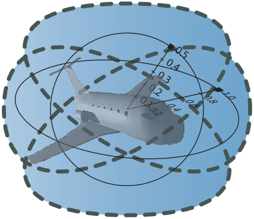
Logic and Compositional Verification of Stochastic Hybrid Systems

André Platzer

Carnegie Mellon University, Pittsburgh, PA



Outline

Cyber-Physical Systems:

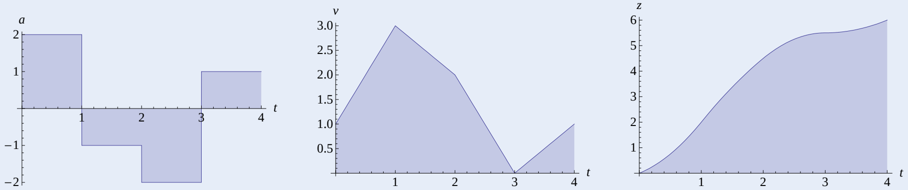
Q: I want to verify trains

Challenge

Q: I want to verify trains A: Hybrid systems

Challenge (Hybrid Systems)

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)

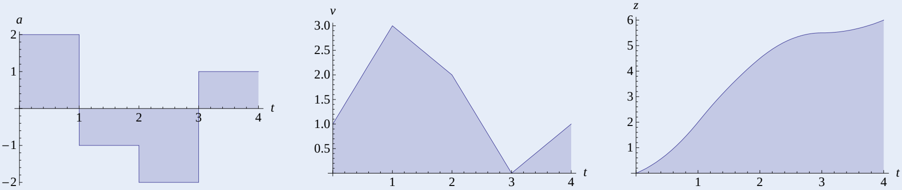


Cyber-Physical Systems: Hybrid Systems

Q: I want to verify trains A: Hybrid systems Q: But there's uncertainties!

Challenge (Hybrid Systems)

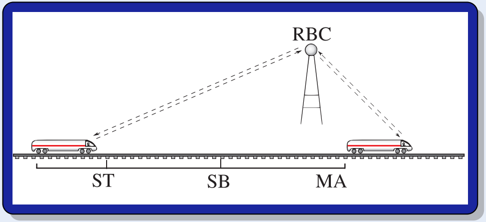
- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)



Cyber-Physical Systems:

Q: I want to verify uncertain trains

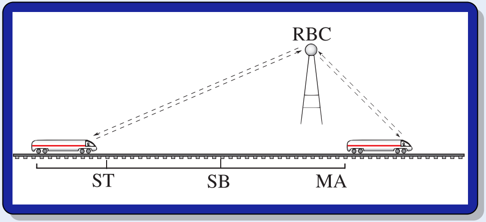
Challenge

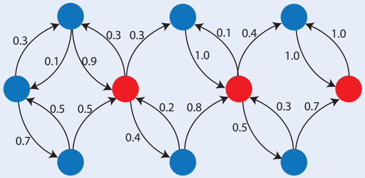


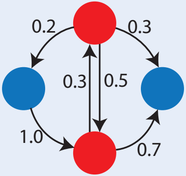
Q: I want to verify uncertain trains A: Markov chains

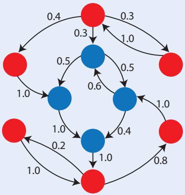
Challenge (Probabilistic Systems)

- Directed graph
  (Countable state space)
- Weighted edges
  (Transition probabilities)





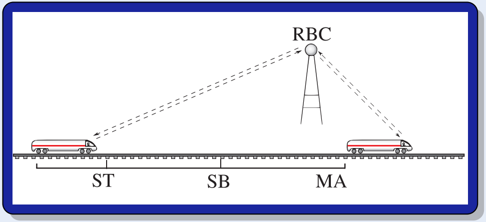


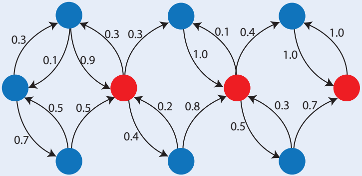


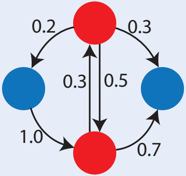
Q: I want to verify uncertain trains A: Markov chains Q: But trains move!

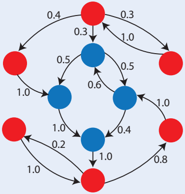
Challenge (Probabilistic Systems)

- Directed graph (Countable state space)
- Weighted edges (Transition probabilities)





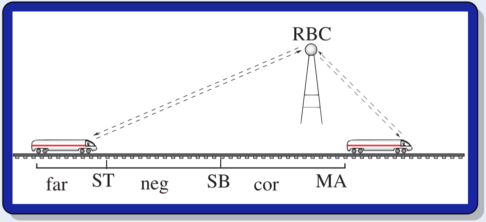




Cyber-Physical Systems:

Q: I want to verify uncertain trains

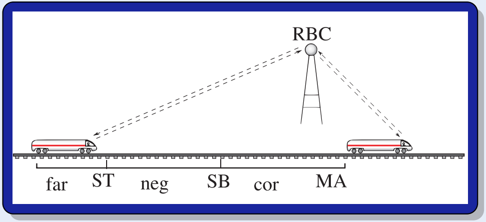
Challenge



Q: I want to verify uncertain trains A: Stochastic hybrid systems

Challenge (Stochastic Hybrid Systems)

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)
- Stochastic dynamics (uncertainty)

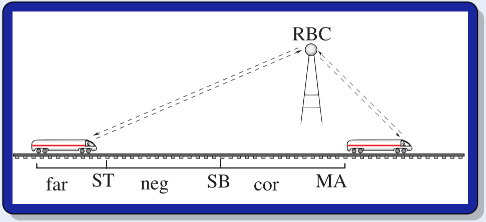


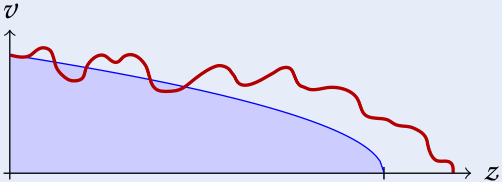
Q: I want to verify uncertain trains A: Stochastic hybrid systems

Challenge (Stochastic Hybrid Systems)

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)
- Stochastic dynamics (uncertainty)

- Discrete stochastic (lossy communication)
- Continuous stochastic (wind, track)



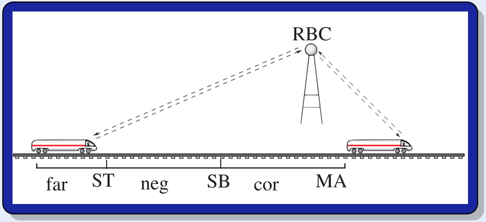


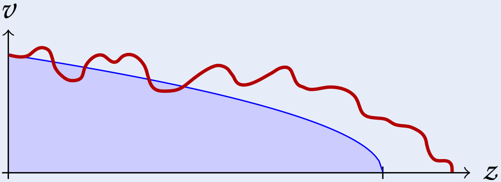
Q: I want to verify uncertain trains A: Stochastic hybrid systems Q: How?

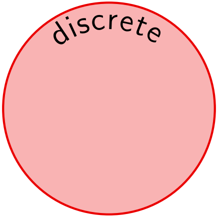
Challenge (Stochastic Hybrid Systems)

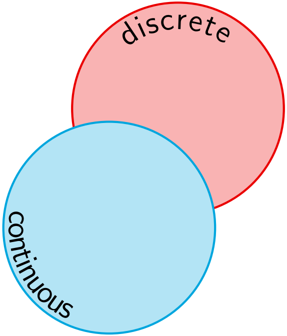
- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)
- Stochastic dynamics (uncertainty)

- Discrete stochastic (lossy communication)
- Continuous stochastic (wind, track)

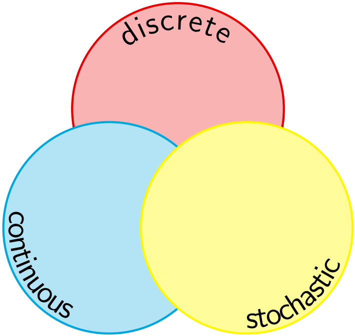




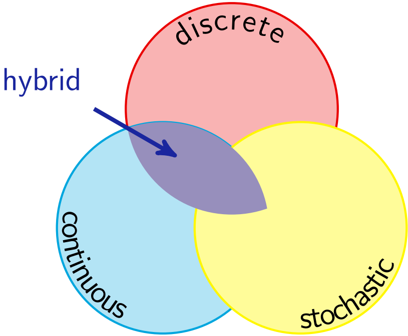

discrete


discrete
continuous

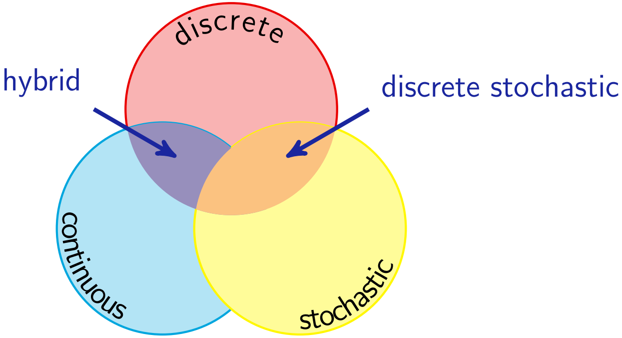
Cyber-Physical Systems



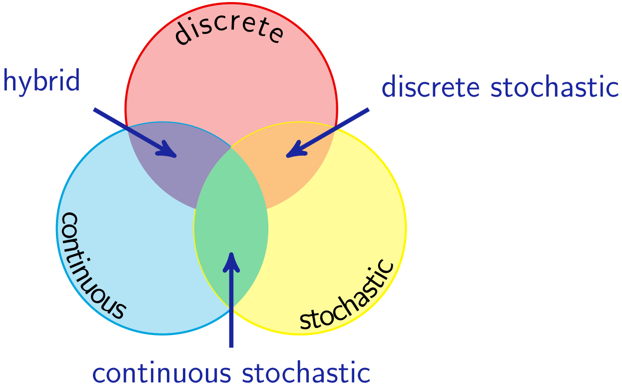
Cyber-Physical Systems

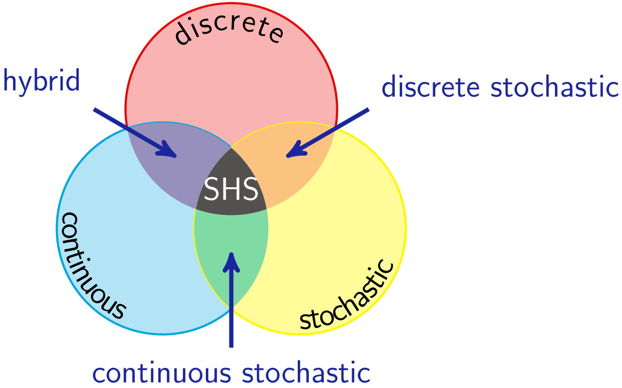


Cyber-Physical Systems



Cyber-Physical Systems




discrete
hybrid
discrete stochastic
SHS
continuous
stochastic
continuous stochastic

Contributions

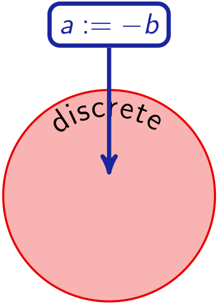
1. System model and semantics for stochastic hybrid systems: SHP
2. Prove semantic processes are adapted and a.s. càdlàg
3. Prove natural process stopping times are Markov times
4. Specification and verification logic: Sd$\mathcal{L}$
5. Prove measurability of Sd$\mathcal{L}$ semantics $\Rightarrow$ probabilities well-defined
6. Proof rules for Sd$\mathcal{L}$
7. Sound Dynkin use of infinitesimal generators of SDEs
8. First compositional verification for stochastic hybrid systems
9. Logical foundation for analysis of stochastic hybrid systems

Outline

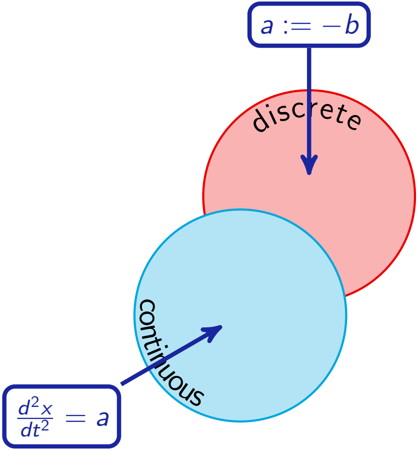
Outline (Conceptual Approach)

1. Motivation
2. Stochastic Differential Dynamic Logic Sd$\mathcal{L}$
   - Design
   - Stochastic Differential Equations
   - Syntax
   - Semantics
   - Well-definedness
3. Stochastic Differential Dynamic Logic
   - Syntax
   - Semantics
   - Well-definedness
4. Proof Calculus for Stochastic Hybrid Systems
   - Compositional Proof Calculus
   - Soundness
5. Conclusions

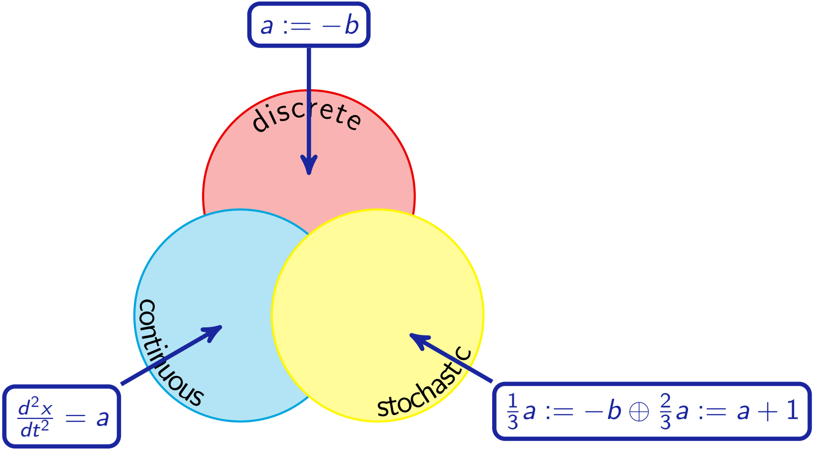
Model for Stochastic Hybrid Systems



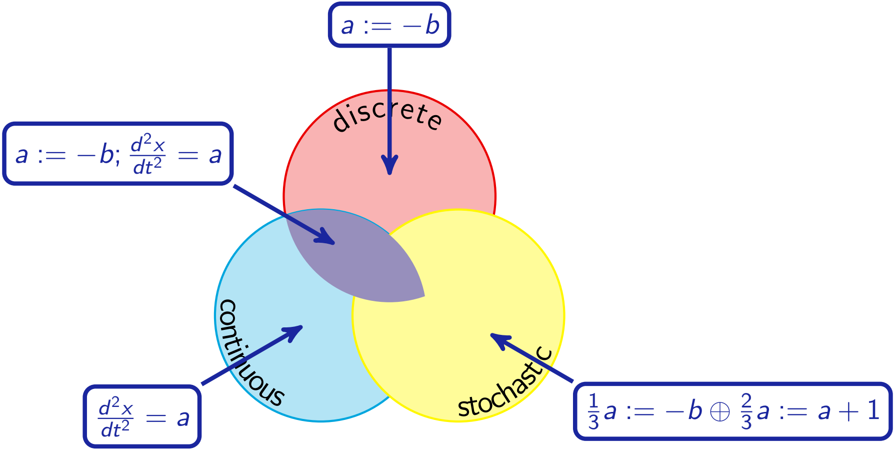
Model for Stochastic Hybrid Systems



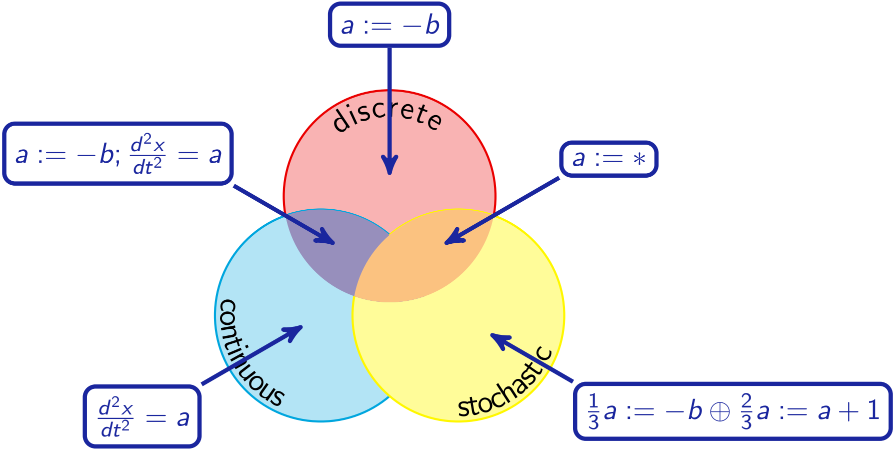
Model for Stochastic Hybrid Systems



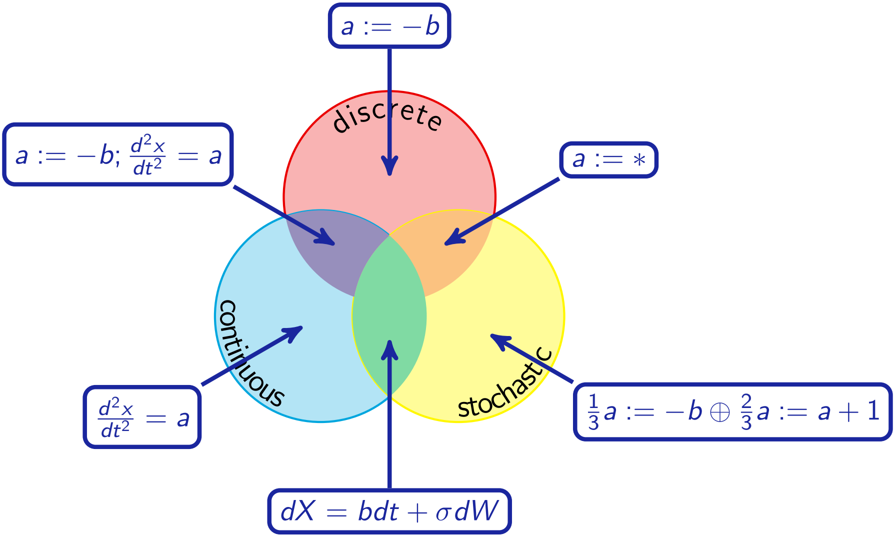
Model for Stochastic Hybrid Systems



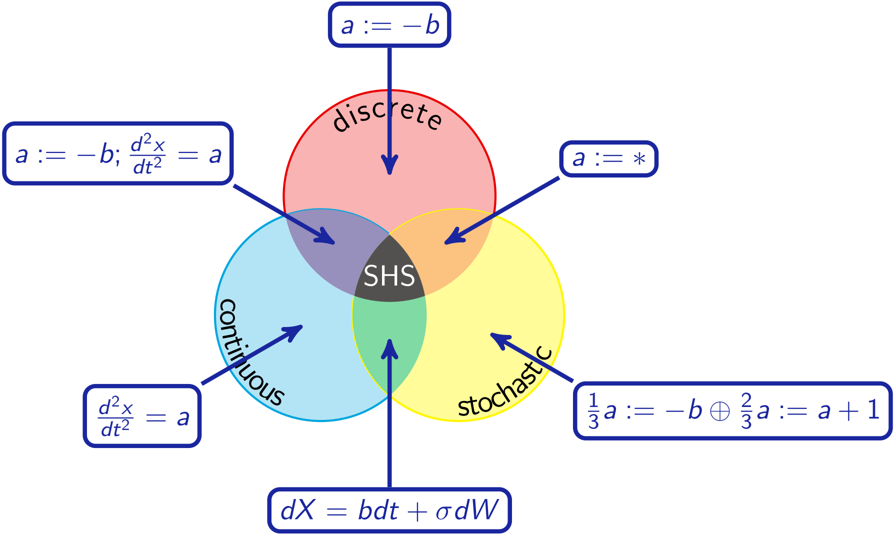
Model for Stochastic Hybrid Systems



Model for Stochastic Hybrid Systems



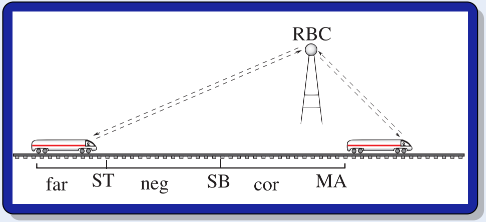
Model for Stochastic Hybrid Systems



Model for Stochastic Hybrid Systems

Q: How to model stochastic hybrid systems

Model (Stochastic Hybrid Systems)



Model for Stochastic Hybrid Systems

Q: How to model stochastic hybrid systems

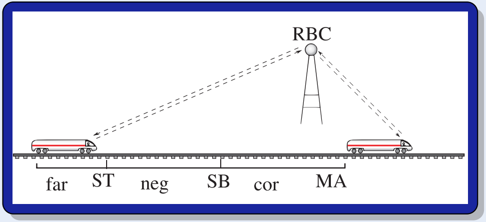
Model (Stochastic Hybrid Systems)

- Discrete dynamics (control decisions)

  $a := -b$

- Continuous dynamics (differential equations)

- Stochastic dynamics (structural)

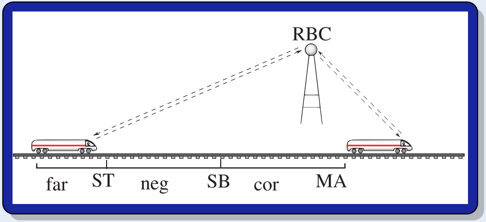


Model for Stochastic Hybrid Systems

Q: How to model stochastic hybrid systems

Model (Stochastic Hybrid Systems)

- Discrete dynamics (control decisions)
  $a := -b$
- Continuous dynamics (differential equations)
  $x'' = a$
- Stochastic dynamics (structural)

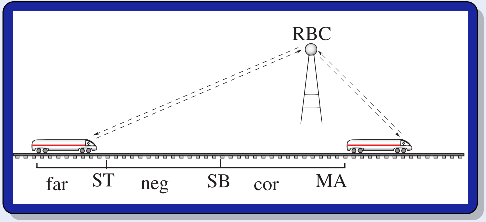


Model for Stochastic Hybrid Systems

Q: How to model stochastic hybrid systems

Model (Stochastic Hybrid Systems)

- Discrete dynamics (control decisions)
  $$a := -b$$
- Continuous dynamics (differential equations)
  $$x'' = a$$
- Stochastic dynamics (structural)
  $$\tfrac{1}{3} a := -b \oplus \tfrac{2}{3} a := a + 1$$



Model for Stochastic Hybrid Systems

Q: How to model stochastic hybrid systems

Model (Stochastic Hybrid Systems)

- Discrete dynamics (control decisions)

  $$a := -b$$

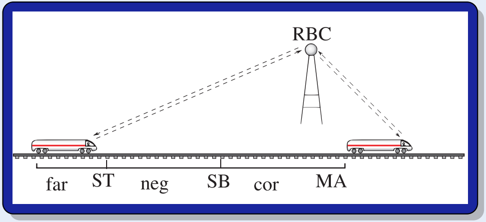
  $$a := *$$

- Continuous dynamics (differential equations)

  $$x'' = a$$

- Stochastic dynamics (structural)

  $$\tfrac{1}{3} a := -b \oplus \tfrac{2}{3} a := a + 1$$



Model for Stochastic Hybrid Systems

Q: How to model stochastic hybrid systems

Model (Stochastic Hybrid Systems)

- Discrete dynamics (control decisions)

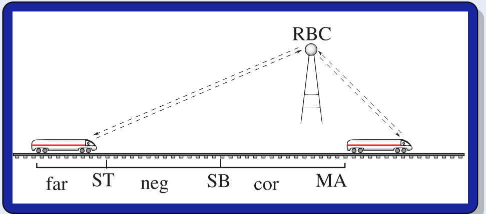
  $$a := -b$$
  $$a := *$$

- Continuous dynamics (differential equations)

  $$x'' = a$$
  $$dx = a dt + \sigma dW$$

- Stochastic dynamics (structural)

  $$\tfrac{1}{3} a := -b \oplus \tfrac{2}{3} a := a + 1$$



Model for Stochastic Hybrid Systems

Q: How to model stochastic hybrid systems

Model (Stochastic Hybrid Systems)

- Discrete dynamics (control decisions)

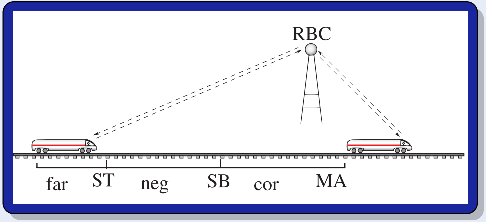
  $$a := -b$$
  $$a := *$$

- Continuous dynamics (differential equations)

  $$x'' = a$$
  $$dx = a dt + \sigma dW$$

- Stochastic dynamics (structural)

  $$\tfrac{1}{3} a := -b \oplus \tfrac{2}{3} a := a + 1$$



Model for Stochastic Hybrid Systems

Q: How to model stochastic hybrid systems

Model (Stochastic Hybrid Systems)

- Discrete dynamics (control decisions)

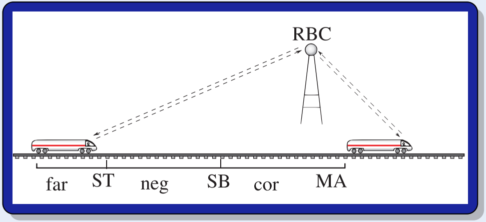
  $$a := -b$$
  $$a := *$$

- Continuous dynamics (differential equations)

  $$x'' = a$$
  $$dx = adt + \sigma dW$$

- Stochastic dynamics (structural)

  $$\tfrac{1}{3} a := -b \oplus \tfrac{2}{3} a := a + 1$$

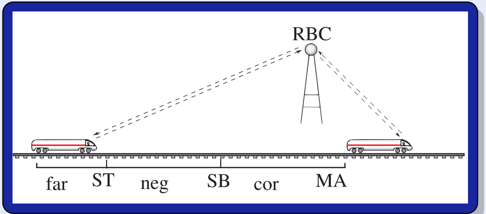


Model for Stochastic Hybrid Systems

Q: How to model stochastic hybrid systems

Model (Stochastic Hybrid Systems)

- Discrete dynamics (control decisions)
  $$a := -b$$
  $$a := *$$
- Continuous dynamics (differential equations)
  $$x'' = a$$
  $$dx = a dt + \sigma dW$$
- Stochastic dynamics (structural)
  $$\tfrac{1}{3} a := -b \oplus \tfrac{2}{3} a := a + 1$$

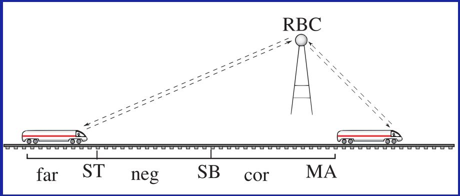


Model for Stochastic Hybrid Systems

Q: How to model stochastic hybrid systems A: Stochastic Hybrid Programs

Model (Stochastic Hybrid Systems)

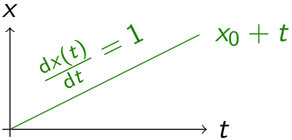
- Discrete dynamics (control decisions)
  $$a := -b$$
  $$a := *$$
- Continuous dynamics (differential equations)
  $$x'' = a$$
  $$dx = a dt + \sigma dW$$
- Stochastic dynamics (structural)
  $$\frac{1}{3} a := -b \oplus \frac{2}{3} a := a + 1$$



Stochastic Differential Equations (SDE)

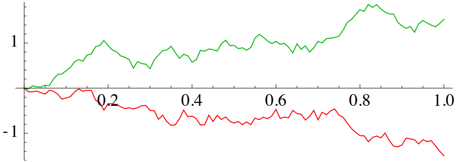
Definition (Ordinary differential equation (ODE))

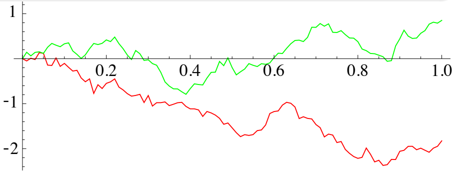
$$\frac{dx(t)}{dt} = b(x(t)) \quad x(0) = x_0$$



Definition (Itō stochastic differential equation (SDE))

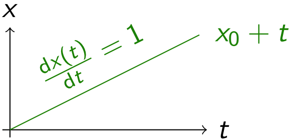
$$dX_t = b(X_t)dt + \sigma(X_t)dW_t \quad X_0 = Z$$





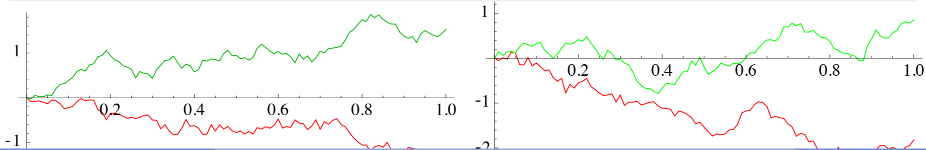
Definition (Ordinary differential equation (ODE))

$$\frac{dx(t)}{dt} = b(x(t)) \quad x(0) = x_0$$



Definition (Itō stochastic differential equation (SDE))

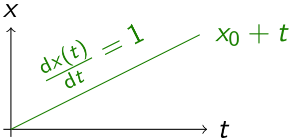
$$X_s = Z + \int_0^s dX_t = Z + \int_0^s b(X_t)dt + \int_0^s \sigma(X_t)dW_t$$

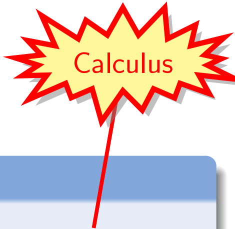


Stochastic Differential Equations (SDE)

Definition (Ordinary differential equation (ODE))

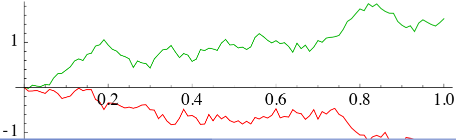
$$\frac{\mathrm{d}x(t)}{\mathrm{d}t} = b(x(t)) \quad x(0) = x_0$$

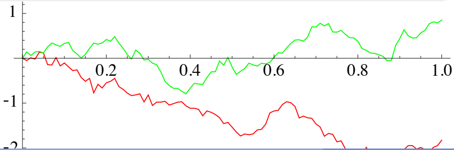




Definition (Itō stochastic differential equation (SDE))

$$X_s = Z + \int_0^s dX_t = Z + \int_0^s b(X_t)dt + \int_0^s \sigma(X_t)dW_t$$

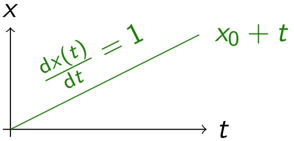


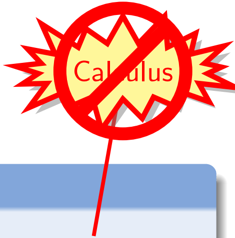


Stochastic Differential Equations (SDE)

Definition (Ordinary differential equation (ODE))

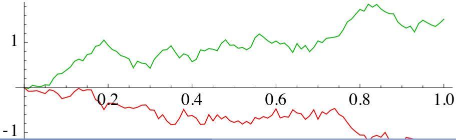
$$\frac{dx(t)}{dt} = b(x(t)) \quad x(0) = x_0$$

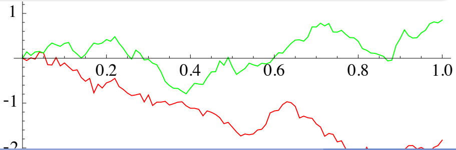




Definition (Itō stochastic differential equation (SDE))

$$X_s = Z + \int_0^s dX_t = Z + \int_0^s b(X_t)dt + \int_0^s \sigma(X_t)dW_t$$





Brownian Motion is Extremely Complex

Definition (Brownian motion W $\Rightarrow$ end of calculus)

1. $W_0 = 0$ (start at 0)
2. W_t almost surely continuous
3. $W_t - W_s \sim \mathcal{N}(0, t - s)$ (independent normal increments)

$\Rightarrow$ a.s. continuous everywhere but nowhere differentiable

$\Rightarrow$ a.s. unbounded variation, $\notin$ FV, nonmonotonic on every interval

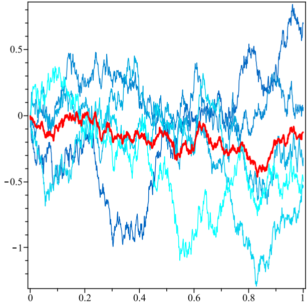
Brownian Motion is Extremely Complex

Definition (Brownian motion W $\Rightarrow$ end of calculus)

1. $W_0 = 0$ (start at 0)
2. W_t almost surely continuous
3. $W_t - W_s \sim \mathcal{N}(0, t-s)$ (independent normal increments)

$\Rightarrow$ a.s. continuous everywhere but nowhere differentiable

$\Rightarrow$ a.s. unbounded variation, $\notin$ FV, nonmonotonic on every interval



Stochastic Hybrid Programs: Syntax

Definition (Stochastic hybrid program α)

$x := \theta$	(assignment)	jump & test
$x := *$	(random assignment)	jump & test
$?H$	(conditional execution)	jump & test
$dx = b dt + \sigma dW \,\&\, H$	(SDE)	
$\alpha; \beta$	(seq. composition)	algebra
$\lambda\alpha \oplus \nu\beta$	(convex combination)	algebra
α^*	(nondet. repetition)	algebra

What is the Semantics of a Stochastic Hybrid Program?

- Usual semantics of system is transition relation $\subseteq \mathbb{R}^d \times \mathbb{R}^d$ on states

What is the Semantics of a Stochastic Hybrid Program?

- Usual semantics of system is transition relation $\subseteq \mathbb{R}^d \times \mathbb{R}^d$ on states
- This does not work here, because we lose stochastic information
- Idea: Start at initial value described by random variable $Z : \Omega \to \mathbb{R}^d$

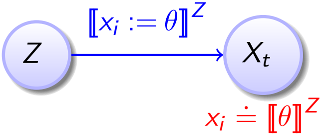
What is the Semantics of a Stochastic Hybrid Program?

- Usual semantics of system is transition relation $\subseteq \mathbb{R}^d \times \mathbb{R}^d$ on states
- This does not work here, because we lose stochastic information
- Idea: Start at initial value described by random variable $Z : \Omega \to \mathbb{R}^d$
- Semantics of program α is stochastic process generator $[\![\alpha]\!] : (\Omega \to \mathbb{R}^d) \to ([0,\infty) \times \Omega \to \mathbb{R}^d)$ giving stochastic process $[\![\alpha]\!]^Z : [0,\infty) \times \Omega \to \mathbb{R}^d$ for each Z

What is the Semantics of a Stochastic Hybrid Program?

- Usual semantics of system is transition relation $\subseteq \mathbb{R}^d \times \mathbb{R}^d$ on states
- This does not work here, because we lose stochastic information
- Idea: Start at initial value described by random variable $Z : \Omega \to \mathbb{R}^d$
- Semantics of program α is stochastic process generator $[\![\alpha]\!] : (\Omega \to \mathbb{R}^d) \to ([0,\infty) \times \Omega \to \mathbb{R}^d)$ giving stochastic process $[\![\alpha]\!]^Z : [0,\infty) \times \Omega \to \mathbb{R}^d$ for each Z
- When does a stochastic process stop?
- Semantics of program α includes stopping time generator $(\!|\alpha|\!) : (\Omega \to \mathbb{R}^d) \to (\Omega \to \mathbb{R})$ giving stopping time $(\!|\alpha|\!)^Z : \Omega \to \mathbb{R}$ for each Z

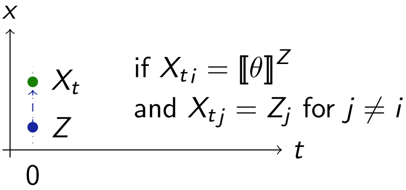
Stochastic Hybrid Program: Process Semantics

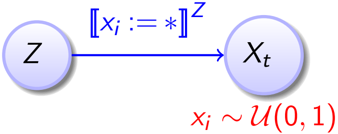


Definition (Stochastic hybrid program α: process semantics)

$$[\![x_i := \theta]\!]^Z = \hat{Y} \quad Y(\omega)_i = [\![\theta]\!]^{Z(\omega)} \text{ and } Y_j = Z_j \text{ (for } j \neq i)$$

$$(\!|x_i := \theta|\!)^Z = 0$$

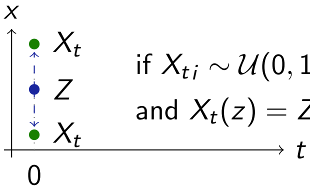




Definition (Stochastic hybrid program α: process semantics)

$$[\![x_i := *]\!]^Z = \hat{U} \qquad U_i \sim \mathcal{U}(0,1) \text{ i.i.d. } \mathcal{F}_0\text{-measurable}$$

$$(\!|x_i := *|\!)^Z = 0$$



if $X_{t\,i} \sim \mathcal{U}(0,1)$

and $X_t(z) = Z(z)$ for $z \neq x$

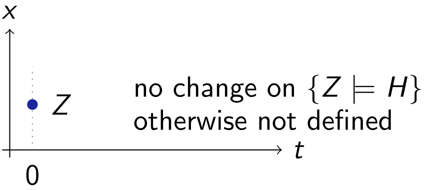
Stochastic Hybrid Program: Process Semantics

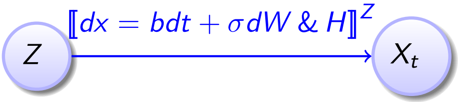
on $\{Z \models H\}$

Definition (Stochastic hybrid program α: process semantics)

$$[\![?H]\!]^Z = \hat{Z} \quad \text{on the event } \{Z \models H\}$$

$$(\!|?H|\!)^Z = 0$$

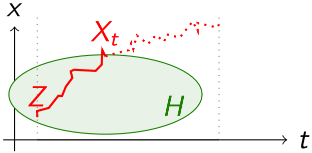




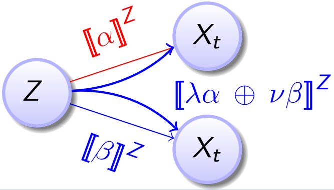
Definition (Stochastic hybrid program α: process semantics)

$[\![dx = bdt + \sigma dW \,\&\, H]\!]^Z$ solves $dX = [\![b]\!]^X dt + [\![\sigma]\!]^X dB_t, X_0 = Z$

$(\!|dx = bdt + \sigma dW \,\&\, H|\!)^Z = \inf\{t \geq 0 \;:\; X \notin H\}$



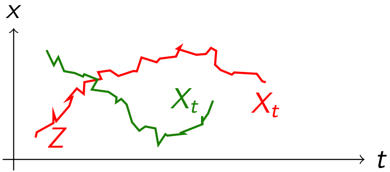
$dx = bdt + \sigma dW \,\&\, H$



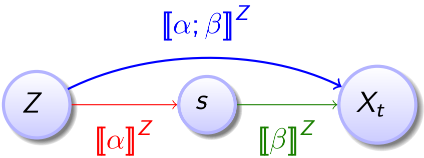
Definition (Stochastic hybrid program α: process semantics)

$$[\![\lambda\alpha \oplus \nu\beta]\!]^Z = \mathcal{I}_{U\le\lambda}[\![\alpha]\!]^Z + \mathcal{I}_{U>\lambda}[\![\beta]\!]^Z = \begin{cases} [\![\alpha]\!]^Z & \text{on event } \{U \le \lambda\} \\ [\![\beta]\!]^Z & \text{on event } \{U > \lambda\} \end{cases}$$

$(\!|\lambda\alpha \oplus \nu\beta|\!)^Z = \mathcal{I}_{U\le\lambda}(\!|\alpha|\!)^Z + \mathcal{I}_{U>\lambda}(\!|\beta|\!)^Z$ with i.i.d. $U \sim \mathcal{U}(0,1)$, $\mathcal{F}_0$-meas



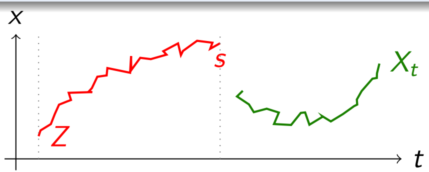
Stochastic Hybrid Program: Process Semantics

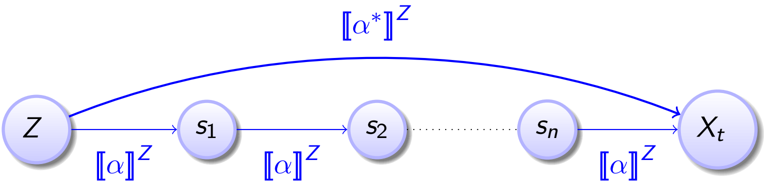


Definition (Stochastic hybrid program α: process semantics)

$$[\![\alpha;\beta]\!]^Z_t = \begin{cases} [\![\alpha]\!]^Z_t & \text{on event } \{t < (\!|\alpha|\!)^Z\} \\ [\![\beta]\!]^{[\![\alpha]\!]^Z_{(\!|\alpha|\!)^Z}}_{t-(\!|\alpha|\!)^Z} & \text{on event } \{t \geq (\!|\alpha|\!)^Z\} \end{cases}$$

$$(\!|\alpha;\beta|\!)^Z = (\!|\alpha|\!)^Z + (\!|\beta|\!)^{[\![\alpha]\!]^Z_{(\!|\alpha|\!)^Z}}$$

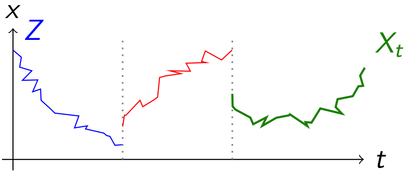




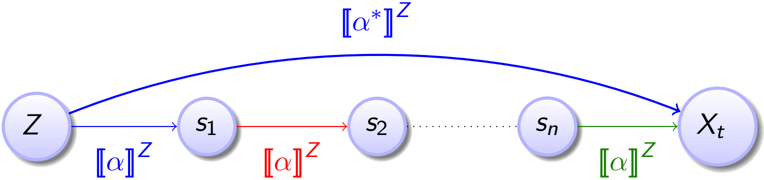
Definition (Stochastic hybrid program α: process semantics)

$$[\![\alpha^*]\!]_t^Z = [\![\alpha^n]\!]_t^Z \text{ on event } \{(\!|\alpha^n|\!)^Z > t\}$$

$$(\!|\alpha^*|\!)^Z = \lim_{n\to\infty} (\!|\alpha^n|\!)^Z$$



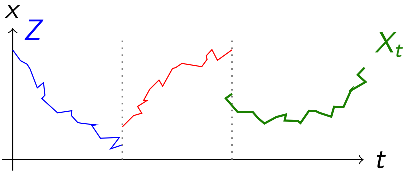
Stochastic Hybrid Program: Process Semantics



Definition (Stochastic hybrid program α: process semantics)

$$[\![\alpha^*]\!]^Z_t = [\![\alpha^n]\!]^Z_t \text{ on event } \{(\!|\alpha^n|\!)^Z > t\}$$

$$(\!|\alpha^*|\!)^Z = \lim_{n\to\infty} (\!|\alpha^n|\!)^Z \qquad \text{monotone!}$$



Well-definedness of Stochastic Process Semantics

Theorem

1. $[\![\alpha]\!]^Z$ *is a.s. càdlàg and adapted*
   (to completed filtration $(\mathcal{F}_t)$ *generated by* Z*,* $(W_s)_{s\leq t}$*,* U*)*
2. $(\!|\alpha|\!)^Z$ *is a Markov time / stopping time*
   (i.e., $\{(\!|\alpha|\!)^Z \leq t\} \in \mathcal{F}_t$*)*

$\Rightarrow$ *End value* $[\![\alpha]\!]^Z_{(\!|\alpha|\!)^Z}$ *is* $\mathcal{F}_{(\!|\alpha|\!)^Z}$*-measurable.*

Outline

Stochastic Differential Dynamic Logic $\mathrm{Sd}\mathcal{L}$: Syntax

Definition ($\mathrm{Sd}\mathcal{L}$ term f)

F	(primitive measurable function, e.g., characteristic $\mathcal{I}_A$)
$\lambda f + \nu g$	(linear term)
Bf	(scalar term for boolean term B)
$\langle\alpha\rangle f$	(reachable)

Definition ($\mathrm{Sd}\mathcal{L}$ formula ϕ)

$$\phi \ ::= \ f \leq g \mid f = g$$

What is the Semantics of Sd$\mathcal{L}$?

- Semantics of classical logics maps interpretations to truth-values.

What is the Semantics of Sd$\mathcal{L}$?

- Semantics of classical logics maps interpretations to truth-values.
- This does not work for Sd$\mathcal{L}$, because state evolution of α in $\langle\alpha\rangle f$ is stochastic.

What is the Semantics of Sd$\mathcal{L}$?

- Semantics of classical logics maps interpretations to truth-values.
- This does not work for Sd$\mathcal{L}$, because state evolution of α in $\langle\alpha\rangle f$ is stochastic.
- Semantics of Sd$\mathcal{L}$ is stochastic.
- Semantics of Sd$\mathcal{L}$ is a random variable generator $[\![f]\!] : (\Omega \to \mathbb{R}^d) \to (\Omega \to \mathbb{R})$ giving a random variable $[\![f]\!]^Z : \Omega \to \mathbb{R}$ for each initial state random variable Z

Stochastic Differential Dynamic Logic Sd$\mathcal{L}$: Semantics

Definition (Measurable semantics)

Stochastic Differential Dynamic Logic Sd$\mathcal{L}$: Semantics

Definition (Measurable semantics)

$$[\![F]\!]^Z = F^\ell(Z) \text{ i.e., } [\![F]\!]^Z(\omega) = F^\ell(Z(\omega))$$

Stochastic Differential Dynamic Logic Sd$\mathcal{L}$: Semantics

Definition (Measurable semantics)

$$[\![F]\!]^Z = F^\ell(Z) \text{ i.e., } [\![F]\!]^Z(\omega) = F^\ell(Z(\omega))$$

$$[\![\lambda f + \nu g]\!]^Z = \lambda [\![f]\!]^Z + \nu [\![g]\!]^Z$$

Stochastic Differential Dynamic Logic Sd$\mathcal{L}$: Semantics

Definition (Measurable semantics)

$$[\![F]\!]^Z = F^\ell(Z) \text{ i.e., } [\![F]\!]^Z(\omega) = F^\ell(Z(\omega))$$

$$[\![\lambda f + \nu g]\!]^Z = \lambda[\![f]\!]^Z + \nu[\![g]\!]^Z$$

$$[\![Bf]\!]^Z = [\![B]\!]^Z * [\![f]\!]^Z \text{ i.e., } [\![Bf]\!]^Z(\omega) = [\![B]\!]^Z(\omega)[\![f]\!]^Z(\omega)$$

Definition (Measurable semantics)

$$[\![F]\!]^Z = F^\ell(Z) \text{ i.e., } [\![F]\!]^Z(\omega) = F^\ell(Z(\omega))$$

$$[\![\lambda f + \nu g]\!]^Z = \lambda[\![f]\!]^Z + \nu[\![g]\!]^Z$$

$$[\![Bf]\!]^Z = [\![B]\!]^Z * [\![f]\!]^Z \text{ i.e., } [\![Bf]\!]^Z(\omega) = [\![B]\!]^Z(\omega)[\![f]\!]^Z(\omega)$$

$$[\![\langle\alpha\rangle f]\!]^Z = \sup\{[\![f]\!]^{[\![\alpha]\!]_t^Z} \ : \ 0 \le t \le (\!|\alpha|\!)^Z\}$$

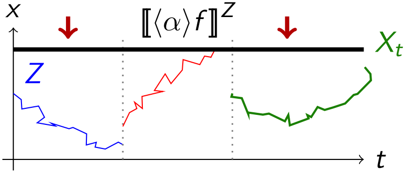
Definition (Measurable semantics)

$$[\![F]\!]^Z = F^\ell(Z) \text{ i.e., } [\![F]\!]^Z(\omega) = F^\ell(Z(\omega))$$

$$[\![\lambda f + \nu g]\!]^Z = \lambda[\![f]\!]^Z + \nu[\![g]\!]^Z$$

$$[\![Bf]\!]^Z = [\![B]\!]^Z * [\![f]\!]^Z \text{ i.e., } [\![Bf]\!]^Z(\omega) = [\![B]\!]^Z(\omega)[\![f]\!]^Z(\omega)$$

$$[\![\langle\alpha\rangle f]\!]^Z = \sup\{[\![f]\!]^{[\![\alpha]\!]_t^Z} \;:\; 0 \le t \le (\!|\alpha|\!)^Z\}$$



Well-definedness of Sd$\mathcal{L}$ Semantics

Theorem (Measurable)

$[\![f]\!]^Z$ *is a random variable (i.e., measurable) for any random variable* Z *and* Sd$\mathcal{L}$ *term* f.

Well-definedness of Sd$\mathcal{L}$ Semantics

Theorem (Measurable)

$[\![f]\!]^Z$ is a random variable (i.e., measurable) for any random variable Z and Sd$\mathcal{L}$ *term f.*

Corollary (Pushforward measure well-defined for Borel-measurable S)

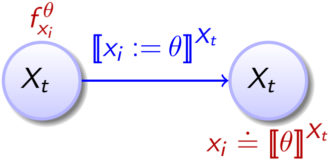
$$S \mapsto P(([\![f]\!]^Z)^{-1}(S)) = P(\{\omega \in \Omega \;:\; [\![f]\!]^Z(\omega) \in S\}) = P([\![f]\!]^Z \in S)$$

Outline (Verification Approach)

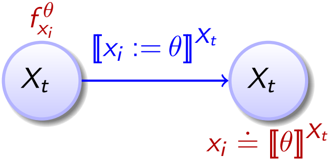
1. Motivation
2. Stochastic Differential Dynamic Logic Sd$\mathcal{L}$
   - Design
   - Stochastic Differential Equations
   - Syntax
   - Semantics
   - Well-definedness
3. Stochastic Differential Dynamic Logic
   - Syntax
   - Semantics
   - Well-definedness
4. Proof Calculus for Stochastic Hybrid Systems
   - Compositional Proof Calculus
   - Soundness
5. Conclusions

Proof Calculus for Stochastic Differential Dynamic Logic

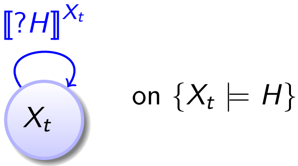
$$\langle x_i := \theta \rangle f \; = \; f_{x_i}^{\theta}$$



$$\langle x_i := \theta \rangle f = f_{x_i}^{\theta}$$

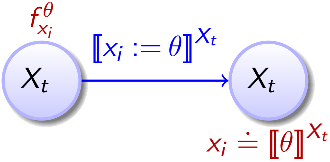


$$\langle ?H \rangle f = Hf$$

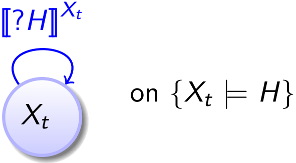


Proof Calculus for Stochastic Differential Dynamic Logic

$$\langle x_i := \theta \rangle f = f_{x_i}^{\theta}$$



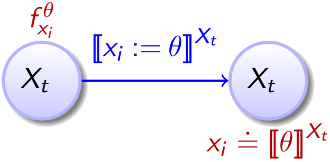
$$\langle ?H \rangle f = Hf$$



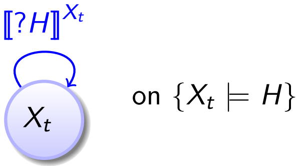
$$\langle \alpha \rangle (\lambda f) = \lambda \langle \alpha \rangle f$$

Proof Calculus for Stochastic Differential Dynamic Logic

$$\langle x_i := \theta \rangle f \;=\; f_{x_i}^{\theta}$$



$$\langle ?H \rangle f \;=\; Hf$$

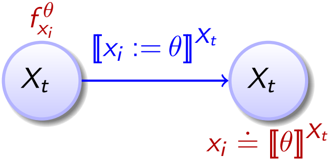


$$\langle \alpha \rangle (\lambda f) \;=\; \lambda \langle \alpha \rangle f$$

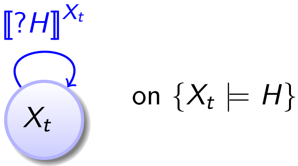
$$\langle \alpha \rangle (\lambda f + \nu g) \;\le\; \lambda \langle \alpha \rangle f + \nu \langle \alpha \rangle g$$

Proof Calculus for Stochastic Differential Dynamic Logic

$$\langle x_i := \theta \rangle f = f_{x_i}^{\theta}$$



$$\langle ?H \rangle f = Hf$$



$$\langle \alpha \rangle (\lambda f) = \lambda \langle \alpha \rangle f$$

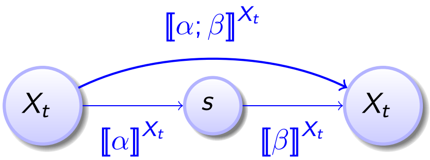
$$\langle \alpha \rangle (\lambda f + \nu g) \leq \lambda \langle \alpha \rangle f + \nu \langle \alpha \rangle g$$

$$f \leq g \models \langle \alpha \rangle f \leq \langle \alpha \rangle g$$

Proof Calculus for Stochastic Differential Dynamic Logic

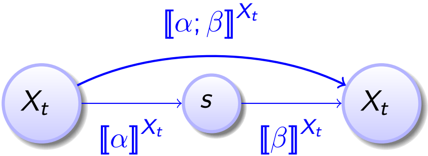
$\langle \alpha; \beta \rangle f \leq \langle \alpha \rangle (f \sqcup \langle \beta \rangle f)$

$f \leq \langle \beta \rangle f \vDash$
$\langle \alpha; \beta \rangle f \leq \langle \alpha \rangle \langle \beta \rangle f$

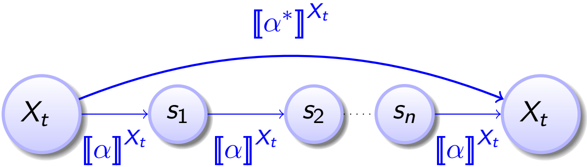


$\langle\alpha;\beta\rangle f \leq \langle\alpha\rangle(f \sqcup \langle\beta\rangle f)$

$f \leq \langle\beta\rangle f \vDash$
$\langle\alpha;\beta\rangle f \leq \langle\alpha\rangle\langle\beta\rangle f$



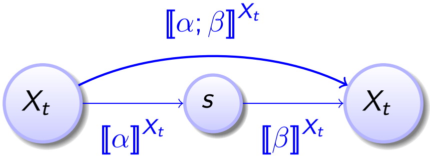
$\langle\alpha\rangle f \leq f \vDash \langle\alpha^*\rangle f \leq f$



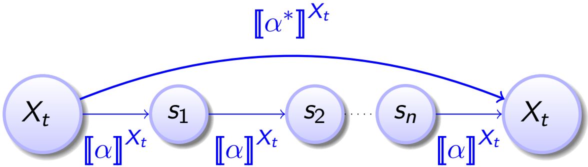
Proof Calculus for Stochastic Differential Dynamic Logic

$$\langle\alpha;\beta\rangle f \;\le\; \langle\alpha\rangle(f \sqcup \langle\beta\rangle f)$$

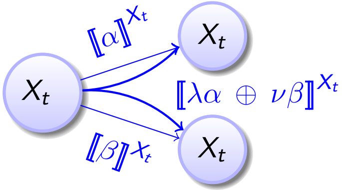
$$f \le \langle\beta\rangle f \vDash$$
$$\langle\alpha;\beta\rangle f \;\le\; \langle\alpha\rangle\langle\beta\rangle f$$



$$\langle\alpha\rangle f \le f \vDash \langle\alpha^*\rangle f \le f$$



$$P(\langle\lambda\alpha \oplus \nu\beta\rangle f \in S)$$
$$= \lambda P(\langle\alpha\rangle f \in S)$$
$$+ \nu P(\langle\beta\rangle f \in S)$$



Soundness

Theorem (Soundness)

Sd$\mathcal{L}$ *calculus is sound.*

1. *Rules are globally sound pathwise, i.e.,* $f_i \leq g_i \vDash f \leq g$ *holds for each initial* Z *pathwise for each* $\omega \in \Omega$
2. $\langle \oplus \rangle$ *is sound in distribution*

Soundness

Theorem (Soundness)

Sd$\mathcal{L}$ *calculus is sound.*

1. *Rules are globally sound pathwise, i.e.,* $f_i \leq g_i \vDash f \leq g$ *holds for each initial* Z *pathwise for each* $\omega \in \Omega$
2. $\langle \oplus \rangle$ *is sound in distribution*

Theorem (Soundness for SDE)

Let $\lambda > 0$, $f \in C^2(\mathbb{R}^d, \mathbb{R})$ *compact support on* H *(e.g.,* H *bounded)*

$$\frac{\langle \alpha \rangle (H \to f) \leq \lambda p \quad H \to f \geq 0 \quad H \to Lf \leq 0}{P(\langle \alpha \rangle \langle dx = bdt + \sigma dW \,\&\, H \rangle f \geq \lambda) \leq p} \text{ sound}$$

Proof Example

$$\frac{\langle\alpha\rangle(H \to f) \le \lambda p \quad H \to f \ge 0 \quad H \to Lf \le 0}{P(\langle\alpha\rangle\langle dx = bdt + \sigma dW \,\&\, H\rangle f \ge \lambda) \le p}$$

$$\langle ?x^2 + y^2 \le \frac{1}{3}\rangle(H \to f) = \left(H \to x^2 + y^2 \le \frac{1}{3}\right)(x^2 + y^2) \le 1 * \frac{1}{3}$$

$$f \equiv x^2 + y^2 \ge 0 \qquad \text{with} \qquad H \equiv x^2 + y^2 < 10$$

$$\frac{Lf = \frac{1}{2}\left(-x\frac{\partial f}{\partial x} - y\frac{\partial f}{\partial y} + y^2\frac{\partial^2 f}{\partial x^2} - 2xy\frac{\partial^2 f}{\partial x \partial y} + x^2\frac{\partial^2 f}{\partial y^2}\right) \le 0}{P(\langle ?x^2 + y^2 \le \frac{1}{3}; dx = -\frac{x}{2}dt - ydW, dy = -\frac{y}{2}dt + xdW \,\&\, H\rangle x^2 + y^2 \ge 1)}$$

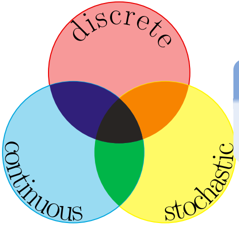
$$\le \qquad (\text{by } \langle;\rangle')$$

$$P(\langle ?x^2 + y^2 \le \frac{1}{3}\rangle\langle dx = -\frac{x}{2}dt - ydW, dy = -\frac{y}{2}dt + xdW \,\&\, H\rangle x^2 + y^2 \ge 1$$

$$\le \frac{1}{3}$$

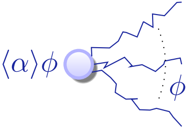
Outline

Conclusions



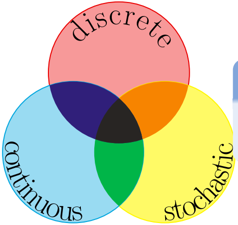
stochastic differential dynamic logic

$$\mathsf{Sd}\mathcal{L} = \mathsf{DL}_{\mathsf{arithmetic}} + \mathsf{SHP}$$



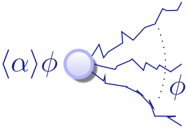
- Stochastic hybrid systems
- Compositional system model & semantics
- Logic for stochastic hybrid systems
- Well-definedness & measurability
- Stochastics accessible in logic
- Compositional proof rules
- Stochastic calculus & symbolic logic

Conclusions

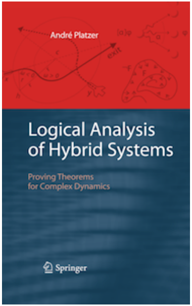


stochastic differential dynamic logic

$$\mathrm{Sd}\mathcal{L} = \mathrm{DL}_{\mathrm{arithmetic}} + \mathrm{SHP}$$



- Stochastic hybrid systems
- Compositional system model & semantics
- Logic for stochastic hybrid systems
- Well-definedness & measurability
- Stochastics accessible in logic
- Compositional proof rules
- Stochastic calculus & symbolic logic



Plan Ahead

- Extend study of stochastic effects in hybrid systems
- Structural properties of differential invariants
- Computing differential invariants and AI
- Heterogeneity in verification