  $$Act(l) = \{f : \mathbb{R}_{\geq 0} \to V_{Var} \mid \dot{f} \in [k_l^{lower}, k_l^{upper}]\} .$$

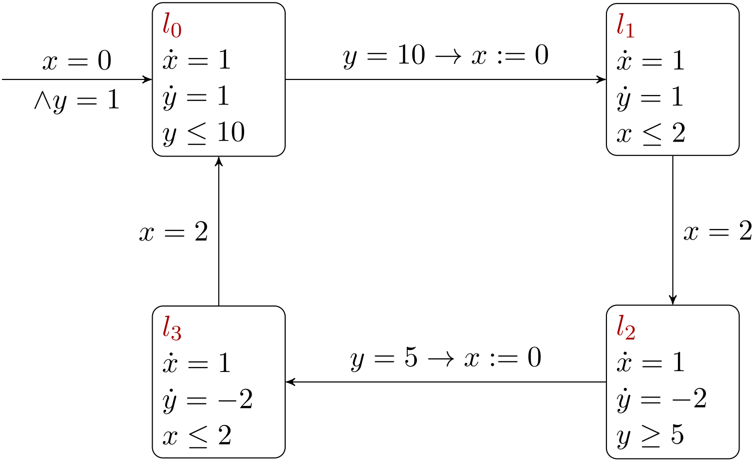
- Each invariant $Inv(l)$ is defined by a $\texttt{Inv}_l \in \Phi_{Var}$ as

$$Inv(l) = \{\nu \in V_{Var} \mid \nu \in Sat(\texttt{Inv}_l)\} .$$

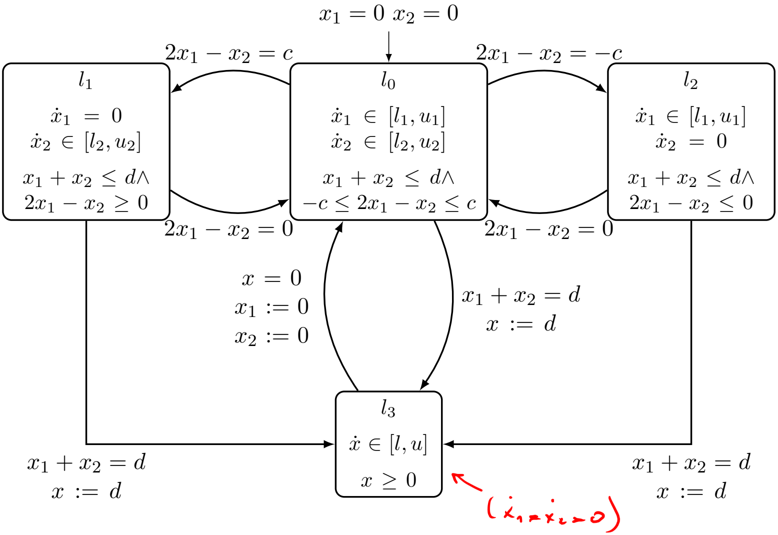
- The initial states $Init$ are specified by a finite set $\texttt{Init} \subset Loc \times \Phi_{Var}$ of regions as

$$Init = \bigcup_{(l,\varphi)\in\texttt{Init}} \{(l, \nu) \mid \nu \in Sat(\varphi)\} .$$

Water-level monitor



$$0 < l_1 < u_1,\ 0 < l_2 < u_2,\ l \leq u \leq 0,\ d > 0,\ c > 0$$



Reminder: Semantics of hybrid automata

$$\frac{(l, a, \mu, l') \in Edge \quad (\nu, \nu') \in \mu \quad \nu' \in Inv(l')}{(l, \nu) \xrightarrow{a} (l', \nu')} \quad \texttt{Rule}_{\texttt{Discrete}}$$

$$\frac{\begin{array}{c} f \in Act(l) \quad f(0) = \nu \quad f(t) = \nu' \\ t \geq 0 \quad \forall 0 \leq t' \leq t.f(t') \in Inv(l) \end{array}}{(l, \nu) \xrightarrow{t} (l, \nu')} \quad \texttt{Rule}_{\texttt{Time}}$$

lin. HA → $f(t) \in Inv(l)$

Forward analysis

- Given a set if initial states $Init \subseteq \Sigma$, we want to compute the set of all states which are reachable from $Init$:

$$Reach^{+}(Init) = \{\sigma' \in \Sigma \mid \exists \sigma \in Init.\ \sigma \rightarrow^{*} \sigma'\}\ .$$

- Given a set if initial states $Init \subseteq \Sigma$, we want to compute the set of all states which are reachable from $Init$:

$$Reach^{+}(Init) = \{\sigma' \in \Sigma \mid \exists \sigma \in Init.\ \sigma \rightarrow^{*} \sigma'\}\ .$$

- More specifically, we want to check whether the reachable region intersects with a set of bad (unsafe) states.

Forward reachability analysis

(*) unsat if non-empty intersection with Bad

```
method forward_reach() {
  i := 0;
  P_0 := {T_l^+(R) | R = (l,φ) ∈ Init}; //time successors of initial
  while P_i ≠ ∅ {
     //compute time successors of
     //discrete successors of all regions from P_i
     for each (R = (l,ϕ) ∈ P_i) {
        for each e = (l,·,·,l') ∈ Edge {
         R' := T_{l'}^+(D_e^+(R));
         if ({R'} ∩̂ P^bad ≠ ∅)
            return unsafe;
         else if (not {R'} ⊆̂ ⋃_{j=0}^{i} P_j)
            P_{i+1} := P_{i+1} ∪ {R'};
        }
     }
     i := i+1;
  }
  return safe;
}
```

∩̂ Inv_e

One-step reachability under time steps

- We define the forward time closure $\mathcal{T}_l^+(\varphi)$ of a formula $\varphi \in \Phi_{Var}$ at $l \in Loc$ as

$$\mathcal{T}_l^+(\varphi) = \exists x_{pre}.\ \exists t.\ t \geq 0 \wedge \varphi[x_{pre}/x] \wedge \texttt{Act}_l[x_{pre}, x/x, x'] \wedge \texttt{Inv}_l$$

- Region $R = (l, \varphi) \in Loc \times \Phi_{Var}$:

$$\mathcal{T}_l^+(R) = (l, \mathcal{T}_l^+(\varphi))$$

- Set of regions $P \subseteq Loc \times \Phi_{Var}$:

$$\mathcal{T}^+(P) = \{\mathcal{T}_l^+(R) \mid R = (l, \varphi) \in P\}$$

One-step reachability under discrete steps

- We define the postcondition $\mathcal{D}_e^+(\varphi)$ of a formula $\varphi \in \Phi_{Var}$ with respect to an edge $e = (l, \varphi_e^{guard}, \varphi_e^{reset}, l')$ as

$$\mathcal{D}_e^+(\varphi) = \exists x_{pre}.\ \varphi[x_{pre}/x] \wedge \varphi_e^{guard}[x_{pre}/x] \wedge \varphi_e^{reset}[x_{pre}, x/x, x'] \wedge \mathtt{Inv}_{l'}.$$

→ F.M.

- Region $R = (l, \varphi) \in Loc \times \Phi_{Var}$:

$$\mathcal{D}_e^+(R) = (l', \mathcal{D}_e^+(\varphi))$$

- Set of regions $P \subseteq Loc \times \Phi_{Var}$:

$$\mathcal{D}^+(P) = \{\mathcal{D}_e^+(R) \mid R = (l, \varphi) \in P,\ e = (l, \varphi_e^{guard}, \varphi_e^{reset}, l') \in \mathtt{Edge}\}$$

Fourier-Motzkin variable elimination

$$\exists x.\ \varphi \iff \varphi'$$

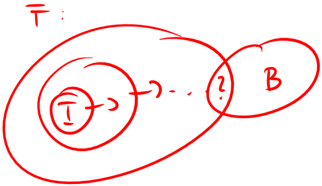
$$l_1 \le x \wedge \ldots \wedge l_n \le x \wedge x \le u_1 \wedge \ldots \wedge x \le u_m \wedge \varphi_{rest}$$

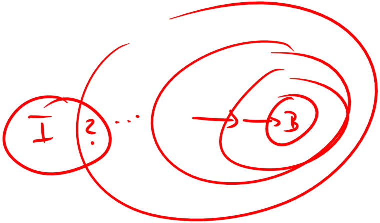
$$\begin{matrix} l_1 \\ \vdots \\ l_n \end{matrix} \le x \le \begin{matrix} u_1 \\ \vdots \\ u_m \end{matrix} \iff \forall i,j.\ l_i \le u_j$$

Backward analysis

- Given a set if target states $B \subseteq \Sigma$, we want to compute the set of all states from which a state in B is reachable:

$$Reach^{-}(B) = \{\sigma \in \Sigma \mid \exists \sigma' \in B.\ \sigma \rightarrow^{*} \sigma'\}\ .$$





- Given a set if target states $B \subseteq \Sigma$, we want to compute the set of all states from which a state in B is reachable:

$$Reach^{-}(B) = \{\sigma \in \Sigma \mid \exists \sigma' \in B.\ \sigma \to^{*} \sigma'\}\ .$$

- More specifically, we want to check whether the set of backward reachable states intersects with a set of initial states.

Backward reachability analysis

+ Inv + check intersec. with initial

```
method backward_reach() {
  i := 0;
  P_0 := {T_l^-(R) | R = (l,φ) ∈ P^bad}; //time predec. of bad regions
  while P_i ≠ ∅ {
     //compute time predecessors of
     //discrete predecessors of all regions from P_i
     for each (R = (l,ϕ) ∈ P_i) {
        for each e = (l',·,·,l) ∈ Edge {
         R' := T_{l'}^-(D_e^-(R));
         if ({R'} ∩̂ Init ≠ ∅)
            return unsafe;
         else if (not {R'} ⊆̂ ⋃_{j=0}^{i} P_j)
            P_{i+1} := P_{i+1} ∪ {R'};
        }
     }
     i := i+1;
  }
  return safe;
}
```

One-step reachability under time steps

$T_l^-(\varphi)$ $\quad x, v \xrightarrow{t} x_{post}, v_{post} \quad \varphi$

- We define the backward time closure $\mathcal{T}_l^-(\varphi)$ of a formula $\varphi \in \Phi_{Var}$ at $l \in Loc$ as

$$\mathcal{T}_l^-(\varphi) = \exists x_{post}.\ \exists t.\ t \geq 0 \wedge \varphi[x_{post}/x] \wedge \texttt{Act}_l[x, x_{post}/x, x'] \wedge \texttt{Inv}_l\ .$$

- Region $R = (l, \varphi) \in Loc \times \Phi_{Var}$:

$$\mathcal{T}_l^-(R) = (l, \mathcal{T}_l^-(\varphi))$$

- Set of regions $P \subseteq Loc \times \Phi_{Var}$:

$$\mathcal{T}^-(P) = \{\mathcal{T}_l^-(R) \mid R = (l, \varphi) \in P\}$$

One-step reachability under discrete steps

- We define the precondition $\mathcal{D}_e^-(\varphi)$ of a formula $\varphi \in \Phi_{Var}$ with respect to an edge $e = (l, \varphi_e^{guard}, \varphi_e^{reset}, l')$ as

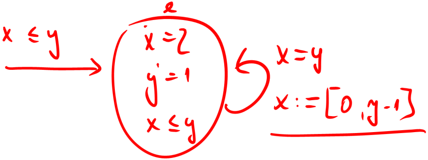
$$\mathcal{D}_e^-(\varphi) = \exists x_{post}.\ \varphi[x_{post}/x] \wedge \varphi_e^{guard} \wedge \varphi_e^{reset}[x, x_{post}/x, x'] \wedge \mathtt{Inv}_l.$$

- Region $R = (l', \varphi) \in Loc \times \Phi_{Var}$:

$$\mathcal{D}_e^-(R) = (l, \mathcal{D}_e^-(\varphi))$$

- Set of regions $P \subseteq Loc \times \Phi_{Var}$:

$$\mathcal{D}^-(P) = \{\mathcal{D}_e^-(R) \mid R = (l', \varphi) \in P,\ e = (l, \varphi_e^{guard}, \varphi_e^{reset}, l') \in \mathtt{Edge}\}$$



$Init = \{ (\ell, x \le y) \}$

$P_0 = T^+(Init) = \{ (\ell, \exists t . \exists x_{pre}, y_{pre} . x_{pre} \le y_{pre} \wedge t \ge 0 \wedge x = x_{pre} + 2t \wedge y = y_{pre} + t \wedge x \le y) \}$

$x_{pre} = x - 2t \qquad y_{pre} = y - t$

$= \{ (\ell, \exists t . x - 2t \le y - t \wedge t \ge 0 \wedge x \le y) \}$

$x - y \le t \qquad 0 \le t$

$\overset{F.M.}{=} \{ (\ell, x \le y) \}$

$D_e^+(P_0) = \{ (\ell, \exists x_{pre}, y_{pre} . x_{pre} \le y_{pre} \wedge \underbrace{x_{pre} = y_{pre}}_{(1)} \wedge 0 \le x \wedge x \le y_{pre} - 1 \wedge \underbrace{y = y_{pre}}_{(2)} \wedge x \le y) \}$

$= \{ (\ell, \exists y_{pre} . y_{pre} \le y_{pre} \wedge 0 \le x \wedge x \le y_{pre} - 1 \wedge y = y_{pre} \wedge x \le y) \}$

$= \{ (\ell, 0 \le x \wedge x \le y - 1) \}$