Measurability for Safety Verification of Stochastic Hybrid Systems [1]

Nicolás Wolovick

Fa.M.A.F., Universidad Nacional de Córdoba, Argentina

Doc10 – 6 December 2010

Joint work with: Martin Fränzle, Ernst Moritz Hahn,
Holger Hermanns and Lijun Zhang

[1] En el lenguaje de Braden

Stochastic Hybrid Systems

Semantic Model

Conclusion

Motivation

Think of an Automatic Braking System

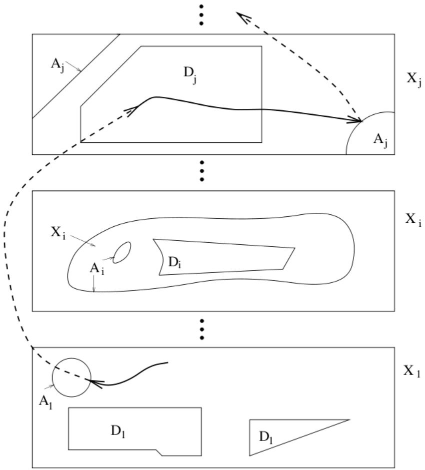
- Continuous Dynamics
- Discrete Dynamics
- Noise
- Underspecification

The Probabilistic Model Checking problem

Given a model $\mathcal{M}$ and an *UnSafe* set, compute the probability of reaching the bad set in n steps from state s

$$Reach_{\leq n}^{\mathcal{M}} : S \to [0, 1]$$

Example of Hybrid System evolution

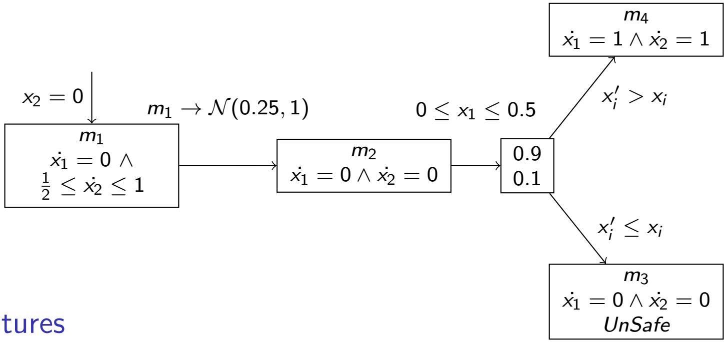


[a]

- Many modes
- Nondeterminism in flows
  continuous
- Nondeterminism in jumps
  discrete

[a] Introduction to Hybrid Systems, Michael S. Branicky, 2005, Fig.12

Stochastic Hybrid Automaton – Overview



Features

- Nondeterministic flows
- Nondeterministic jumps with targets:
  - Continuous probability over states
  - Discrete probability of sets of states

Stochastic Hybrid Automata – Components

$$(\mathtt{M}, \mathbf{x}, \mathit{Init}, \mathit{Flow}, \mathtt{C}, \mathit{UnSafe})$$

- State space $\mathtt{M} \times \mathbb{R}^k$
- Starting states *Init*
- Continuous dynamics control *Flow* $\subseteq \mathtt{M} \times \mathbb{R}^k \times \mathbb{R}^k$
- Discrete dynamics control commands $\mathtt{C}$
- Bad set *UnSafe*

Nondeterministic Flow Example

$$0 \leq x_1 + x_2 \leq 1 \ \wedge \ x_1 \leq 3\dot{x}_1 \ \wedge \ \dot{x}_2 = 1$$

Stochastic Hybrid Automata – Commands

Stochastic Guarded Command

condition $\rightarrow \mu$

$$\mu(m_1, x_1, x_2)\,(\{m_2\} \times [a, b] \times \{x_2\}) = \frac{1}{\sqrt{2\pi}} \int_a^b \exp\left(-\frac{1}{2}x_2^2\right)\,\mathrm{d}x$$

Probabilistic Guarded Command

condition $\rightarrow p_1 : update_1 + \cdots + p_n : update_n$

$$\begin{array}{lcl} m = m_1 & \rightarrow & 0.2 : m' = m_2 \wedge x_1' \leq x_2 - 0.84 \\ & + & 0.2 : m' = m_2 \wedge x_2 - 0.85 \leq x_1' \leq x_2 - 0.25 \\ & + & 0.2 : m' = m_2 \wedge x_2 - 0.26 \leq x_1' \leq x_2 + 0.26 \\ & + & 0.2 : m' = m_2 \wedge x_2 + 0.25 \leq x_1' \leq x_2 + 0.85 \\ & + & 0.2 : m' = m_2 \wedge x_1' \geq x_2 + 0.84 \end{array}$$

Both are state dependent

Stochastic Hybrid Systems

Semantic Model

Conclusion

Nondeterministic Markov Process – NMP

$$(S, \Sigma, Init, Steps, UnSafe)$$

Nondeterministic Markov Process – NMP

$$(S, \Sigma, Init, Steps, UnSafe)$$

Transition Function

$$Steps : S \to \Delta(S)$$

where $\Delta(S)$ is the set of all probability distributions

Nondeterministic Markov Process – NMP

$$(S, \Sigma, \mathit{Init}, \mathit{Steps}, \mathit{UnSafe})$$

Transition Function

$$\mathit{Steps} : S \to 2^{\Delta(S)}$$

where $\Delta(S)$ is the set of all probability distributions

Nondeterministic Markov Process – NMP

$$(S, \Sigma, \mathit{Init}, \mathit{Steps}, \mathit{UnSafe})$$

Transition Function

$$\mathit{Steps} : S \to \Delta(\Sigma)$$

where $\Delta(\Sigma)$ is the σ-algebra of probability distributions

Nondeterministic Markov Process – NMP

$$(S, \Sigma, Init, Steps, UnSafe)$$

Transition Function

$$Steps : S \to \Delta(\Sigma)$$

where $\Delta(\Sigma)$ is the σ-algebra of probability distributions

What is $\Delta(\Sigma)$

- Generators $\Delta^{<q}(A) = \{\mu \mid \mu(A) < q\} \in \Delta(\Sigma)$
- Closed by σ-unions $\Theta_i \in \Delta(\Sigma) \Rightarrow \bigcup_i \Theta_i \in \Delta(\Sigma)$
- Closed by cpl $\Theta \in \Delta(\Sigma) \Rightarrow \Theta^c \in \Delta(\Sigma)$

Probabilistic Nondeterminism using $\Delta^{<q}(A)$

Use $\Delta^{<q}(A)$ as building blocks
A tool for (under)specify probabilism

Examples

- $Steps(s) = \Delta^{>\frac{1}{2}}([0,1] \times [0,1])$

Probabilistic Nondeterminism using $\Delta^{<q}(A)$

Use $\Delta^{<q}(A)$ as building blocks
A tool for (under)specify probabilism

Examples

- $\mathit{Steps}(s) = \Delta^{>\frac{1}{2}}([0,1] \times [0,1])$
- $\mathit{Steps}((0,0)) = \Delta^{=0}(\{0\} \times \mathbb{R}^{+}) \cap \Delta^{=0}(\mathbb{R}^{+} \times \{0\})$

Probabilistic Nondeterminism using $\Delta^{<q}(A)$

Use $\Delta^{<q}(A)$ as building blocks
A tool for (under)specify probabilism

Examples

- $\mathit{Steps}(s) = \Delta^{>\frac{1}{2}}([0,1] \times [0,1])$
- $\mathit{Steps}((0,0)) = \Delta^{=0}(\{0\} \times \mathbb{R}^+) \cap \Delta^{=0}(\mathbb{R}^+ \times \{0\})$
- $\mathit{Steps}([0,\frac{1}{2}] \times \mathbb{R}^+) = \Delta^{=\frac{1}{2}}((\frac{1}{2},\frac{3}{4}] \times \{1\}) \cup \Delta^{=\frac{1}{2}}((\frac{3}{4},1] \times \{1\})$

Probabilistic Nondeterminism using $\Delta^{<q}(A)$

Use $\Delta^{<q}(A)$ as building blocks
A tool for (under)specify probabilism

Examples

- $Steps(s) = \Delta^{>\frac{1}{2}}([0,1] \times [0,1])$
- $Steps((0,0)) = \Delta^{=0}(\{0\} \times \mathbb{R}^{+}) \cap \Delta^{=0}(\mathbb{R}^{+} \times \{0\})$
- $Steps([0,\frac{1}{2}] \times \mathbb{R}^{+}) = \Delta^{=\frac{1}{2}}((\frac{1}{2},\frac{3}{4}] \times \{1\}) \cup \Delta^{=\frac{1}{2}}((\frac{3}{4},1] \times \{1\})$
- $Steps(s) = \bigcap_n \Delta^{<\frac{1}{\Sigma_{i=0}^{n} \frac{1}{k!}}}(\mathbb{R} \times \mathbb{R}^{+})$

The Problem

Capturing the semantics of probabilistic guarded command c

$$condition \to p_1 : update_1 + \cdots + p_n : update_n$$

Semantics is $Steps_{\mathrm{c}}(s)$ in terms of the nondeterministic update functions $u_i : S \to \Sigma$

Try 1

$$Steps_{\mathrm{c}}(s) = p_1 u_n(s) + \cdots + p_n u_n(s)$$

The Problem

Capturing the semantics of probabilistic guarded command c

$$condition \rightarrow p_1 : update_1 + \cdots + p_n : update_n$$

Semantics is $Steps_c(s)$ in terms of the nondeterministic update functions $u_i : S \rightarrow \Sigma$

Try 1

$$Steps_c(s) = p_1 u_n(s) + \cdots + p_n u_n(s)$$

Nop! It has to be written in terms of the $\Delta^{\bowtie q}(A)$

The Problem

Capturing the semantics of probabilistic guarded command c

$$\mathit{condition} \rightarrow p_1 : \mathit{update}_1 + \cdots + p_n : \mathit{update}_n$$

Semantics is $\mathit{Steps}_{\mathrm{c}}(s)$ in terms of the nondeterministic update functions $u_i : S \rightarrow \Sigma$

Try 2

$$\mathit{Steps}_{\mathrm{c}}(s) = \Delta^{=p_1}(u_1(s)) \cap \cdots \cap \Delta^{=p_n}(u_n(s))$$

The Problem

Capturing the semantics of probabilistic guarded command c

$$condition \rightarrow p_1 : update_1 + \cdots + p_n : update_n$$

Semantics is $Steps_{\mathrm{c}}(s)$ in terms of the nondeterministic update functions $u_i : S \rightarrow \Sigma$

Try 2

$$Steps_{\mathrm{c}}(s) = \Delta^{=p_1}(u_1(s)) \cap \cdots \cap \Delta^{=p_n}(u_n(s))$$

Problem: allows continuous distributions

The Problem

Capturing the semantics of probabilistic guarded command c

$$condition \rightarrow p_1 : update_1 + \cdots + p_n : update_n$$

Semantics is $Steps_{\mathrm{c}}(s)$ in terms of the nondeterministic update functions $u_i : S \rightarrow \Sigma$

Try 3

$$Steps_{\mathrm{c}}(s) = \Phi_{\leq n} \cap \Delta^{=p_1}(u_1(s)) \cap \cdots \cap \Delta^{=p_n}(u_n(s))$$

The Problem

Capturing the semantics of probabilistic guarded command c

$$condition \rightarrow p_1 : update_1 + \cdots + p_n : update_n$$

Semantics is $Steps_{\mathsf{c}}(s)$ in terms of the nondeterministic update functions $u_i : S \rightarrow \Sigma$

Try 3

$$Steps_{\mathsf{c}}(s) = \Phi_{\leq n} \cap \Delta^{=p_1}(u_1(s)) \cap \cdots \cap \Delta^{=p_n}(u_n(s))$$

How do we express the set at most n points probabilities?

$\Phi_{\leq n}$

Idea by pedrost – one point, unidimensional

$$\Phi_{\leq 1} = \bigcap_{\substack{p<p' \\ p,p' \in \mathbb{Q}}} \left(\Delta^{=0}([p,p']) \cup \Delta^{=0}([p,p']^c) \right)$$

$\Phi_{\leq n}$

Idea by `pedrost` – one point, unidimensional

$$\Phi_{\leq 1} = \bigcap_{\substack{p<p' \\ p,p' \in \mathbb{Q}}} \left(\Delta^{=0}([p, p']) \cup \Delta^{=0}([p, p']^c) \right)$$

Easy to extrapolate to: at most/exactly n points, in k dimensions

$\Phi_{\leq n}$

Idea by pedrost – one point, unidimensional

$$\Phi_{\leq 1} = \bigcap_{\substack{p<p' \\ p,p' \in \mathbb{Q}}} \left(\Delta^{=0}([p,p']) \cup \Delta^{=0}([p,p']^c)\right)$$

Easy to extrapolate to: at most/exactly n points, in k dimensions

One caveat $u_i(s) \cap u_j(s) \neq \emptyset$, add probabilities
Original version:

$$Steps_c(s) = \Phi_{\leq n} \cap \bigcap_{i=1}^{n} \Delta^{=p_i}(u_i(s))$$

$\Phi_{\leq n}$

Idea by `pedrost` – one point, unidimensional

$$\Phi_{\leq 1} = \bigcap_{\substack{p<p' \\ p,p' \in \mathbb{Q}}} \left(\Delta^{=0}([p,p']) \cup \Delta^{=0}([p,p']^c)\right)$$

Easy to extrapolate to: at most/exactly n points, in k dimensions

One caveat $u_i(s) \cap u_j(s) \neq \emptyset$, add probabilities
Final version:

$$Steps_c(s) = \bigcup_{P \in SetPart(n)} \Phi_{=|P|} \cap \bigcap_{i=1}^{|P|} \Delta^{=\sum_{j \in P_i} p_j}\left(\cap_{j \in P_i} u_j(s)\right)$$

Stochastic Hybrid Systems

Semantic Model

Conclusion

Our group contribution

Sufficiently complex model to try with N(L)MP:

- Continuous evolution: continuous nondeterministic DE
- Discrete evolution: continuous probabilistic and nondeterministic operators

We showed:

- $\mathit{Reach} : S \to [0,1]$ is well defined
- The SHA semantics $\mathit{Steps}(s)$ is a NMP

We learned:

- $\Delta^{\bowtie q}(Q)$ nice way to express probabilistic nondeterminism
- Measurability for general flows is (still) a good question

The rest of the work

A lot more has been done:

- Nondeterministic update u_i is used to abstract
- A tool out of three layer sandwich of abstractions:
  - Stochastic Hybrid Automata (ProHVer – HSCC2011? [2])
  - Probabilistic Hybrid Automata (ProHVer – CAV2010)
  - Hybrid Automata (PHAVer – HSCC2005)
- Many examples have been conducted

[2] Submitted

Thanks