Hybrid Systems
Modeling, Analysis and Control

Radu Grosu
Vienna University of Technology

Lecture 12
Reachability Analysis
Using Interval Approximation

Constraints for Hybrid Systems

Variables:

- Discrete (mode) var: $s \in S = \{s_1,\ldots,s_n\}$
- Continuous vars: $x_1,\ldots,x_k \in I_1,\ldots,I_k$
- Derivatives: $\dot{x}_1,\ldots,\dot{x}_k \in I_1,\ldots,I_k$
- Jump targets: $s', x'_1,\ldots,x'_k \in S, I_1,\ldots,I_k$
- State space: $\Phi = S \times I_1 \times \ldots \times I_k$

Constraints are:

- Boolean combinations of inequalities over terms

Terms contain:

- Function symbols in $\{+,\times,\exp,\sin,\ldots\}$ and constants
- Variable symbols $s,s',x_1,\ldots,x_k,x'_1,\ldots,x'_k$ and $\dot{x}_1,\ldots,\dot{x}_k$

Hybrid Systems (HS)

A HS is a tuple (Flow, Jump, Init, Unsafe) where:

- $\text{Flow}(s,x_1,\dots,x_k,\dot{x}_1,\dots,\dot{x}_k) \subseteq \Phi \times \mathbb{R}^k$: is a flow constraint
- $\text{Jump}(s,x_1,\dots,x_k,s',x'_1,\dots,x'_k) \subseteq \Phi \times \Phi$: is a jump constraint
- $\text{Init}(s,x_1,\dots,x_k) \subseteq \Phi$: is a state-space constraint
- $\text{Unsafe}(s,x_1,\dots,x_k) \subseteq \Phi$: is a state-space constraint

Example:

- Flow_1: $(s = s_1 \Rightarrow \dot{x} = x) \wedge (s = s_2 \Rightarrow \dot{x} = -x)$
- Flow_2: $\dot{x}_1 = x_1 - x_2 \wedge \dot{x}_2 = -x_1 - x_2 \wedge x_1 > 1 \wedge x_1 < 3 \wedge x_2 > 1 \wedge x_2 < 3$
- Jump_1: $(s = s_1 \wedge x \geq 10) \Rightarrow (s' = s_2 \Rightarrow x' = 0)$
- Init_2: $s = s_1 \wedge x_1 > 1 \wedge x_1 < 3 \wedge x_2 > 1 \wedge x_2 < 3$
- Unsafe_2: $s = s_2 \wedge x_1 > 2 \wedge x_1 < 3 \wedge x_2 > 2 \wedge x_2 < 3$

Trajectory of a Hybrid System

A flow of length l in mode s: function $r : [0,l] \mapsto \Phi$:

- The countinuous projection of r : is differentiable
- For all $t \in [0,l]$ the mode of r(t) is s

A trajectory: sequence of flows $r_0 \ldots r_p$ of length $l_0 \ldots l_p$:

- If $i > 0$ then: $(r_{i-1}(l_{i-1}),\ r_i(0)) \in \mathrm{Jump}$
- If $l_i > 0$ then: $\forall t \in [0,l_i].\ (r_i(t),\ \dot{r}_i(t)) \in \mathrm{Flow}$

A HS is safe iff there is no trajectory $r_0 \ldots r_p$:

- $r_0(0) \in \mathrm{Init}$
- $r_p(l_p) \in \mathrm{Unsafe}$

Discrete Systems (DS): Reachability

Discrete transition system (Trans, Init, Unsafe) over S:

- S is a finite set (the states)
- $Trans \subseteq S \times S$: is the transition relation
- $Init \subseteq S$: is the set of initial states
- $Unsafe \subseteq S$: is the set of bad states

Trajectory of a DS over S: a function $r \in \{0,\ldots,p\} \mapsto S$:

- For all $t \in \{1,\ldots,p\}$. $(r(t-1), r(t)) \in Trans$
- Safe DS: $\neg\exists r.\ r(0) \in Init \wedge r(p) \in Unsafe$

Discrete Abstraction of an HS

Discrete abstracton of an HS:

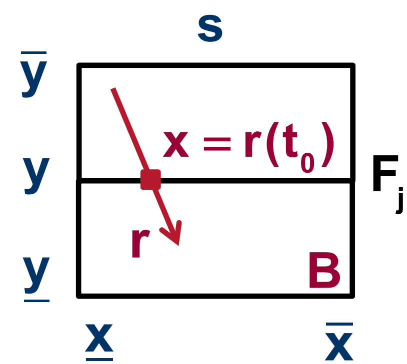
- **States S:** Pairs (s,B) where s is a mode, B is a box
- **Initial abstraction:** $\{(s_i, \{x \mid (s_i, x) \in \Phi\}) \mid 1 \leq i \leq n\}$
- **Init** $= \{(s,B) \mid$ cannot disprove $\exists x \in B.\mathrm{Init}(s,x)\ \}$
- **Unsafe** $= \{(s,B) \mid$ cannot disprove $\exists x \in B.\mathrm{Unsafe}(s,x)\ \}$
- **Trans** $= \{\ ((s,B),\ (s',B'))\ \mid$

  $s = s' \wedge B = B' \ \vee$

  cannot disprove $\exists x \in B, x' \in B'.\ \mathrm{Jump}(s,x,s',x') \ \vee$

  $s = s' \wedge B \neq B' \wedge$ cannot disprove $\mathrm{transition}_{s,B,B'}\ \}$

Flow Between Non-Overlapping Boxes



Flow r in s enters box B at $x \in B$ iff :

- $\exists t_0.\ r(t_0) = (s, x)$
- $\exists \delta > 0. \forall t \in (t_0, t_0 + \delta)$: $r(t) \in (s, B)$

Lemma: If r enters B at x then $\forall$ faces $F \in B$. $x \in F$:

- $\exists \dot{x}_1, \ldots, \dot{x}_k.\ \mathrm{Flow}(s, x, (\dot{x}_1, \ldots, \dot{x}_k)) \wedge \dot{x}_j \geq 0$ if F is j^{th} lower face of B
- $\exists \dot{x}_1, \ldots, \dot{x}_k.\ \mathrm{Flow}(s, x, (\dot{x}_1, \ldots, \dot{x}_k)) \wedge \dot{x}_j \leq 0$ if F is j^{th} upper face of B
- $\mathrm{incoming}^F_{s,B}(x)$: this constraint

Lemma: For a mode s, non-overlapping boxes B,B':

- if $\exists$r in s entering B' on a common point of B and B' then
- $\exists x \in B.\ x \in B' \wedge \forall F \in B.\ x \in F \Rightarrow \mathrm{incoming}^F_{s,B'}(x)$
- $\mathrm{transition}_{s,B,B'}$: this constraint

Safe Abstraction

Theorem: For all HS D and sets of abstract states $\mathcal{B}$

- Covering the whole state space such that
- All boxes B of the same mode are nonoverlapping
- The safety of $\text{Abstract}_D(\mathcal{B})$ implies the safety of D

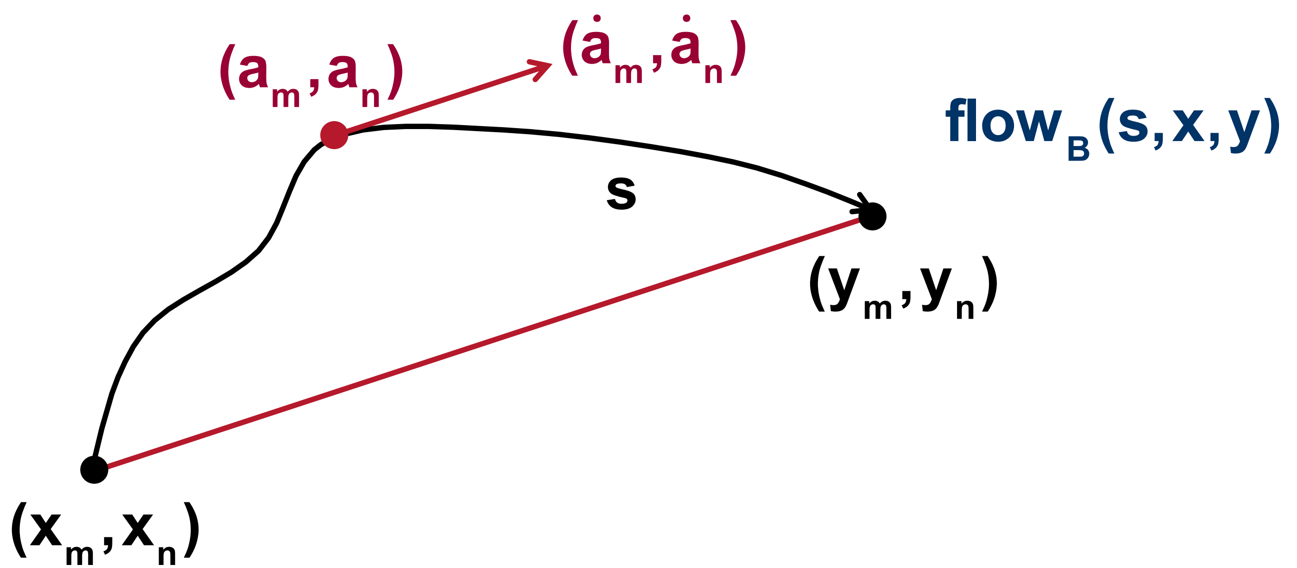
Problem with naive algorithm:

- Splitting can result in a huge number of boxes
- Abstract only states reachable from Init via flows or jumps

Generalized Mean-Value Lemma

Lemma: Given (s, B) if $y \in B$ is reachable from $x \in B$:

- $\wedge_{1 \le m < n \le k} \; \exists a_1,\ldots,a_k,\dot{a}_1,\ldots,\dot{a}_k.$
- $(a_1,\ldots,a_k) \in B \wedge \mathrm{Flow}(s,a_1,\ldots,a_k,\dot{a}_1,\ldots,\dot{a}_k) \wedge$
- $(y_n - x_n) / (y_m - x_m) = \dot{a}_n / \dot{a}_m$



Reachability

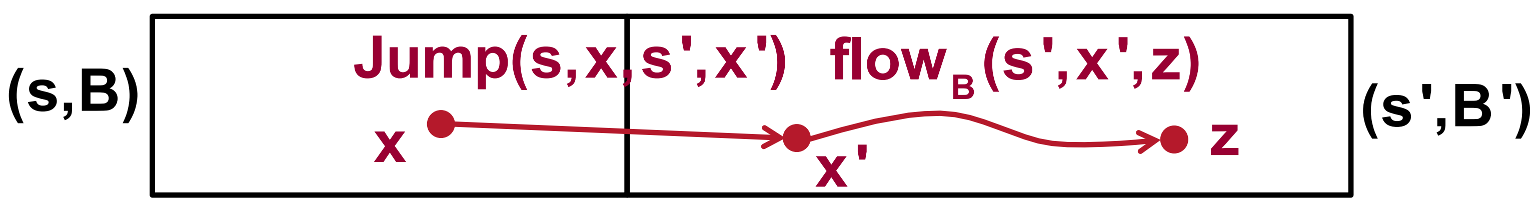
Lemma: Given (s, B) if $z \in B$ is reachable via a flow:

- $\exists x \in B.\ Init(s,x) \wedge flow_B(s,x,y)$

Lemma: Given (s, B), (s',B') and $z \in B'$:

- If reachable (s',z) from a jump from (s,B) via a flow in (s',B')
- $\exists x \in B, x' \in B'.\ Jump(s,x,s',x') \wedge flow_B(s',x',z)$

$jumpflow_{B,B'}(s,s',z)$



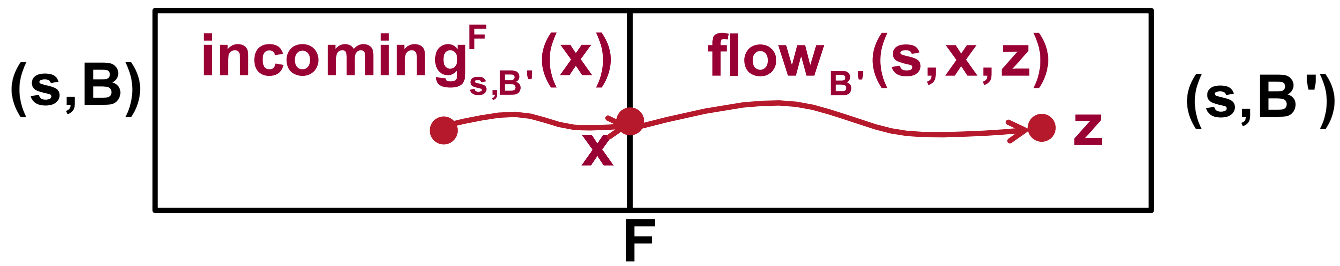
Reachability

Lemma: Given s, nonoveraping B,B' and $z \in B' \backslash B$:

– If reachable z via a flow entering B' at common point

– $\exists x \in B.\ x \in B' \wedge (\forall F \in B.\ x \in F \Rightarrow \text{incoming}^{F}_{s,B'}(x)) \wedge \text{flow}_{B'}(s,x,z)$

$\text{boundaryflow}_{B,B'}(s,z)$



Theorem: If (s',z) is reachable

– $\text{initflow}_{B'}(s',z) \vee$

– $\bigvee_{(s,B)\in\mathcal{B}} \text{jumpflow}_{B,B'}(s,s',z) \vee$

– $\bigvee_{(s,B)\in\mathcal{B},\, s=s',\, B\neq B'} \text{boudaryflow}_{B,B'}(s'z)$

- RSolver implementation
- dReal implementation