Logic and Compositional Verification of Stochastic Hybrid Systems

André Platzer

Carnegie Mellon University, Pittsburgh, PA
Outline

1. Motivation

2. Stochastic Differential Dynamic Logic SdL
   - 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
Cyber-Physical Systems:

Q: I want to verify trains

Challenge

André Platzer (CMU) Logic and Compositional Verification of Stochastic Hybrid Systems

CMACS 2 / 24
Q: I want to verify trains  
A: Hybrid systems

Challenge (Hybrid Systems)

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)
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)
Q: I want to verify uncertain trains

Challenge

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

André Platzer (CMU)
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)
Q: I want to verify uncertain trains

Challenge

Continuous dynamics (differential equations)
Discrete dynamics (control decisions)
Stochastic dynamics (uncertainty)
Discrete stochastic (lossy communication)
Continuous stochastic (wind, track)

André Platzer (CMU)
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)
Cyber-Physical Systems

discrete
Cyber-Physical Systems

Logic and Compositional Verification of Stochastic Hybrid Systems
Cyber-Physical Systems

André Platzer (CMU) Logic and Compositional Verification of Stochastic Hybrid Systems CMACS 5 / 24
Cyber-Physical Systems

André Platzer (CMU) Logic and Compositional Verification of Stochastic Hybrid Systems

CMACS 5 / 24
Cyber-Physical Systems

André Platzer (CMU)  Logic and Compositional Verification of Stochastic Hybrid Systems  CMACS 5 / 24
Cyber-Physical Systems

André Platzer (CMU) Logic and Compositional Verification of Stochastic Hybrid Systems CMACS 5 / 24
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

1. Motivation

2. Stochastic Differential Dynamic Logic $\mathcal{SdL}$
   - 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
Outline (Conceptual Approach)

1 Motivation

2 Stochastic Differential Dynamic Logic $\mathcal{SdL}$
   - 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

\[ a := -b \]

discrete
Model for Stochastic Hybrid Systems

\[ a := -b \]

\[ \frac{d^2 x}{dt^2} = a \]
Model for Stochastic Hybrid Systems

\[ a := -b \]

\[ \frac{d^2 x}{dt^2} = a \]

\[ \frac{1}{3} a := -b \oplus \frac{2}{3} a := a + 1 \]
Model for Stochastic Hybrid Systems

\[ a := -b \]

\[ \frac{d^2 x}{dt^2} = a \]

\[ \frac{1}{3} a := -b \oplus \frac{2}{3} a := a + 1 \]

 André Platzer (CMU)  Logic and Compositional Verification of Stochastic Hybrid Systems  CMACS  7 / 24
Model for Stochastic Hybrid Systems

\[
\frac{d^2 x}{dt^2} = a
\]

\[
a := -b; \frac{d^2 x}{dt^2} = a
\]

\[
\frac{1}{3} a := -b \oplus \frac{2}{3} a := a + 1
\]
Model for Stochastic Hybrid Systems

\[ \begin{align*}
  a &:= -b \\
  \frac{d^2 x}{dt^2} &:= a \\
  \frac{\partial^2 X}{\partial t^2} &:= a \\
  dX = bdt + \sigma dW
\end{align*} \]
Model for Stochastic Hybrid Systems

\[
\begin{align*}
  a &:= -b \\
  \frac{d^2x}{dt^2} &= a \\
  dX &= bdt + \sigma dW \\
  \frac{1}{3} a &:= -b \oplus \frac{2}{3} a := a + 1
\end{align*}
\]
Q: How to model stochastic hybrid systems

Model (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)
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)
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)
  \[ \frac{1}{3}a := -b \oplus \frac{2}{3}a := a + 1 \]
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)
  \[ \frac{1}{3}a := -b \oplus \frac{2}{3}a := a + 1 \]
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)
  \[ \frac{1}{3}a := -b \oplus \frac{2}{3}a := a + 1 \]
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)
  \[ \frac{1}{3}a := -b \oplus \frac{2}{3}a := a + 1 \]
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)
  \[ \frac{1}{3}a := -b \oplus \frac{2}{3}a := a + 1 \]
Q: How to model stochastic hybrid systems

Model (Stochastic Hybrid Systems)

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

- 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 (Itô stochastic differential equation (SDE))**

$$dX_t = b(X_t)dt + \sigma(X_t)dW_t \quad X_0 = Z$$
Stochastic Differential Equations (SDE)

Definition (Ordinary differential equation (ODE))

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

Definition (Itô 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))

\[
X_s = Z + \int_0^s dX_t = Z + \int_0^s b(X_t)dt + \int_0^s \sigma(X_t)dW_t
\]
Stochastic Differential Equations (SDE)

**Definition (Ordinary differential equation (ODE))**

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

**Definition (Itô 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 $W$)

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 $W$)**

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, $\not\in FV$, nonmonotonic on every interval
### Definition (Stochastic hybrid program $\alpha$)

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x := \theta$</td>
<td>Assignment</td>
</tr>
<tr>
<td>$x := *$</td>
<td>Random assignment</td>
</tr>
<tr>
<td>$?H$</td>
<td>Conditional execution</td>
</tr>
<tr>
<td>$dx = bdt + \sigma dW &amp; H$</td>
<td>SDE</td>
</tr>
<tr>
<td>$\alpha; \beta$</td>
<td>Seq. composition</td>
</tr>
<tr>
<td>$\lambda \alpha \oplus \nu \beta$</td>
<td>Convex combination</td>
</tr>
<tr>
<td>$\alpha^*$</td>
<td>Nondet. repetition</td>
</tr>
</tbody>
</table>

Jump & Test: $\{\}$

Algebra: $\{\}$
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 $Z : \Omega \rightarrow \mathbb{R}^d$.
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 \( Z : \Omega \rightarrow \mathbb{R}^d \)
- Semantics of program \( \alpha \) is stochastic process generator
  \[ [\alpha] : (\Omega \rightarrow \mathbb{R}^d) \rightarrow ([0, \infty) \times \Omega \rightarrow \mathbb{R}^d) \] giving stochastic process
  \[ [\alpha]^Z : [0, \infty) \times \Omega \rightarrow \mathbb{R}^d \] 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 $\alpha$ is stochastic process generator $\llbracket \alpha \rrbracket : (\Omega \to \mathbb{R}^d) \to ([0, \infty) \times \Omega \to \mathbb{R}^d)$ giving stochastic process $\llbracket \alpha \rrbracket^Z : [0, \infty) \times \Omega \to \mathbb{R}^d$ for each $Z$
- When does a stochastic process stop?
- Semantics of program $\alpha$ includes stopping time generator $\llbracket \alpha \rrbracket : (\Omega \to \mathbb{R}^d) \to (\Omega \to \mathbb{R})$ giving stopping time $\llbracket \alpha \rrbracket^Z : \Omega \to \mathbb{R}$ for each $Z$
**Stochastic Hybrid Program: Process Semantics**

Definition (Stochastic hybrid program $\alpha$: process semantics)

- $[x_i := \theta]^Z = \hat{Y}$
- $Y(\omega)_i = [\theta]^Z(\omega)$ and $Y_j = Z_j$ (for $j \neq i$)
- $(|x_i := \theta|^Z = 0$

![Diagram](attachment:image.png)

- $X_t$ if $X_t,i = [\theta]^Z$ and $X_t,j = Z_j$ for $j \neq i$
Stochastic Hybrid Program: Process Semantics

Definition (Stochastic hybrid program $\alpha$: process semantics)

$$\left[ x_i := \ast \right]^Z = \hat{U} \quad U_i \sim U(0, 1) \text{ i.i.d. } F_0\text{-measurable}$$

$$\left( x_i := \ast \right)^Z = 0$$

- $x_i \sim U(0, 1)$
- $X_t(z) = Z(z)$ for $z \neq x$

André Platzer (CMU) Logic and Compositional Verification of Stochastic Hybrid Systems CMACS 13 / 24
Stochastic Hybrid Program: Process Semantics

Definition (Stochastic hybrid program $\alpha$: process semantics)

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

\[
(\neg ?H)^Z = 0
\]

no change on $\{ Z \models H \}$
otherwise not defined

Andre Platzer (CMU)
Stochastic Hybrid Program: Process Semantics

\[
\begin{align*}
\text{Definition (Stochastic hybrid program } \alpha \text{: process semantics)} \\
\left[ dx = b dt + \sigma dW &\ H \right]_Z \\
\text{solves } \ dX = \left[ b \right]_X dt + \left[ \sigma \right]_X dB_t, \ X_0 = Z \\
\left( dx = b dt + \sigma dW &\ H \right)_Z = \inf \{ t \geq 0 : X \notin H \}
\end{align*}
\]
Definition (Stochastic hybrid program $\alpha$: process semantics)

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

$$
\left(\lambda \alpha \oplus \nu \beta\right)_Z^Z = \mathcal{I}_{U \leq \lambda} \left(|\alpha|\right)_Z^Z + \mathcal{I}_{U > \lambda} \left(|\beta|\right)_Z^Z \text{ with i.i.d. } U \sim \mathcal{U}(0, 1), \mathcal{F}_0\text{-meas}
$$
Definition (Stochastic hybrid program $\alpha$: process semantics)

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

\[
(|\alpha; \beta|)^Z = (|\alpha|)^Z + (|\beta|)[\alpha]^{Z}_{(\alpha)^Z}
\]
Definition (Stochastic hybrid program $\alpha$: process semantics)

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

\[
([\alpha^*]^Z = \lim_{n \to \infty} ([\alpha^n]^Z)
\]
Definition (Stochastic hybrid program $\alpha$: process semantics)

\[
\begin{align*}
[\alpha^*]^Z_t &= [\alpha^n]^Z_t \text{ on event } \{([\alpha^n]^Z > t) \}
\\
([\alpha^*]^Z &= \lim_{n \to \infty} ([\alpha^n]^Z \text{ monotone!})
\end{align*}
\]
Theorem

1. $\llbracket \alpha \rrbracket^Z$ 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., $\{(|\alpha|^Z \leq t}\in \mathcal{F}_t$)

$\implies$ End value $\llbracket \alpha \rrbracket^Z_{|\alpha|^Z}$ is $\mathcal{F}_{|\alpha|^Z}$-measurable.
Outline

1 Motivation

2 Stochastic Differential Dynamic Logic \( SdL \)
   - 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
### Definition (SdL term \( f \))

- \( F \) (primitive measurable function, e.g., characteristic \( I_A \))
- \( \lambda f + \nu g \) (linear term)
- \( Bf \) (scalar term for boolean term \( B \))
- \( \langle \alpha \rangle f \) (reachable)

### Definition (SdL formula \( \phi \))

\[
\phi ::= f \leq g \mid f = g
\]
What is the Semantics of $SdL$?

- Semantics of classical logics maps interpretations to truth-values.
  - Semantics of $SdL$ is stochastic.
  - Semantics of $SdL$ is a random variable generator $\mathbb{E}[f] : (\Omega \rightarrow \mathbb{R}^d) \rightarrow (\Omega \rightarrow \mathbb{R})$ giving a random variable $\mathbb{E}[f]Z$ for each initial state random variable $Z$. 
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 \(\alpha\) in \(\langle \alpha \rangle f\) is stochastic.
What is the Semantics of SdL?

- Semantics of classical logics maps interpretations to truth-values.
- This does not work for SdL, because state evolution of $\alpha$ in $\langle \alpha \rangle f$ is stochastic.
- Semantics of SdL is stochastic.
- Semantics of SdL is a random variable generator $\llbracket f \rrbracket : (\Omega \rightarrow \mathbb{R}^d) \rightarrow (\Omega \rightarrow \mathbb{R})$ giving a random variable $\llbracket f \rrbracket^Z : \Omega \rightarrow \mathbb{R}$ for each initial state random variable $Z$. 
Definition (Measurable semantics)

\[ F[Z] = F[\ell](Z) \]

\[ \lambda[f] + \nu[g] = \lambda[f[Z]] + \nu[g[Z]] \]

\[ B[f] = [B[Z]] \]

\[ \langle \alpha \rangle [f] = \sup_{0 \leq t \leq |\alpha|} [f[Z]]_{t} \]
Definition (Measurable semantics)

\[
[F]^Z = F^\ell(Z) \text{ i.e., } [F]^Z(\omega) = F^\ell(Z(\omega))
\]
Definition (Measurable semantics)

\[ \llbracket F \rrbracket^Z = F^\ell(Z) \text{ i.e., } \llbracket F \rrbracket^Z(\omega) = F^\ell(Z(\omega)) \]
\[ \llbracket \lambda f + \nu g \rrbracket^Z = \lambda \llbracket f \rrbracket^Z + \nu \llbracket g \rrbracket^Z \]
Definition (Measurable semantics)

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

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

\[ [Bf]^Z = [B]^Z * [f]^Z \text{ i.e., } [Bf]^Z(\omega) = [B]^Z(\omega)[f]^Z(\omega) \]
### Definition (Measurable semantics)

\[
\begin{align*}
[F]^Z &= F^\ell(Z) \text{ i.e., } [F]^Z(\omega) = F^\ell(Z(\omega)) \\
[\lambda f + \nu g]^Z &= \lambda [f]^Z + \nu [g]^Z \\
[Bf]^Z &= [B]^Z \ast [f]^Z \text{ i.e., } [Bf]^Z(\omega) = [B]^Z(\omega)[f]^Z(\omega) \\
[\langle \alpha \rangle f]^Z &= \sup\{[f][\alpha]^Z_t : 0 \leq t \leq (|\alpha|)^Z\}
\end{align*}
\]
Definition (Measurable semantics)

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

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

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

\[ \langle \alpha \rangle f]^Z = \sup\{[f]^Z_{\lambda f} : 0 \leq t \leq (|\alpha|)^Z \} \]
Well-definedness of SdL Semantics

**Theorem (Measurable)**

$[f]^Z$ is a random variable (i.e., measurable) for any random variable $Z$ and SdL term $f$. 
Well-definedness of Sd$L$ Semantics

**Theorem (Measurable)**

$[f]^Z$ is a random variable (i.e., measurable) for any random variable $Z$ and Sd$L$ term $f$.

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

$$S \mapsto P((f^Z)^{-1}(S)) = P\left(\{\omega \in \Omega : f^Z(\omega) \in S\}\right) = P(f^Z \in S)$$
Outline (Verification Approach)

1. Motivation

2. Stochastic Differential Dynamic Logic $\mathcal{SdL}$
   - 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
\[ \langle x_i := \theta \rangle f = f^\theta_{x_i} \]
\[ \langle x_i := \theta \rangle f = f^\theta_{x_i} \]

\[ \langle ?H \rangle f = Hf \]
Proof Calculus for Stochastic Dynamic Logic

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

$\langle ? H \rangle f = Hf$

$\langle \alpha \rangle (\lambda f) = \lambda \langle \alpha \rangle f$
\[ \langle x_i := \theta \rangle f = f^\theta_{x_i} \]

\[ \langle ?H \rangle f = Hf \]

\[ \langle \alpha \rangle (\lambda f) = \lambda \langle \alpha \rangle f \]

\[ \langle \alpha \rangle (\lambda f + \nu g) \leq \lambda \langle \alpha \rangle f + \nu \langle \alpha \rangle g \]
\[ \langle x_i := \theta \rangle f = f^\theta_{x_i} \]

\[ \langle ?H \rangle f = Hf \]

\[ \langle \alpha \rangle (\lambda f) = \lambda \langle \alpha \rangle f \]

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

\[ f \leq g \models \langle \alpha \rangle f \leq \langle \alpha \rangle g \]
\[ \langle \alpha; \beta \rangle f \leq \langle \alpha \rangle (f \sqcup \langle \beta \rangle f) \]

\[ f \leq \langle \beta \rangle f \models \]

\[ \langle \alpha; \beta \rangle f \leq \langle \alpha \rangle \langle \beta \rangle f \]
\[ \langle \alpha; \beta \rangle f \leq \langle \alpha \rangle (f \sqcup \langle \beta \rangle f) \]
\[ f \leq \langle \beta \rangle f \models \]
\[ \langle \alpha; \beta \rangle f \leq \langle \alpha \rangle \langle \beta \rangle f \]

\[ \langle \alpha \rangle f \leq f \models \langle \alpha^* \rangle f \leq f \]

\[ P(\langle \lambda \alpha \oplus \nu \beta \rangle f \in S) = \lambda P(\langle \alpha \rangle f \in S) + \nu P(\langle \beta \rangle f \in S) \]
\[
\langle \alpha; \beta \rangle f \leq \langle \alpha \rangle (f \sqcup \langle \beta \rangle f)
\]

\[
f \leq \langle \beta \rangle f \models \langle \alpha; \beta \rangle f \leq \langle \alpha \rangle \langle \beta \rangle f
\]

\[
\langle \alpha \rangle f \leq f \models \langle \alpha^* \rangle f \leq f
\]

\[
P(\langle \lambda \alpha \oplus \nu \beta \rangle f \in S) = \lambda P(\langle \alpha \rangle f \in S) + \nu P(\langle \beta \rangle f \in S)
\]
Theorem (Soundness)

SdŁ calculus is sound.

1. Rules are globally sound pathwise, i.e., \( f_i \leq g_i \models f \leq g \) holds for each initial \( Z \) pathwise for each \( \omega \in \Omega \).

2. \( \langle \oplus \rangle \) is sound in distribution.
Soundness

Theorem (Soundness)

\( \text{SdL calculus is sound.} \)

1. Rules are globally sound pathwise, i.e., \( f_i \leq g_i \models f \leq g \) 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)

\[
\langle \alpha \rangle (H \rightarrow f) \leq \lambda p \quad H \rightarrow f \geq 0 \quad H \rightarrow Lf \leq 0
\]

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

\frac{P(\langle \alpha \rangle \langle dx = b dt + \sigma dW & H \rangle f \geq \lambda)}{p} \leq 1

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

f \equiv x^2 + y^2 \geq 0 \quad \text{with} \quad H \equiv x^2 + y^2 < 10

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) \leq 0

P(\langle ?x^2 + y^2 \leq \frac{1}{3}; dx = -\frac{x}{2} dt - ydW, dy = -\frac{y}{2} dt + xdW & H \rangle x^2 + y^2 \geq 1) \leq \frac{1}{3} \quad \text{(by } \langle ; / \rangle')

P(\langle ?x^2 + y^2 \leq \frac{1}{3} \rangle \langle dx = -\frac{x}{2} dt - ydW, dy = -\frac{y}{2} dt + xdW & H \rangle x^2 + y^2 \geq 1) \leq \frac{1}{3}
Outline

1. Motivation

2. Stochastic Differential Dynamic Logic $\mathcal{SdL}$
   - 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
Conclusions

- 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

\[ Sd\mathcal{L} = DL_{\text{arithmetic}} + SHP \]
Conclusions

- 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

\[ \text{stochastic differential dynamic logic} \]

\[ SdL = DL_{\text{arithmetic}} + \text{SHP} \]
Plan Ahead

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