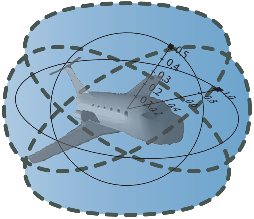
Logics of Dynamical Systems

André Platzer

aplatzer@cs.cmu.edu
Computer Science Department
Carnegie Mellon University, Pittsburgh, PA

http://symbolaris.com/



Outline

1. Motivation
2. Differential Dynamic Logic $d\mathcal{L}$
   - Syntax
   - Branching Transition Structures
   - Semantics
   - Ex: Car Control Design
   - Ex: Bouncing Ball
   - Compositionality in Hybrid Systems
3. Axiomatization
   - Compositional Proof Calculus
   - Deduction Modulo by Side Deduction
   - Deduction Modulo with Free Variables & Skolemization
   - Soundness and Completeness
4. Survey
5. Summary

Outline

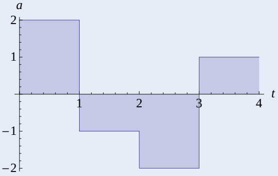
1. Motivation
2. Differential Dynamic Logic d$\mathcal{L}$
   - Syntax
   - Branching Transition Structures
   - Semantics
   - Ex: Car Control Design
   - Ex: Bouncing Ball
   - Compositionality in Hybrid Systems
3. Axiomatization
   - Compositional Proof Calculus
   - Deduction Modulo by Side Deduction
   - Deduction Modulo with Free Variables & Skolemization
   - Soundness and Completeness
4. Survey
5. Summary

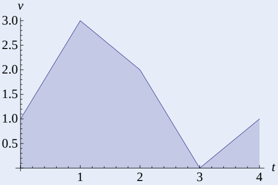
How can we design computers that are guaranteed to interact correctly with the physical world?

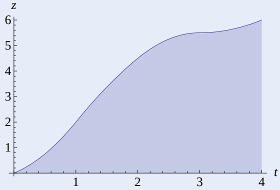
Hybrid Systems Analysis: Car Control

Challenge (Hybrid Systems)

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







Hybrid Systems Analysis: Car Control

Challenge (Hybrid Systems)

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

1. More than computers: no `NullPointerException` $\not\Rightarrow$ safe

Hybrid Systems Analysis: Car Control

Challenge (Hybrid Systems)

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

1. More than computers: no `NullPointerException` $\not\Rightarrow$ safe
2. More than physics: braking control $v^2 \leq 2b(MA - z)$ $\not\Rightarrow$ safe

Hybrid Systems Analysis: Car Control

Challenge (Hybrid Systems)

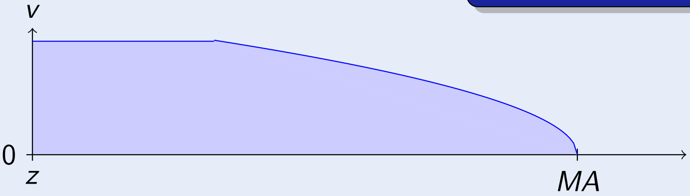
- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)

1. More than computers: no `NullPointerException` $\not\Rightarrow$ safe
2. More than physics: braking control $v^2 \leq 2b(MA - z) \not\Rightarrow$ safe
3. Joint dynamics requires: $SB \geq \frac{v^2}{2b} + \frac{a^2\varepsilon^2}{2b} + \frac{a}{b}\varepsilon v + \frac{a}{2}\varepsilon^2 + \varepsilon v \dots$

Hybrid Systems Analysis: Car Control

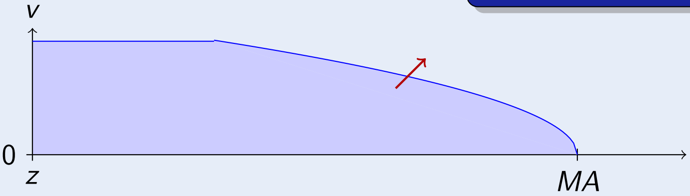
Challenge (Hybrid Systems)

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



Challenge (Hybrid Systems)

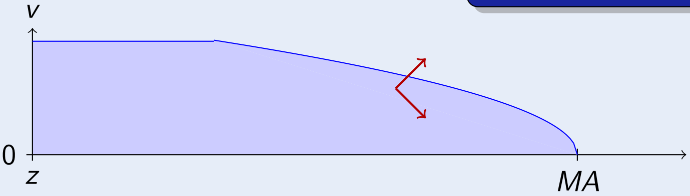
- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)



Hybrid Systems Analysis: Car Control

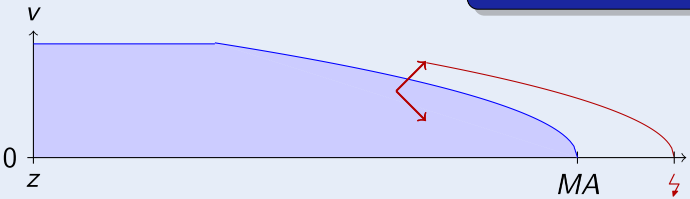
Challenge (Hybrid Systems)

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



Challenge (Hybrid Systems)

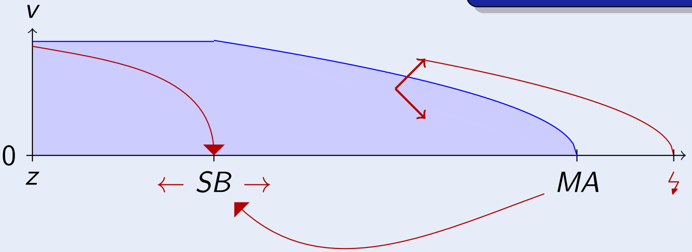
- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)



Hybrid Systems Analysis: Car Control

Challenge (Hybrid Systems)

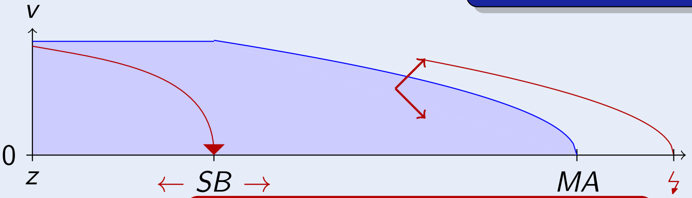
- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)



Hybrid Systems Analysis: Car Control

Challenge (Hybrid Systems)

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

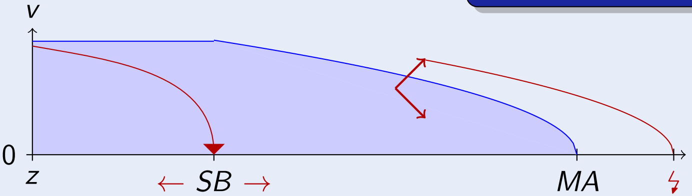


$$SB \geq \frac{v^2}{2b} + \frac{a^2\varepsilon^2}{2b} + \frac{a}{b}\varepsilon v + \frac{a}{2}\varepsilon^2 + \varepsilon v$$

Hybrid Systems Analysis: Car Control

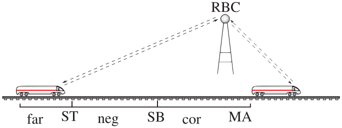
Challenge (Hybrid Systems)

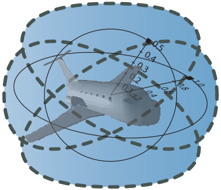
- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)

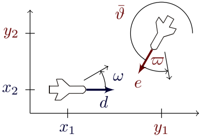


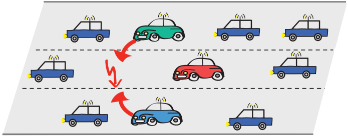
$\forall MA \, \exists SB$ "Car always safe"

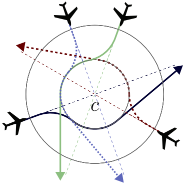
Hybrid Systems Analysis is Important for . . .

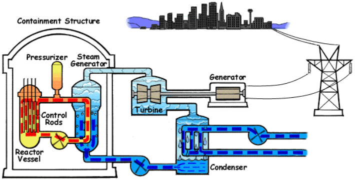


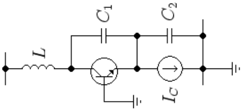












Outline

1. Motivation
2. Differential Dynamic Logic $d\mathcal{L}$
   - Syntax
   - Branching Transition Structures
   - Semantics
   - Ex: Car Control Design
   - Ex: Bouncing Ball
   - Compositionality in Hybrid Systems
3. Axiomatization
   - Compositional Proof Calculus
   - Deduction Modulo by Side Deduction
   - Deduction Modulo with Free Variables & Skolemization
   - Soundness and Completeness
4. Survey
5. Summary

Outline

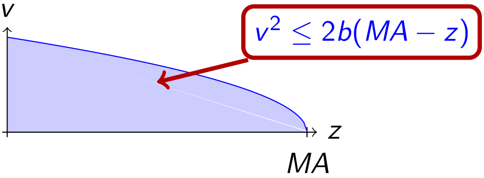
differential dynamic logic

$d\mathcal{L} = \quad \mathrm{DL} + \mathrm{HP}$

Differential Dynamic Logic for Hybrid Systems

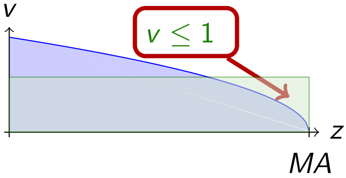
differential dynamic logic

$d\mathcal{L} = \text{FOL}_{\mathbb{R}}$



differential dynamic logic

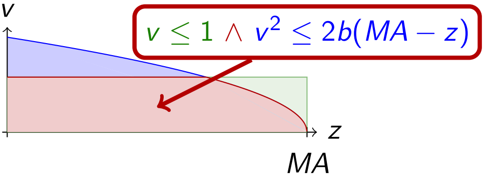
$d\mathcal{L} = \mathrm{FOL}_{\mathbb{R}}$



Differential Dynamic Logic for Hybrid Systems

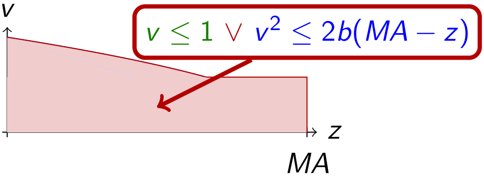
differential dynamic logic

$\mathrm{d}\mathcal{L} = \mathrm{FOL}_{\mathbb{R}}$



differential dynamic logic

$d\mathcal{L} = \text{FOL}_{\mathbb{R}}$



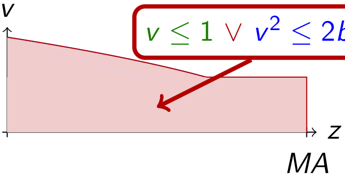
Differential Dynamic Logic for Hybrid Systems

differential dynamic logic

$d\mathcal{L} = \text{FOL}_{\mathbb{R}}$

$\forall MA\, \exists SB \ldots$

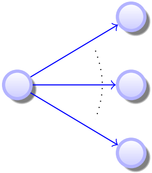
$\forall t{\geq}0 \ldots$



$v \leq 1 \lor v^2 \leq 2b(MA - z)$

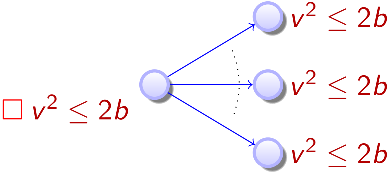
differential dynamic logic

$d\mathcal{L} = \text{FOL}_{\mathbb{R}} +$



differential dynamic logic

$\mathsf{d}\mathcal{L} = \mathrm{FOL}_{\mathbb{R}} + \mathrm{ML}$

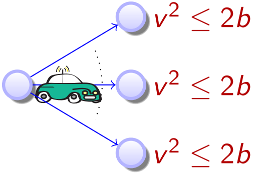


Differential Dynamic Logic for Hybrid Systems

differential dynamic logic

$d\mathcal{L} = \mathrm{FOL}_{\mathbb{R}} + \mathrm{DL}$

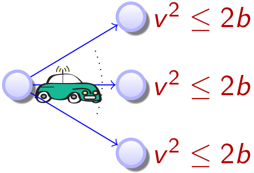
$[$  $]\; v^2 \leq 2b$



differential dynamic logic

$$\mathsf{d}\mathcal{L} = \mathrm{FOL}_{\mathbb{R}} + \mathrm{DL} + \mathrm{HP}$$

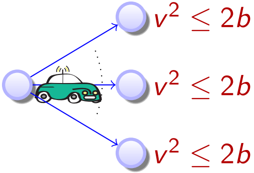
$$[z'' = a]\, v^2 \le 2b$$



differential dynamic logic

$$d\mathcal{L} = FOL_{\mathbb{R}} + DL + HP$$

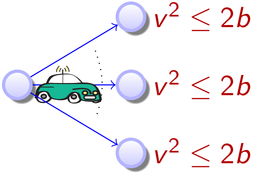
$$[\mathtt{if}(z > SB)\, a := -b;\ z'' = a]\, v^2 \leq 2b$$



differential dynamic logic

$$d\mathcal{L} = \mathrm{FOL}_{\mathbb{R}} + \mathrm{DL} + \mathrm{HP}$$

$$[\underbrace{\mathtt{if}(z > SB)\, a := -b;\ z'' = a}_{\text{hybrid program}}]\, v^2 \leq 2b$$

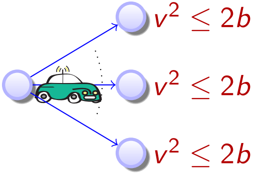


Differential Dynamic Logic for Hybrid Systems

differential dynamic logic

$d\mathcal{L} = \mathrm{FOL}_{\mathbb{R}} + \mathrm{DL} + \mathrm{HP}$

$$\mathcal{C} \to [\underbrace{\mathtt{if}(z > SB)\, a := -b;\ z'' = a}_{\text{hybrid program}}]\, v^2 \le 2b$$

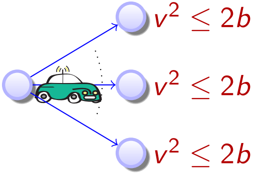


Differential Dynamic Logic for Hybrid Systems

differential dynamic logic

$$d\mathcal{L} = \mathrm{FOL}_{\mathbb{R}} + \mathrm{DL} + \mathrm{HP}$$

$$\mathcal{C} \rightarrow [\underbrace{\mathtt{if}(z > SB)\, a := -b;\ z'' = a}_{\text{hybrid program}}]\, v^2 \leq 2b$$



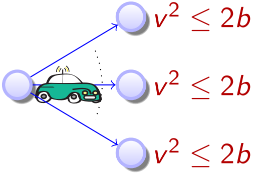
Initial condition

Differential Dynamic Logic for Hybrid Systems

differential dynamic logic

$d\mathcal{L} = \mathrm{FOL}_{\mathbb{R}} + \mathrm{DL} + \mathrm{HP}$

$$\mathcal{C} \rightarrow [\underbrace{\mathtt{if}(z > SB)\, a := -b;\ z'' = a}_{\text{hybrid program}}]\, v^2 \le 2b$$



Initial condition

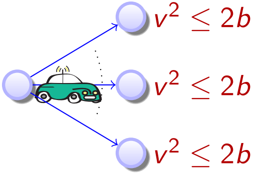
System dynamics

Differential Dynamic Logic for Hybrid Systems

differential dynamic logic

$d\mathcal{L} = \mathrm{FOL}_{\mathbb{R}} + \mathrm{DL} + \mathrm{HP}$

$$\mathcal{C} \rightarrow [\underbrace{\mathtt{if}(z > SB)\, a := -b;\ z'' = a}_{\text{hybrid program}}]\, v^2 \leq 2b$$



Initial condition

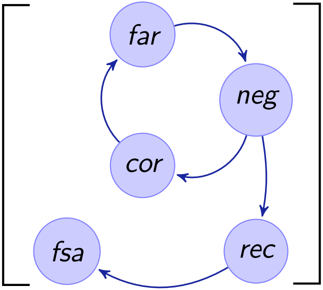
System dynamics

Post condition

Differential Dynamic Logic for Hybrid Systems

differential dynamic logic

$d\mathcal{L} = FOL_{\mathbb{R}} + DL + HP$

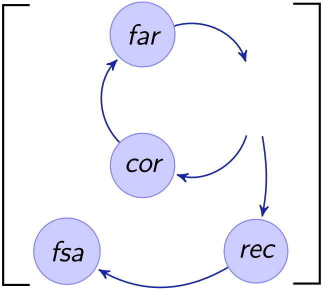


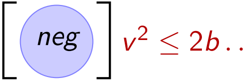
$v^2 \leq 2b..$

Differential Dynamic Logic for Hybrid Systems

differential dynamic logic

$d\mathcal{L} = FOL_{\mathbb{R}} + DL + HP$

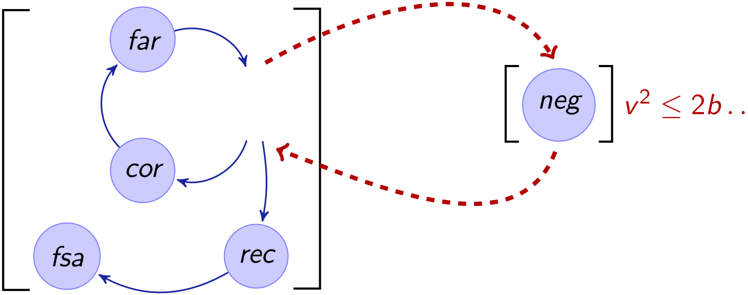




Differential Dynamic Logic for Hybrid Systems

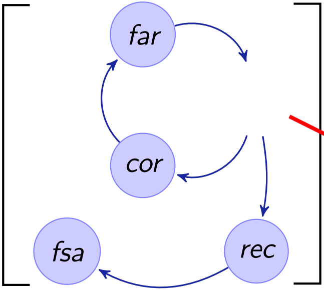
differential dynamic logic

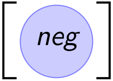
$d\mathcal{L} = FOL_{\mathbb{R}} + DL + HP$



differential dynamic logic

$d\mathcal{L} = \text{FOL}_{\mathbb{R}} + \text{DL} + \text{HP}$





$v^2 \leq 2b\,..$

Not Compositional

Differential Dynamic Logic d$\mathcal{L}$: Syntax

Definition (Hybrid program α)

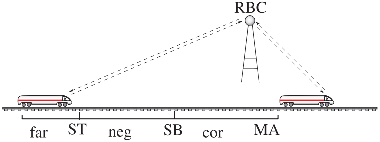
$x' = f(x)$	(continuous evolution)	
$x := f(x)$	(discrete jump)	jump & test
$?H$	(conditional execution)	
$\alpha; \beta$	(seq. composition)	Kleene algebra
$\alpha \cup \beta$	(nondet. choice)	
α^*	(nondet. repetition)	

Differential Dynamic Logic d$\mathcal{L}$: Syntax

Definition (Hybrid program α)

$x' = f(x)$	(continuous evolution)	
$x := f(x)$	(discrete jump)	jump & test
$?H$	(conditional execution)	
$\alpha; \beta$	(seq. composition)	Kleene algebra
$\alpha \cup \beta$	(nondet. choice)	
α^*	(nondet. repetition)	

$$
\begin{aligned}
ETCS &\equiv (ctrl; drive)^* \\
ctrl &\equiv (?MA - z \leq SB; a := -b) \\
&\quad \cup (?MA - z \geq SB; a := \ldots) \\
drive &\equiv \quad z'' = a \\
&\quad \& \, v \geq 0 \wedge \tau \leq \varepsilon
\end{aligned}
$$

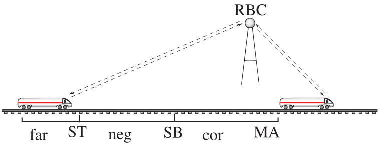


Differential Dynamic Logic d$\mathcal{L}$: Syntax

Definition (Hybrid program α)

$x' = f(x)$	(continuous evolution)	
$x := f(x)$	(discrete jump)	jump & test
$?H$	(conditional execution)	
$\alpha; \beta$	(seq. composition)	Kleene algebra
$\alpha \cup \beta$	(nondet. choice)	
α^*	(nondet. repetition)	

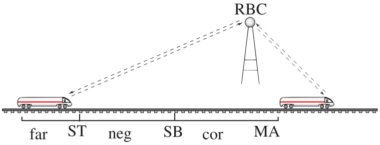
$$
\begin{aligned}
ETCS &\equiv (ctrl; drive)^* \\
ctrl &\equiv (?MA - z \le SB; a := -b) \\
&\quad \cup (?MA - z \ge SB; a := \ldots) \\
drive &\equiv \tau := 0; z' = v, v' = a, \tau' = 1 \\
&\quad \& \; v \ge 0 \land \tau \le \varepsilon
\end{aligned}
$$



Definition (Hybrid program α)

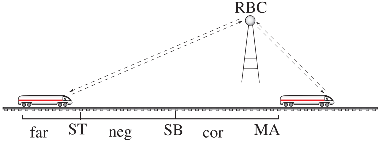
$x' = f(x) \,\&\, H$	(continuous evolution)	
$x := f(x)$	(discrete jump)	jump & test
$?H$	(conditional execution)	
$\alpha; \beta$	(seq. composition)	Kleene algebra
$\alpha \cup \beta$	(nondet. choice)	
α^*	(nondet. repetition)	

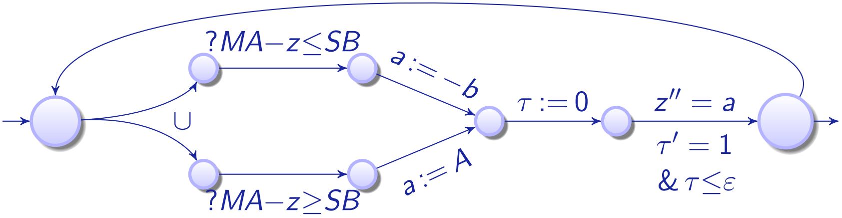
$$
\begin{aligned}
ETCS &\equiv (ctrl; drive)^* \\
ctrl &\equiv (?MA - z \le SB; a := -b) \\
&\quad \cup (?MA - z \ge SB; a := \dots) \\
drive &\equiv \tau := 0; z' = v, v' = a, \tau' = 1 \\
&\quad \& \, v \ge 0 \land \tau \le \varepsilon
\end{aligned}
$$



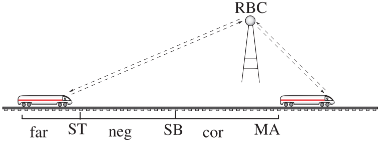
Branching Transitions in Hybrid Programs

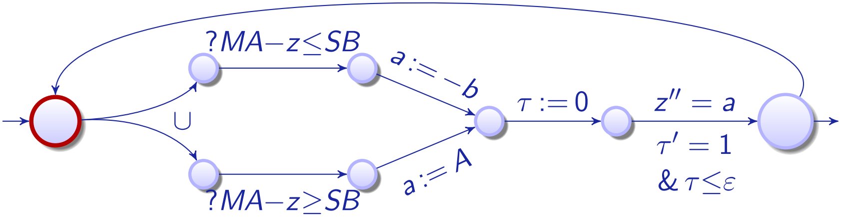
$$ETCS \equiv (ctrl\,; drive)^*$$
$$ctrl \equiv (?MA - z \leq SB; a := -b)$$
$$\cup\, (?MA - z \geq SB; a := A)$$
$$drive \equiv \tau := 0; z' = v, v' = a, \tau' = 1$$
$$\&\, v \geq 0 \land \tau \leq \varepsilon$$



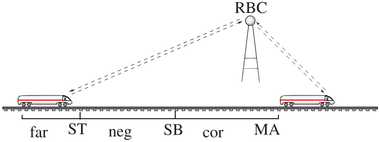


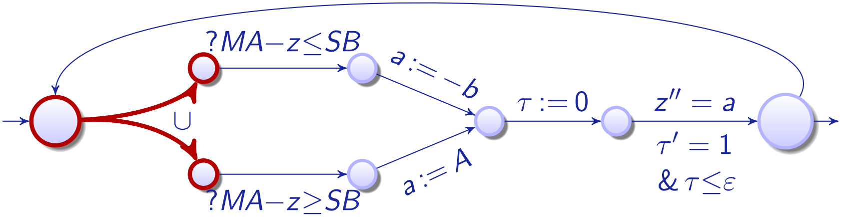
$$
\begin{aligned}
ETCS &\equiv (ctrl\,;drive)^*\\
ctrl &\equiv (?MA - z \le SB;\, a := -b)\\
&\quad \cup (?MA - z \ge SB;\, a := A)\\
drive &\equiv \tau := 0;\, z' = v,\, v' = a,\, \tau' = 1\\
&\quad \&\, v \ge 0 \land \tau \le \varepsilon
\end{aligned}
$$





$$ETCS \equiv (ctrl\,;drive)^*$$
$$ctrl \equiv (?MA - z \leq SB; a := -b)$$
$$\cup\,(?MA - z \geq SB; a := A)$$
$$drive \equiv \tau := 0; z' = v, v' = a, \tau' = 1$$
$$\&\, v \geq 0 \land \tau \leq \varepsilon$$





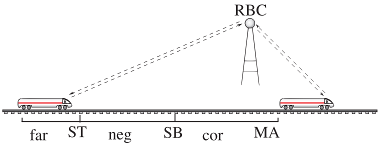
$$ETCS \equiv (ctrl\,;drive)^*$$

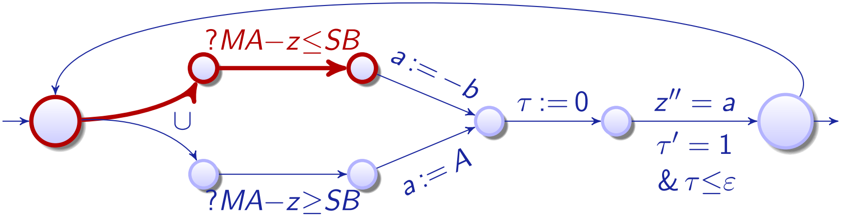
$$ctrl \equiv (?MA - z \leq SB; a := -b)$$

$$\cup\ (?MA - z \geq SB; a := A)$$

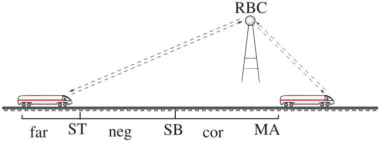
$$drive \equiv \tau := 0; z' = v, v' = a, \tau' = 1$$

$$\&\ v \geq 0 \land \tau \leq \varepsilon$$

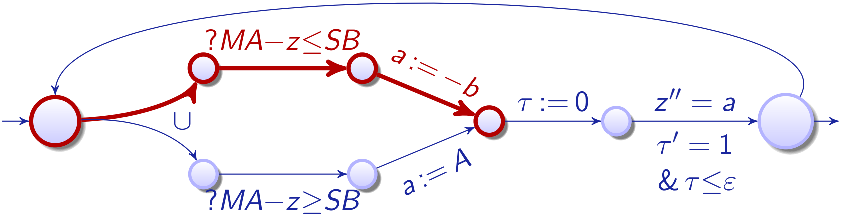




$$ETCS \equiv (ctrl\,;drive)^*$$
$$ctrl \equiv (?MA - z \leq SB; a := -b)$$
$$\cup\,(?MA - z \geq SB; a := A)$$
$$drive \equiv \tau := 0; z' = v, v' = a, \tau' = 1$$
$$\&\, v \geq 0 \land \tau \leq \varepsilon$$

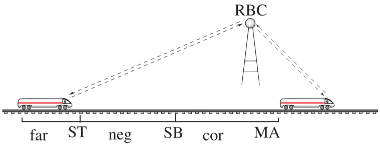


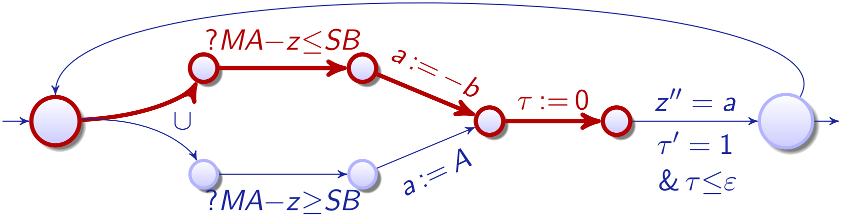
Branching Transitions in Hybrid Programs



$$ETCS \equiv (ctrl\,; drive)^*$$

$$ctrl \equiv (?MA - z \leq SB; a := -b)$$
$$\cup\,(?MA - z \geq SB; a := A)$$
$$drive \equiv \tau := 0; z' = v, v' = a, \tau' = 1$$
$$\&\, v \geq 0 \land \tau \leq \varepsilon$$





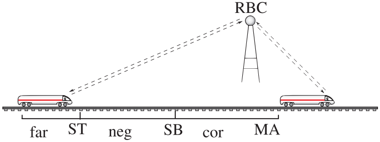
$$ETCS \equiv (ctrl\,;drive)^*$$

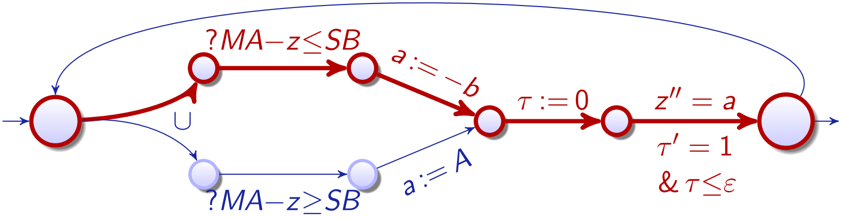
$$ctrl \equiv (?MA - z \leq SB; a := -b)$$

$$\cup\,(?MA - z \geq SB; a := A)$$

$$drive \equiv \tau := 0; z' = v, v' = a, \tau' = 1$$

$$\&\, v \geq 0 \land \tau \leq \varepsilon$$





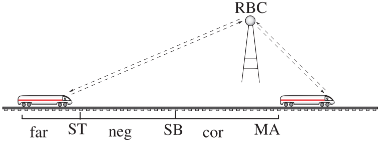
$$ETCS \equiv (ctrl\,;\, drive)^*$$

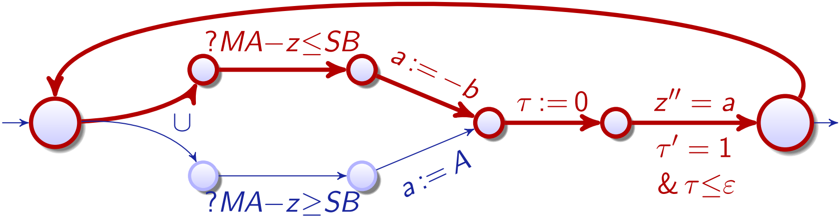
$$ctrl \equiv (?MA - z \leq SB;\, a := -b)$$

$$\cup\, (?MA - z \geq SB;\, a := A)$$

$$drive \equiv \tau := 0;\, z' = v, v' = a, \tau' = 1$$

$$\&\, v \geq 0 \land \tau \leq \varepsilon$$





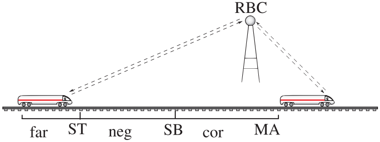
$$ETCS \equiv (ctrl\,;drive)^*$$

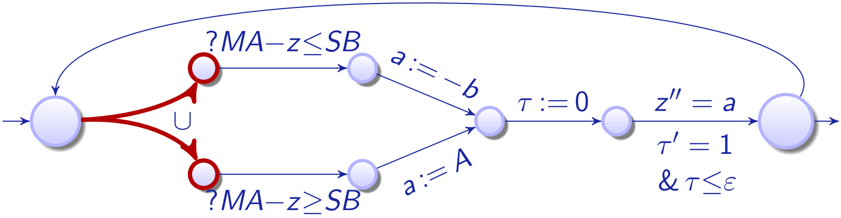
$$ctrl \equiv (?MA - z \leq SB; a := -b)$$

$$\cup\, (?MA - z \geq SB; a := A)$$

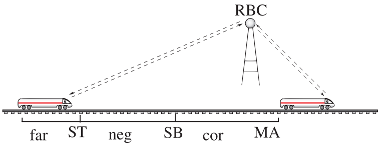
$$drive \equiv \tau := 0; z' = v, v' = a, \tau' = 1$$

$$\&\, v \geq 0 \land \tau \leq \varepsilon$$

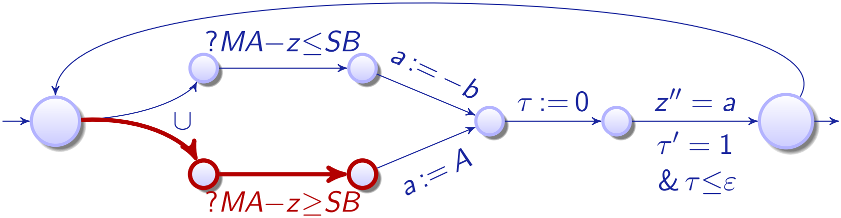




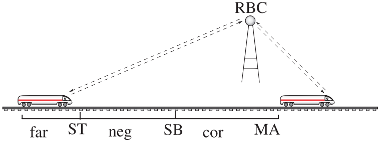
$$ETCS \equiv (ctrl\,; drive)^*$$
$$ctrl \equiv (?MA - z \leq SB; a := -b)$$
$$\cup\, (?MA - z \geq SB; a := A)$$
$$drive \equiv \tau := 0; z' = v, v' = a, \tau' = 1$$
$$\&\, v \geq 0 \land \tau \leq \varepsilon$$

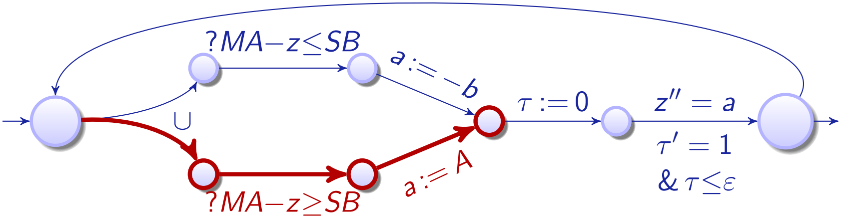


Branching Transitions in Hybrid Programs



$$ETCS \equiv (ctrl\,;drive)^*$$
$$ctrl \equiv (?MA - z \leq SB; a := -b)$$
$$\cup\, (?MA - z \geq SB; a := A)$$
$$drive \equiv \tau := 0; z' = v, v' = a, \tau' = 1$$
$$\&\, v \geq 0 \land \tau \leq \varepsilon$$





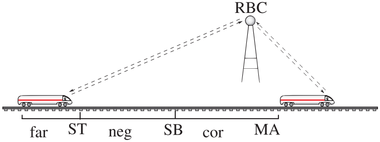
$ETCS \equiv (ctrl\,; drive)^*$

$ctrl \equiv (?MA - z \leq SB; a := -b)$

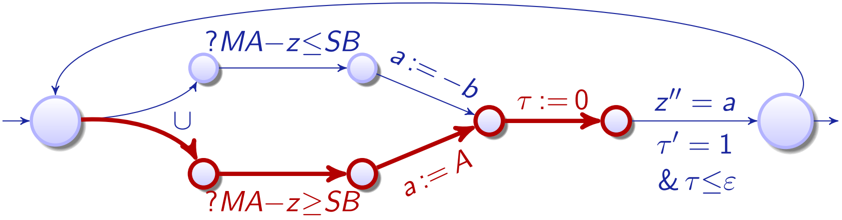
$\cup\,(?MA - z \geq SB; a := A)$

$drive \equiv \tau := 0; z' = v, v' = a, \tau' = 1$

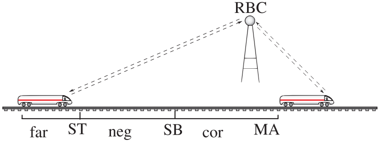
$\&\, v \geq 0 \wedge \tau \leq \varepsilon$



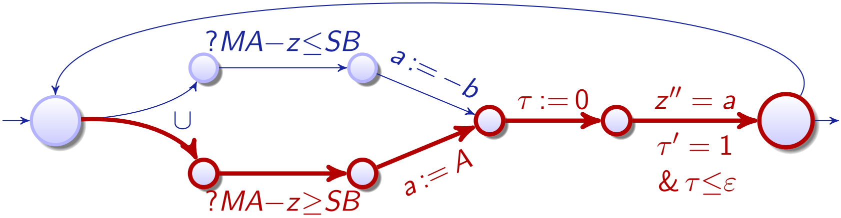
Branching Transitions in Hybrid Programs



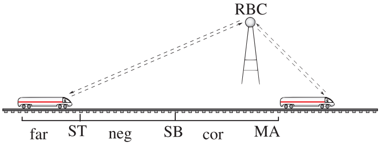
$$ETCS \equiv (ctrl\,;\,drive)^*$$
$$ctrl \equiv (?MA - z \leq SB;\, a := -b)$$
$$\cup\, (?MA - z \geq SB;\, a := A)$$
$$drive \equiv \tau := 0;\, z' = v,\, v' = a,\, \tau' = 1$$
$$\&\, v \geq 0 \land \tau \leq \varepsilon$$

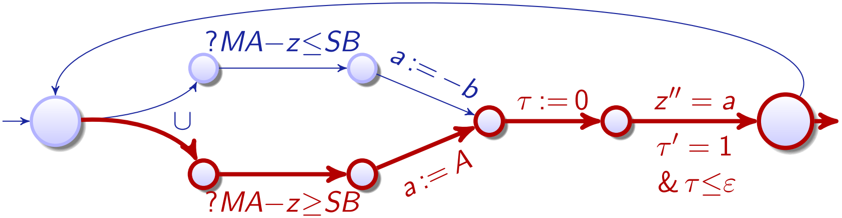


Branching Transitions in Hybrid Programs

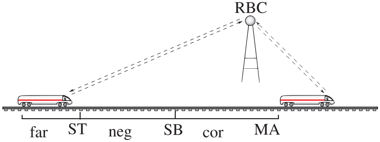


$$ETCS \equiv (ctrl\,;\, drive)^*$$
$$ctrl \equiv (?MA - z \leq SB;\, a := -b)$$
$$\cup\, (?MA - z \geq SB;\, a := A)$$
$$drive \equiv \tau := 0;\, z' = v,\, v' = a,\, \tau' = 1$$
$$\&\, v \geq 0 \land \tau \leq \varepsilon$$

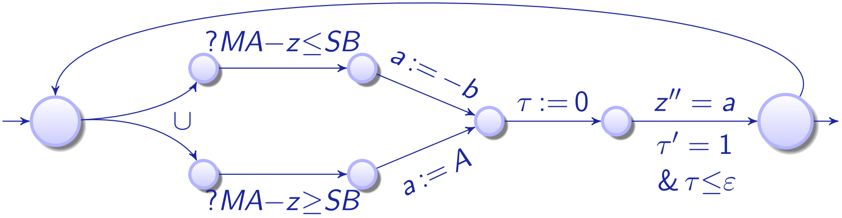




$$ETCS \equiv (ctrl\,;drive)^*$$
$$ctrl \equiv (?MA - z \le SB; a := -b)$$
$$\cup\,(?MA - z \ge SB; a := A)$$
$$drive \equiv \tau := 0; z' = v, v' = a, \tau' = 1$$
$$\&\, v \ge 0 \land \tau \le \varepsilon$$



Branching Transitions in Hybrid Programs



$$\texttt{if}(H)\,\alpha\,\texttt{else}\,\beta \equiv$$

$$\texttt{while}(H)\,\alpha \equiv$$

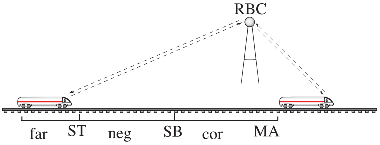
$$ETCS \equiv (ctrl\,;drive)^*$$

$$ctrl \equiv (?MA - z \leq SB; a := -b)$$

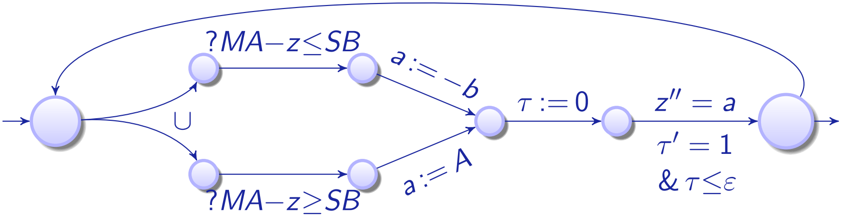
$$\cup\,(?MA - z \geq SB; a := A)$$

$$drive \equiv \tau := 0; z' = v, v' = a, \tau' = 1$$

$$\&\, v \geq 0 \land \tau \leq \varepsilon$$



Branching Transitions in Hybrid Programs



$$\texttt{if}(H)\,\alpha\,\texttt{else}\,\beta \equiv (?H;\alpha) \cup (?\neg H;\beta)$$

$$\texttt{while}(H)\,\alpha \equiv$$

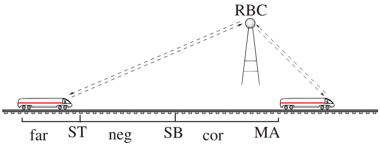
$$ETCS \equiv (ctrl\,;drive)^*$$

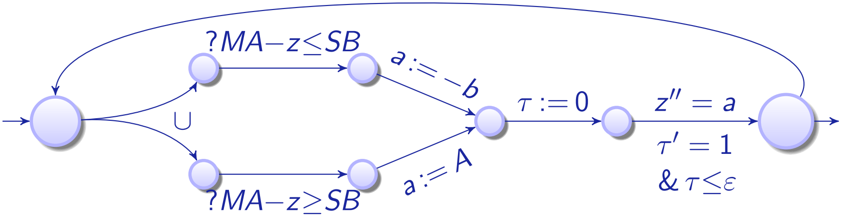
$$ctrl \equiv (?MA - z \leq SB; a := -b)$$

$$\cup\,(?MA - z \geq SB; a := A)$$

$$drive \equiv \tau := 0; z' = v, v' = a, \tau' = 1$$

$$\&\, v \geq 0 \land \tau \leq \varepsilon$$





$$\texttt{if}(H)\,\alpha\,\texttt{else}\,\beta \equiv (?H;\alpha)\cup(?\neg H;\beta)$$

$$\texttt{while}(H)\,\alpha \equiv (?H;\alpha)^*;\,?\neg H$$

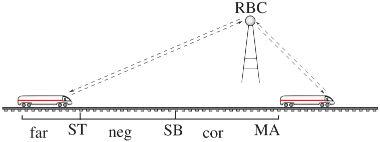
$$ETCS \equiv (ctrl\,;drive)^*$$

$$ctrl \equiv (?MA - z \leq SB;\, a := -b)$$

$$\cup\,(?MA - z \geq SB;\, a := A)$$

$$drive \equiv \tau := 0;\, z' = v,\, v' = a,\, \tau' = 1$$

$$\&\, v \geq 0 \land \tau \leq \varepsilon$$



Differential Dynamic Logic d$\mathcal{L}$: Syntax

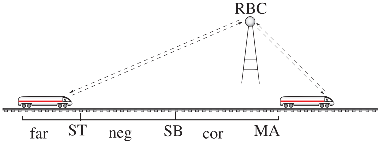
Definition (d$\mathcal{L}$ Formula ϕ)

$$\theta_1 \geq \theta_2 \mid \neg\phi \mid \phi \wedge \psi \mid \phi \vee \psi \mid \phi \rightarrow \psi \mid \forall x\, \phi \mid \exists x\, \phi \mid [\alpha]\phi \mid \langle\alpha\rangle\phi$$

with terms θ_1, θ_2 of nonlinear real arithmetic $(+, \cdot)$

$$SB \geq \ldots \;\rightarrow\; [(ctrl; drive)^*]\, z \leq MA$$

All trains respect MA
RBC partitions MA
$\Rightarrow$ system collision free



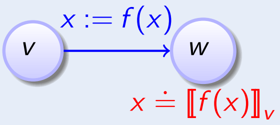
Definition (Hybrid program α)

$$\begin{aligned}
\rho(x := \theta) &= \{(v,w) \;:\; w = v \text{ except } [\![x]\!]_w = [\![\theta]\!]_v\} \\
\rho(?H) &= \{(v,v) \;:\; v \models H\} \\
\rho(x' = f(x)) &= \{(\varphi(0),\varphi(r)) \;:\; \varphi \models x' = f(x) \text{ for some duration } r\} \\
\rho(\alpha \cup \beta) &= \rho(\alpha) \cup \rho(\beta) \\
\rho(\alpha;\beta) &= \rho(\beta) \circ \rho(\alpha) \\
\rho(\alpha^*) &= \bigcup_{n \in \mathbb{N}} \rho(\alpha^n)
\end{aligned}$$

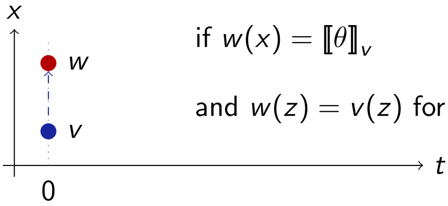
Definition (d$\mathcal{L}$ Formula ϕ)

$$\begin{aligned}
v &\models \theta_1 \geq \theta_2 && \text{iff} \quad [\![\theta_1]\!]_v \geq [\![\theta_2]\!]_v \\
v &\models [\alpha]\phi && \text{iff} \quad w \models \phi \text{ for all } w \text{ with } (v,w) \in \rho(\alpha) \\
v &\models \langle\alpha\rangle\phi && \text{iff} \quad w \models \phi \text{ for some } w \text{ with } (v,w) \in \rho(\alpha) \\
v &\models \forall x\,\phi && \text{iff} \quad w \models \phi \text{ for all } w \text{ that agree with } v \text{ except for } x \\
v &\models \exists x\,\phi && \text{iff} \quad w \models \phi \text{ for some } w \text{ that agrees with } v \text{ except for } x \\
v &\models \phi \wedge \psi && \text{iff} \quad v \models \phi \text{ and } v \models \psi
\end{aligned}$$

Definition (Hybrid programs α: transition semantics)



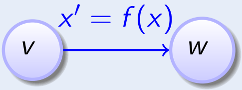
Example



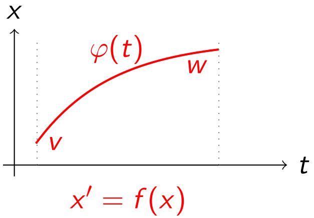
if $w(x) = [\![\theta]\!]_v$

and $w(z) = v(z)$ for $z \neq x$

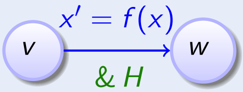
Definition (Hybrid programs α: transition semantics)



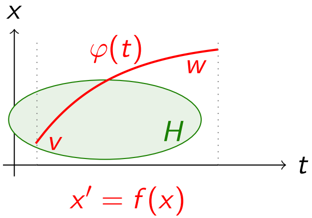
Example



Definition (Hybrid programs α: transition semantics)

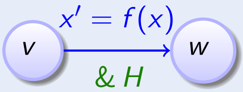


Example

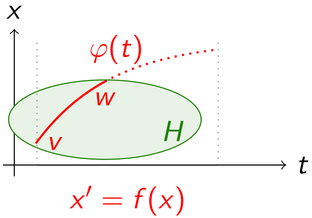


Differential Dynamic Logic d$\mathcal{L}$: Transition Semantics

Definition (Hybrid programs α: transition semantics)

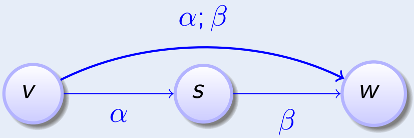


Example



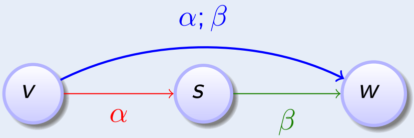
Differential Dynamic Logic d$\mathcal{L}$: Transition Semantics

Definition (Hybrid programs α: transition semantics)

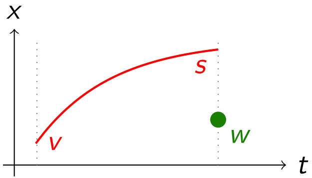


Example

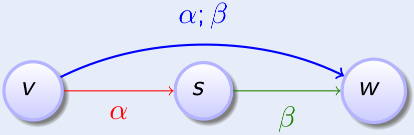
Definition (Hybrid programs α: transition semantics)



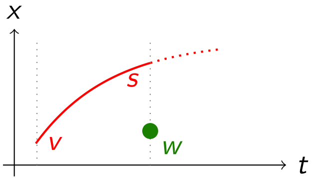
Example



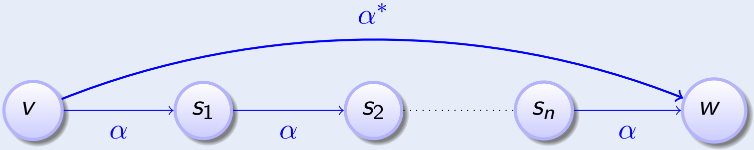
Definition (Hybrid programs α: transition semantics)



Example



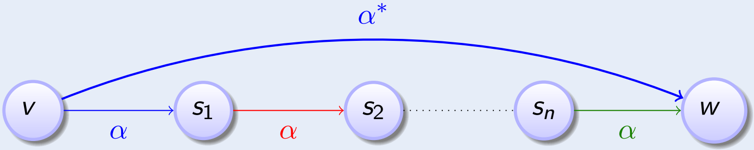
Definition (Hybrid programs α: transition semantics)



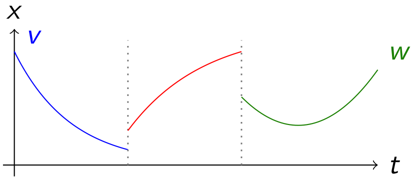
Example

Differential Dynamic Logic d$\mathcal{L}$: Transition Semantics

Definition (Hybrid programs α: transition semantics)

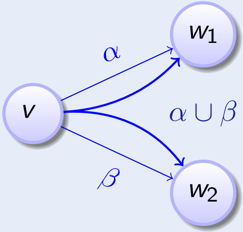


Example



Differential Dynamic Logic d$\mathcal{L}$: Transition Semantics

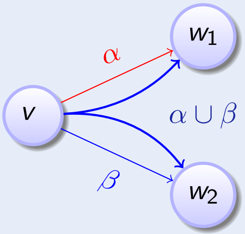
Definition (Hybrid programs α: transition semantics)



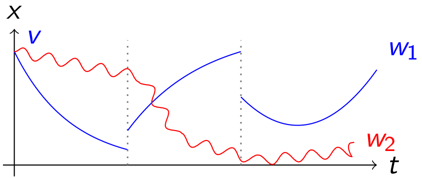
Example

Differential Dynamic Logic d$\mathcal{L}$: Transition Semantics

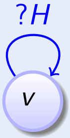
Definition (Hybrid programs α: transition semantics)



Example

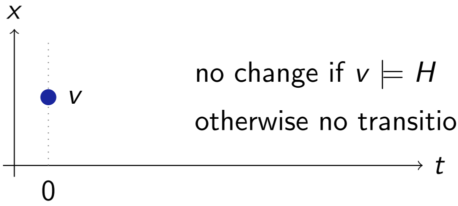


Definition (Hybrid programs α: transition semantics)



if $v \models H$

Example



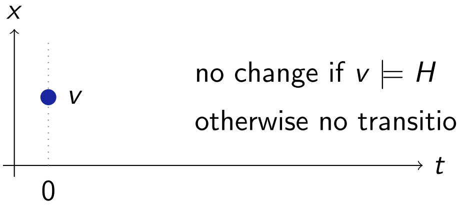
no change if $v \models H$

otherwise no transition

Definition (Hybrid programs α: transition semantics)

if $v \not\models H$

Example

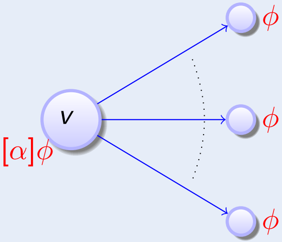


no change if $v \models H$

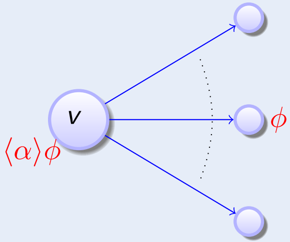
otherwise no transition

Differential Dynamic Logic d$\mathcal{L}$: Semantics

Definition (Formulas ϕ)

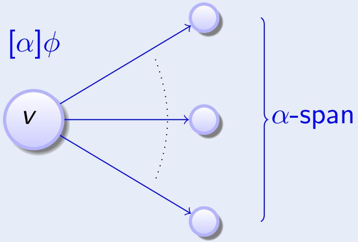


Definition (Formulas ϕ)



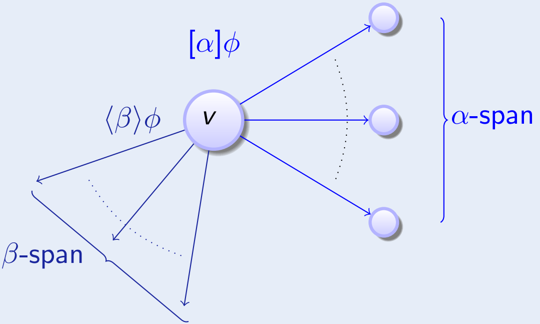
Differential Dynamic Logic d$\mathcal{L}$: Semantics

Definition (Formulas ϕ)

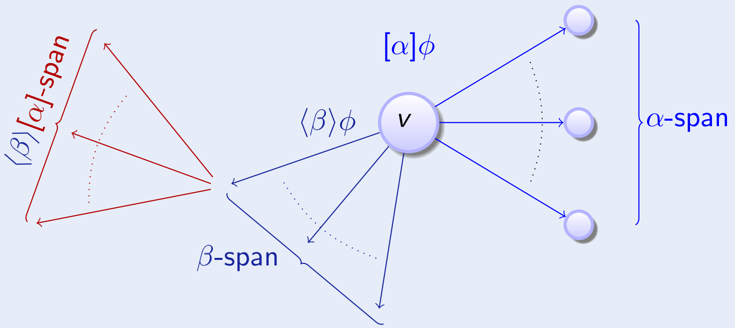


Differential Dynamic Logic d$\mathcal{L}$: Semantics

Definition (Formulas ϕ)

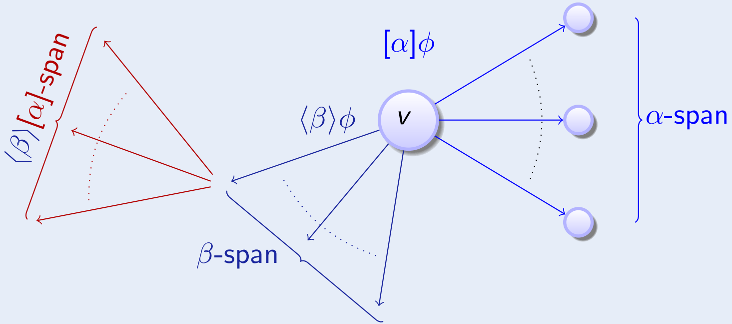


Definition (Formulas ϕ)



Differential Dynamic Logic d$\mathcal{L}$: Semantics

Definition (Formulas ϕ)

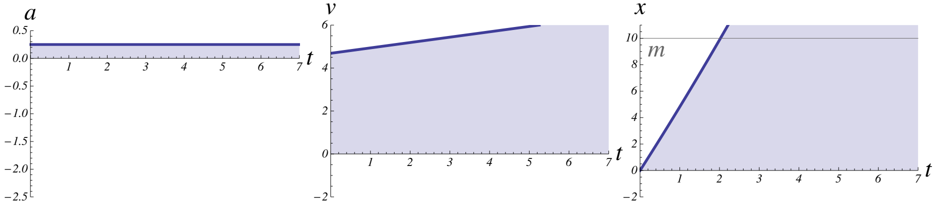


compositional semantics $\Rightarrow$ compositional proofs!

Ex: Car Control

Example (Single car car_s)

$$x' = v, v' = a$$

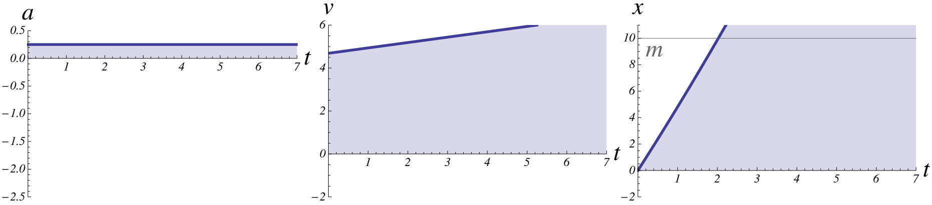


Ex: Car Control

Control decision: accelerate or brake

Example (Single car car_s)

$$(a := A \cup a := -b);\ x' = v, v' = a$$

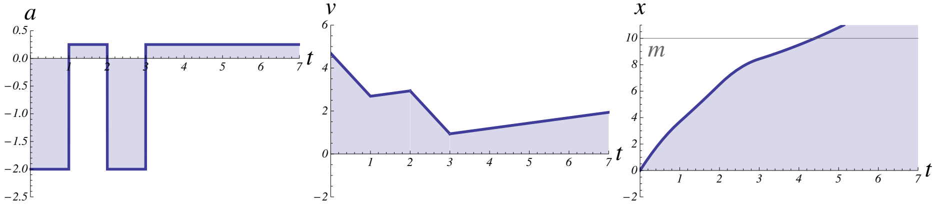


Ex: Car Control

Repeat control decisions

Example (Single car car_s)

$$\big((a := A \cup a := -b);\ x' = v, v' = a\big)^*$$

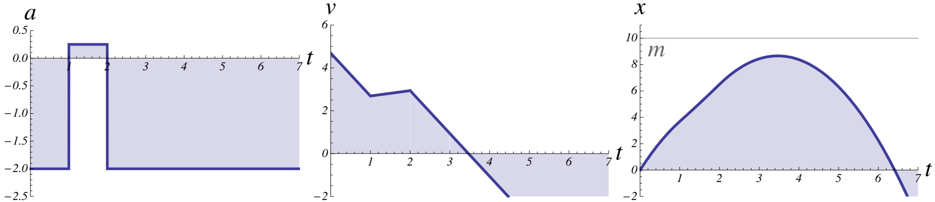


Ex: Car Control

Repeat control decisions

Example (Single car car_s)

$$\left(\left(a := A \cup a := -b\right);\ x' = v, v' = a\right)^*$$

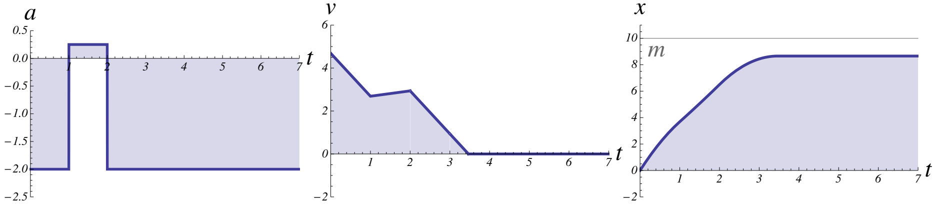


Ex: Car Control

Velocity bound $v \geq 0$

Example (Single car car_s)

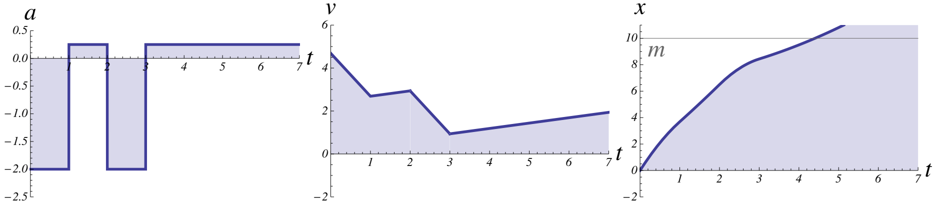
$$\left(\left(\, a := A \;\cup a := -b\right);\; x' = v, v' = a \,\&\, v \geq 0\right)^*$$



Accelerate not always safe

Example (Single car car_s)

$$\left(\left(a := A \;\cup a := -b\right);\; x' = v, v' = a \,\&\, v \geq 0\right)^*$$

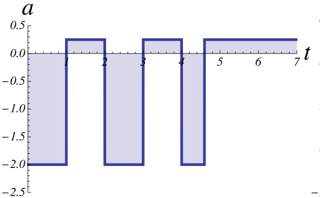


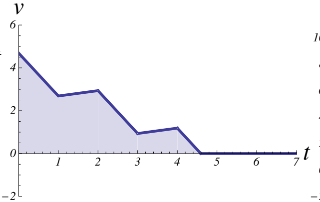
Ex: Car Control

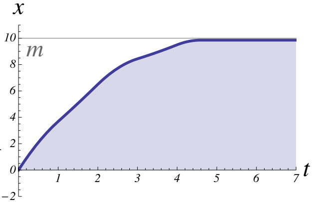
Accelerate condition $?H$

Example (Single car car_s)

$$(((?H;\, a := A) \cup a := -b);\ x' = v, v' = a \,\&\, v \geq 0)^*$$





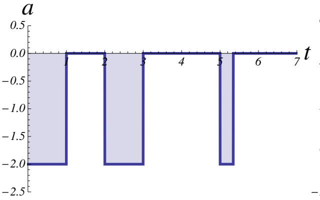


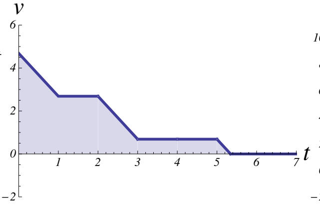
Ex: Car Control

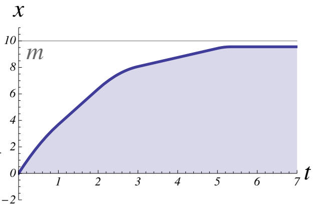
Accelerate condition $?H$ depends on A

Example (Single car car_s)

$$\left(\left((?H;\, a := 0) \cup a := -b\right);\ x' = v, v' = a \,\&\, v \geq 0\right)^*$$







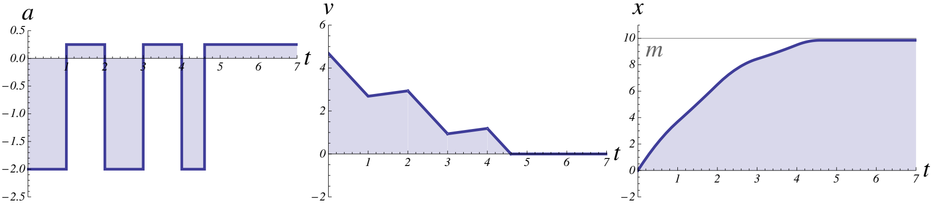
Example (Single car car_e)

$$\big(((?H;\, a := A) \cup a := -b);\;\; x' = v, v' = a \,\&\, v \geq 0\big)^*$$

Accelerate condition tests proximity to m

Example (Single car car_e)

$$(((?m-x \geq 2; a := A) \cup a := -b);\ x' = v, v' = a \,\&\, v \geq 0)^*$$

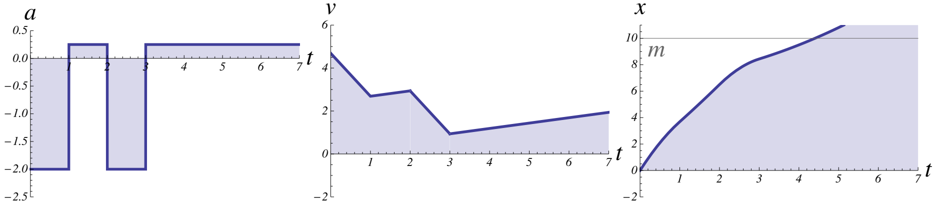


Ex: Car Control & Sensors — event-triggered

Miss event $m - x \leq 2 \Rightarrow$ crash

Example (Single car car_e)

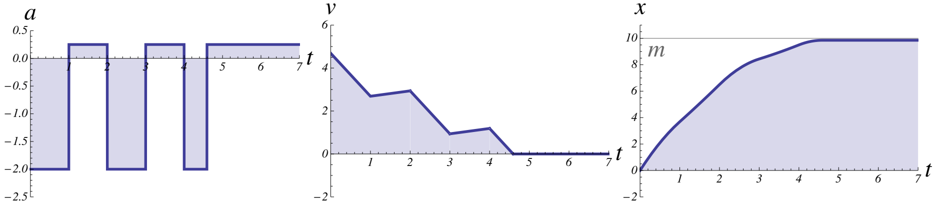
$$\big(((?m-x \geq 2;\, a := A) \cup a := -b);\ x' = v, v' = a \,\&\, v \geq 0\big)^*$$



Guard for event $1 \leq m - x \leq 2$

Example (Single car car_e event-triggered)

$$\Big(\big((?m-x \geq 2;\, a := A) \cup a := -b\big);\;\; x' = v, v' = a \,\&\, v \geq 0 \wedge m-x \geq 1\Big)^*$$

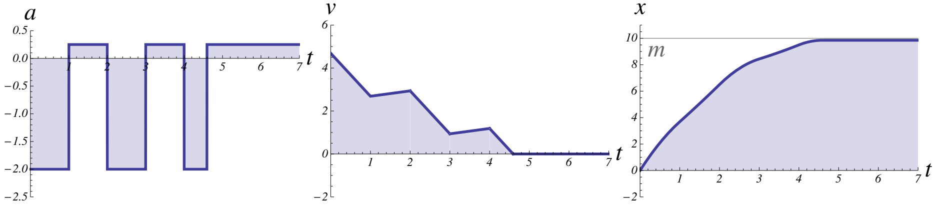


Ex: Car Control & Sensors — event-triggered

Guard for event $1 \leq m - x \leq 2$ hard to implement

Example (Single car car_e event-triggered)

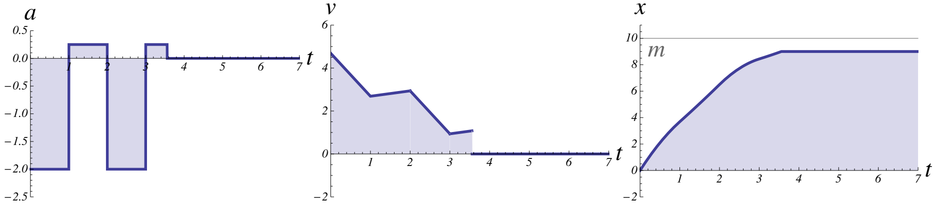
$$\left(\left(\left(?m-x \geq 2;\, a := A\right) \cup a := -b\right);\;\; x' = v, v' = a \,\&\, v \geq 0 \wedge m-x \geq 1\right)^*$$



Careful with evolution domains!

Example (Single car car_e event-triggered)

$$\big(((?m - x \geq 2;\ a := A) \cup a := -b);\ x' = v, v' = a \,\&\, v \geq 0 \land m - x \geq 1\big)^*$$



Example (Single car car_ε)

$$\big(((?H;\, a := A) \cup a := -b);\ x' = v, v' = a \,\&\, v \geq 0\big)^*$$

Ex: Car Control & Sensors

Example (Single car car_ε time-triggered)

$$\left(((?H; a := A) \cup a := -b);\ x' = v, v' = a \,\&\, v \geq 0 \wedge t \leq \varepsilon\right)^*$$

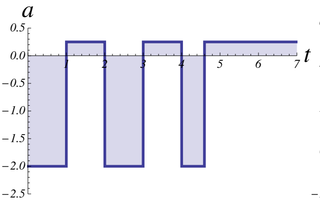
Example (Single car car_ε time-triggered)

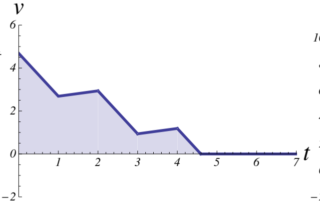
$$\left(((?H; a := A) \cup a := -b);\ x' = v, v' = a, t' = 1 \,\&\, v \geq 0 \land t \leq \varepsilon\right)^*$$

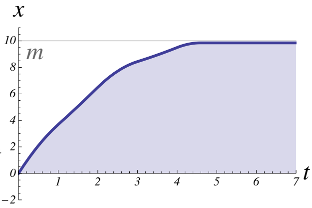
Trigger control every $\leq \varepsilon$ time units

Example (Single car car_ε time-triggered)

$$\big(((?H;\, a := A) \cup a := -b);\ t := 0;\ x' = v, v' = a, t' = 1 \,\&\, v \geq 0 \land t \leq \varepsilon\big)^*$$



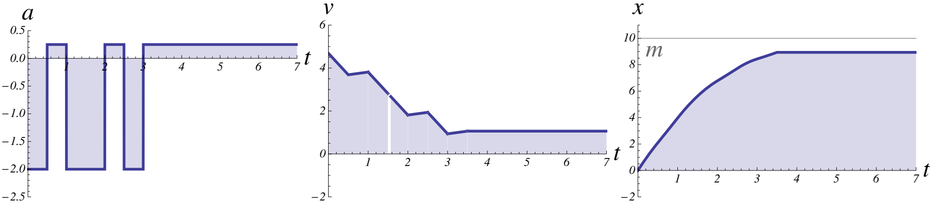




Really faster $\Rightarrow$ inefficient

Example (Single car car_ε time-triggered)

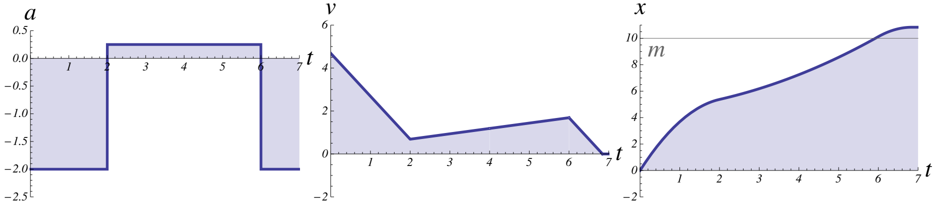
$$\left(\left(\left(?H; a := A\right) \cup a := -b\right);\ t := 0;\ x' = v, v' = a, t' = 1 \,\&\, v \geq 0 \land t \leq \varepsilon\right)^*$$



Really slower $\Rightarrow$ crash

Example (Single car car_ε time-triggered)

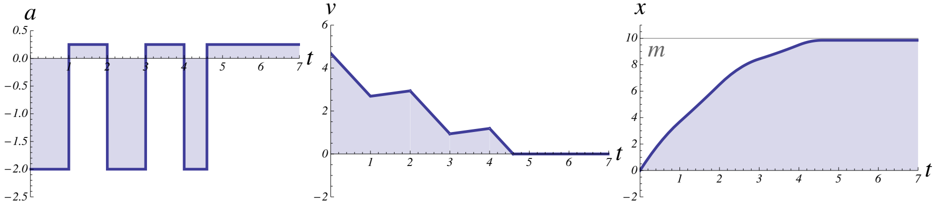
$$(((?H; a := A) \cup a := -b);\ t := 0;\ x' = v, v' = a, t' = 1 \,\&\, v \geq 0 \wedge t \leq \varepsilon)^*$$



Accelerate condition ?H depends on . . .

Example (Single car car_ε time-triggered)

$$(((?H;\, a := A) \cup a := -b);\ \ t := 0;\ \ x' = v, v' = a, t' = 1 \,\&\, v \geq 0 \wedge t \leq \varepsilon)^*$$

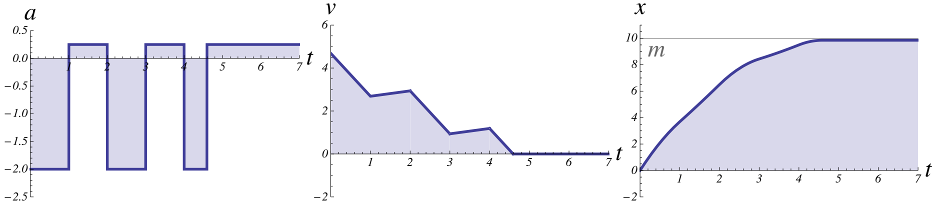


Accelerate condition $?H$ depends on …

$$H \equiv 2b(m-x) \geq v^2 + (A+b)(A\varepsilon^2 + 2\varepsilon v)$$

Example (Single car car_ε time-triggered)

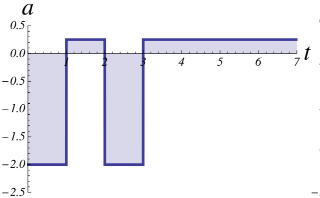
$$(((?H; a := A) \cup a := -b);\ t := 0;\ x' = v, v' = a, t' = 1 \,\&\, v \geq 0 \land t \leq \varepsilon)^*$$

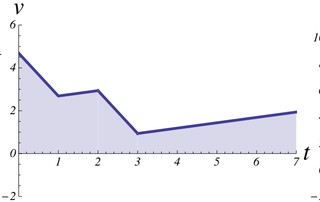


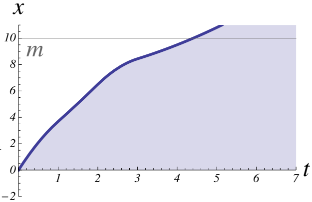
Ex: Car Control Properties

Example (Single car car_s)

$$\left(((?m{-}x \geq 2; a := A) \cup a := -b);\ x' = v, v' = a \,\&\, v \geq 0\right)^*$$





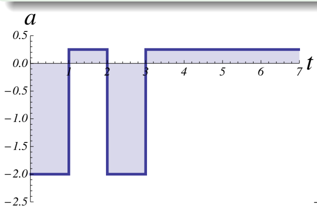


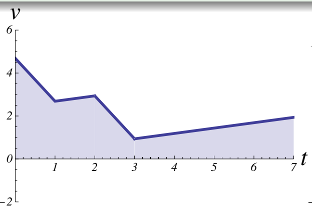
Ex: Car Control Properties

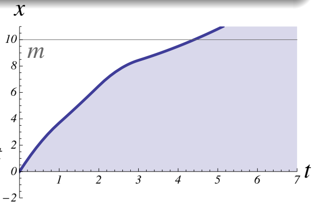
Example (Single car car_s)

$$(((?m - x \geq 2; a := A) \cup a := -b);\ x' = v, v' = a \,\&\, v \geq 0)^*$$

Example (Drives forward)







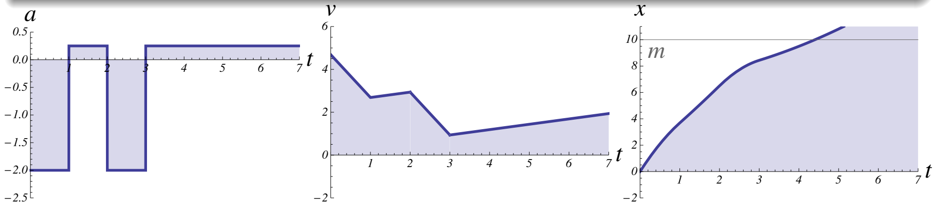
Ex: Car Control Properties

Example (Single car car_s)

$$(((?m - x \geq 2; a := A) \cup a := -b);\ x' = v, v' = a \,\&\, v \geq 0)^*$$

Example (Drives forward)

$$v \geq 0 \land A \geq 0 \land b > 0 \rightarrow [car_s]v \geq 0$$



Ex: Car Control Properties

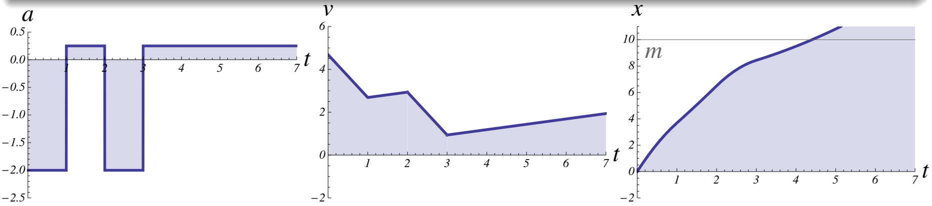
True initially, preserved by definition

Example (Single car car_s)

$$(((?m - x \geq 2; a := A) \cup a := -b);\; x' = v, v' = a \,\&\, v \geq 0)^*$$

Example (Drives forward)

$$v \geq 0 \land A \geq 0 \land b > 0 \rightarrow [car_s] v \geq 0$$

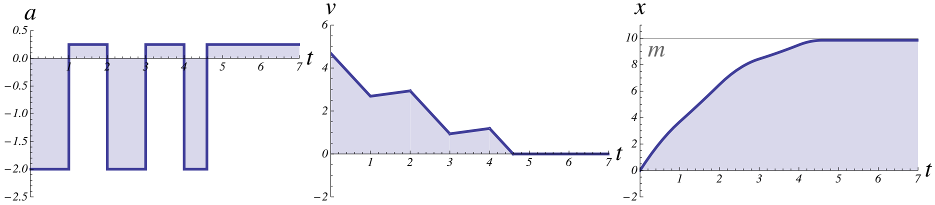


Ex: Car Control Properties

$$H \equiv 2b(m - x) \geq v^2 + (A + b)(A\varepsilon^2 + 2\varepsilon v)$$

Example (Single car car_ε event-triggered)

$$(((?H; a := A) \cup a := -b);\ t := 0;\ x' = v, v' = a, t' = 1 \,\&\, v \geq 0 \wedge t \leq \varepsilon)^*$$



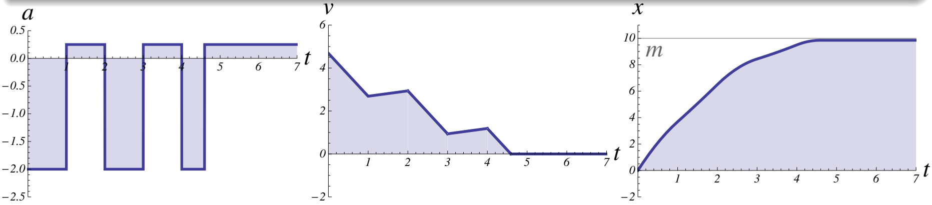
Ex: Car Control Properties time-triggered

$H \equiv 2b(m-x) \geq v^2 + (A+b)(A\varepsilon^2 + 2\varepsilon v)$

Example (Single car car_ε event-triggered)

$$(((?H; a := A) \cup a := -b);\ t := 0;\ x' = v, v' = a, t' = 1 \,\&\, v \geq 0 \wedge t \leq \varepsilon)^*$$

Example (Stays before traffic light m)



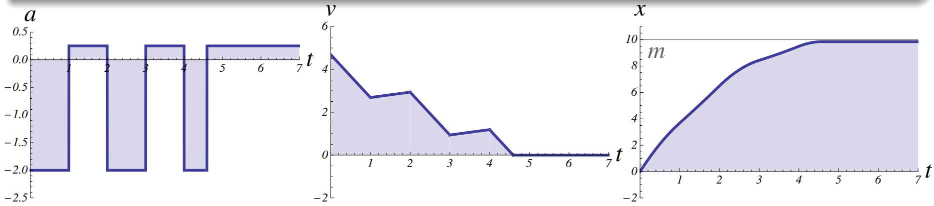
$$H \equiv 2b(m-x) \geq v^2 + (A+b)(A\varepsilon^2 + 2\varepsilon v)$$

Example (Single car car_ε event-triggered)

$$(((?H; a := A) \cup a := -b);\ t := 0;\ x' = v, v' = a, t' = 1 \,\&\, v \geq 0 \wedge t \leq \varepsilon)^*$$

Example (Stays before traffic light m)

$$v^2 \leq 2b(m-x) \wedge A \geq 0 \wedge b > 0 \rightarrow [car_\varepsilon]x \leq m$$



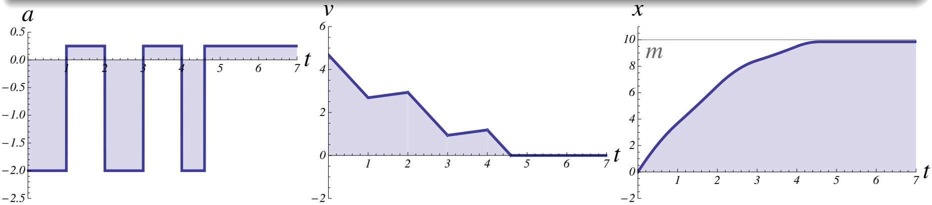
Ex: Car Control Properties — time-triggered

$H \equiv 2b(m - x) \geq v^2 + (A + b)(A\varepsilon^2 + 2\varepsilon v)$

Example (Single car car_ε event-triggered)

$(((?H; a := A) \cup a := -b);\ t := 0;\ x' = v, v' = a, t' = 1 \,\&\, v \geq 0 \wedge t \leq \varepsilon)^*$

Example (Live, can move everywhere)



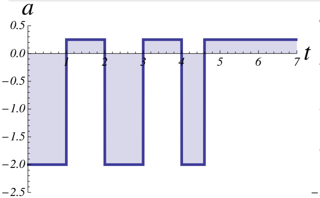
$$H \equiv 2b(m-x) \geq v^2 + (A+b)(A\varepsilon^2 + 2\varepsilon v)$$

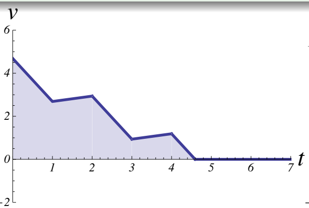
Example (Single car car_ε event-triggered)

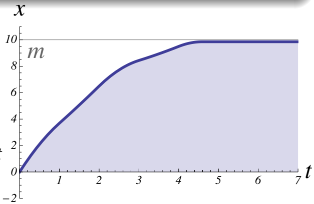
$$(((?H; a := A) \cup a := -b);\ t := 0;\ x' = v, v' = a, t' = 1 \,\&\, v \geq 0 \wedge t \leq \varepsilon)^*$$

Example (Live, can move everywhere)

$$\varepsilon > 0 \wedge A > 0 \wedge b > 0 \rightarrow \forall p\, \exists m\, \langle car_\varepsilon \rangle\, x \geq p$$







Ex: Car Control Properties — time-triggered

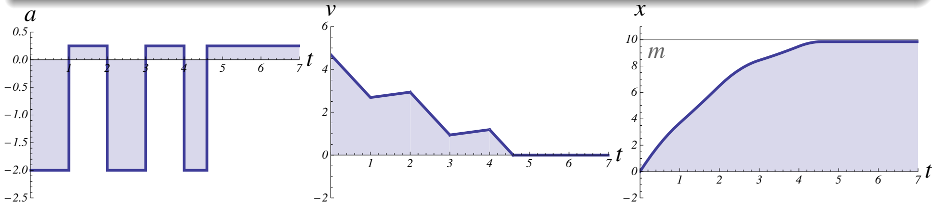
$$H \equiv 2b(m - x) \geq v^2 + (A + b)(A\varepsilon^2 + 2\varepsilon v)$$

Example (Single car car_ε event-triggered)

$$(((?H; a := A) \cup a := -b);\ t := 0;\ x' = v, v' = a, t' = 1 \,\&\, v \geq 0 \wedge t \leq \varepsilon)^*$$

Example (Stays before traffic light m)

$$v^2 \leq 2b(m - x) \wedge A \geq 0 \wedge b > 0 \rightarrow [car_\varepsilon]x \leq m$$



Ex: Car Control Properties   time-triggered

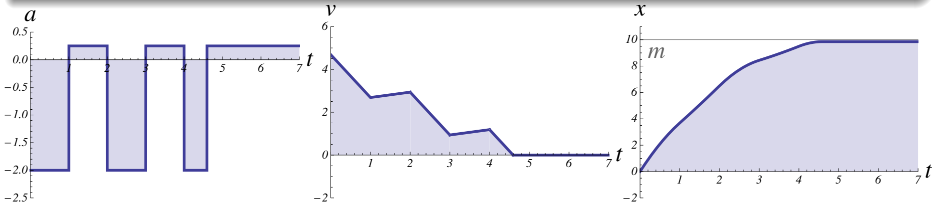
$H \equiv 2b(m - x) \geq v^2 + (A + b)(A\varepsilon^2 + 2\varepsilon v)$

Example (Single car car_ε event-triggered)

$$(((?H; a := A) \cup a := -b);\ t := 0;\ x' = v, v' = a, t' = 1 \,\&\, v \geq 0 \land t \leq \varepsilon)^*$$

Example (Stays before traffic light m if braking would)

$$[x' = v, v' = -b]x \leq m \land v \geq 0 \land A \geq 0 \land b > 0 \rightarrow [car_\varepsilon]x \leq m$$



Example (Controllability equivalence)

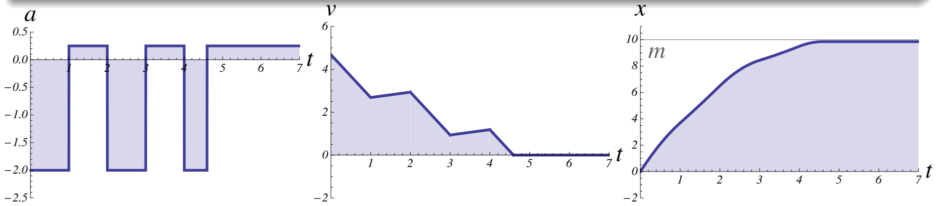
$$v \geq 0 \land b > 0 \rightarrow \left(v^2 \leq 2b(m - x) \leftrightarrow [x' = v, v' = -b]x \leq m\right)$$

Example (Single car car_ε event-triggered)

$$\left(((?H; a := A) \cup a := -b);\ t := 0;\ x' = v, v' = a, t' = 1 \,\&\, v \geq 0 \land t \leq \varepsilon\right)^*$$

Example (Stays before traffic light m if braking would)

$$[x' = v, v' = -b]x \leq m \land v \geq 0 \land A \geq 0 \land b > 0 \rightarrow [car_\varepsilon]x \leq m$$



Example ()

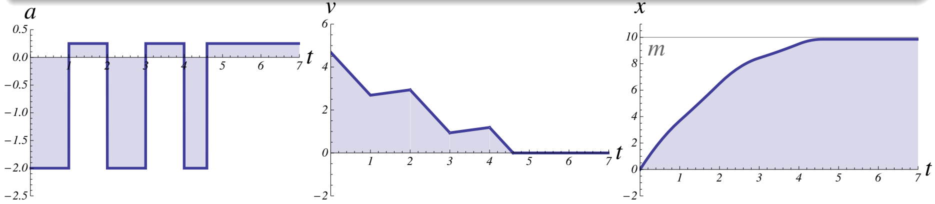
$H \equiv$

Example (Single car car_ε event-triggered)

$$(((?H; a := A) \cup a := -b);\ t := 0;\ x' = v, v' = a, t' = 1 \,\&\, v \geq 0 \wedge t \leq \varepsilon)^*$$

Example (Stays before traffic light m if braking would)

$$[x' = v, v' = -b]x \leq m \wedge v \geq 0 \wedge A \geq 0 \wedge b > 0 \rightarrow [car_\varepsilon]x \leq m$$



Example (Model-predictive control)

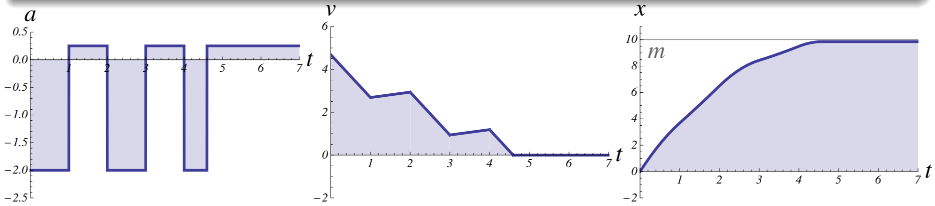
$$H \equiv [t := 0; x' = v, v' = A, t' = 1 \,\&\, v \geq 0 \land t \leq \varepsilon][x' = v, v' = -b]x \leq m$$

Example (Single car car_ε event-triggered)

$$(((?H; a := A) \cup a := -b);\ t := 0;\ x' = v, v' = a, t' = 1 \,\&\, v \geq 0 \land t \leq \varepsilon)^*$$

Example (Stays before traffic light m if braking would)

$$[x' = v, v' = -b]x \leq m \land v \geq 0 \land A \geq 0 \land b > 0 \rightarrow [car_\varepsilon]x \leq m$$



Example (Model-predictive control equivalence)

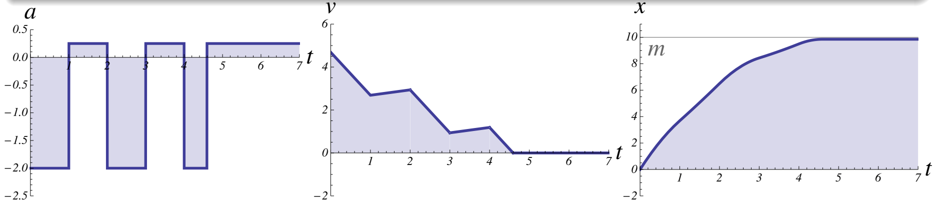
$$H \equiv [t := 0; x' = v, v' = A, t' = 1 \,\&\, v \geq 0 \land t \leq \varepsilon][x' = v, v' = -b]x \leq m$$
$$\leftrightarrow 2b(m - x) \geq v^2 + (A + b)(A\varepsilon^2 + 2\varepsilon v)$$

Example (Single car car_ε event-triggered)

$$(((?H; a := A) \cup a := -b);\ t := 0;\ x' = v, v' = a, t' = 1 \,\&\, v \geq 0 \land t \leq \varepsilon)^*$$

Example (Stays before traffic light m if braking would)

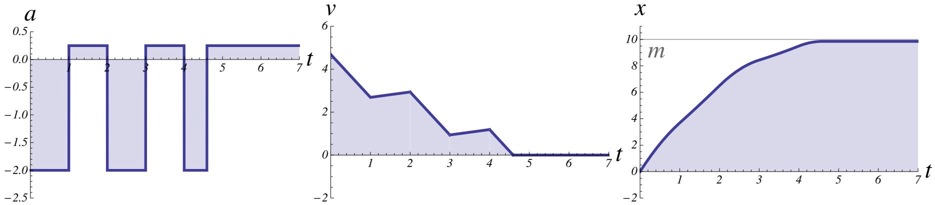
$$[x' = v, v' = -b]x \leq m \land v \geq 0 \land A \geq 0 \land b > 0 \rightarrow [car_\varepsilon]x \leq m$$



Example (dℒ-based model-predictive control design trafo)

$$\underline{\qquad\qquad\qquad} \land v \geq 0 \land A \geq 0 \land b > 0 \rightarrow$$

$$[((\;(?\underline{\qquad\qquad\qquad};\; a := A) \cup a := -b);\; t := 0;\; x' = v, v' = a, t' = 1 \,\&\, v \geq 0 \land t \leq \varepsilon)^*]\, x \leq m$$



Example (d$\mathcal{L}$-based model-predictive control design trafo)

$$\underline{\qquad\qquad ??? \qquad\qquad} \land v \geq 0 \land A \geq 0 \land b > 0 \rightarrow$$

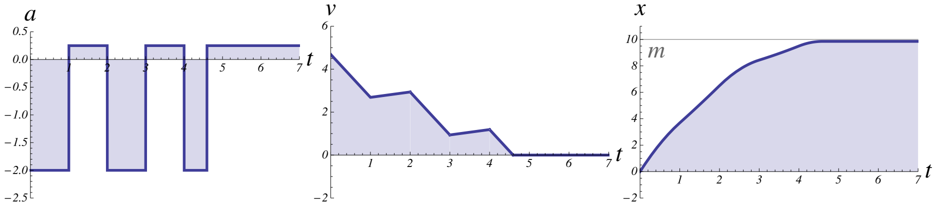
$$\Big[\big(\big($$

$$\quad (?\underline{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}\,;$$

$$\qquad a := A)$$

$$\quad \cup\, a := -b);$$

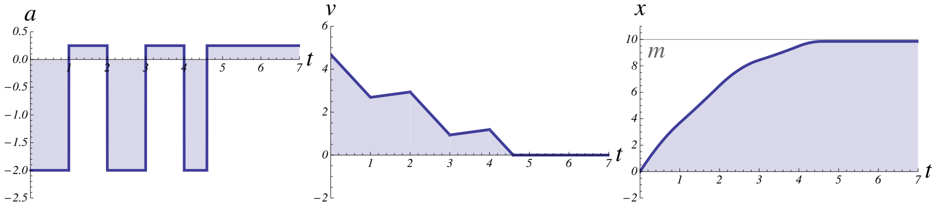
$$\quad t := 0;\ x' = v, v' = a, t' = 1 \,\&\, v \geq 0 \land t \leq \varepsilon\big)^*\Big]\, x \leq m$$



Example (dℒ-based model-predictive control design trafo)

$$\underline{[x' = v, v' = -b]x \le m} \land v \ge 0 \land A \ge 0 \land b > 0 \rightarrow$$

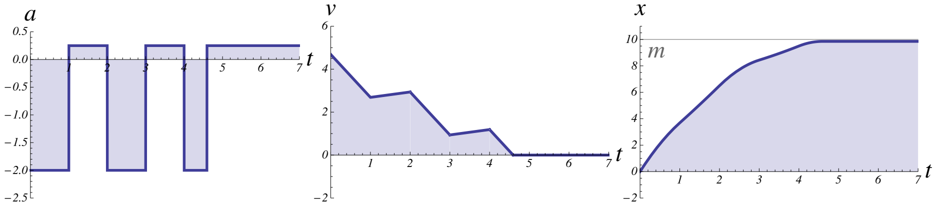
$$\Big[\Big((\, (?\underline{\qquad\qquad\qquad} ;\; a := A) \cup a := -b);\; t := 0;\; x' = v, v' = a, t' = 1 \,\&\, v \ge 0 \land t \le \varepsilon\Big)^*\Big]\, x \le m$$



Example (dℒ-based model-predictive control design trafo)

$$\underline{[x' = v, v' = -b]x \le m} \land v \ge 0 \land A \ge 0 \land b > 0 \rightarrow$$

$$\Big[\Big(\Big(\big(?\ \underline{\quad\color{red}{???}\quad};\ a := A\big) \cup a := -b\Big);\ t := 0;\ x' = v, v' = a, t' = 1 \,\&\, v \ge 0 \land t \le \varepsilon\Big)^*\Big]\, x \le m$$



Ex: Car Control — d$\mathcal{L}$ MPC Design

Example (d$\mathcal{L}$-based model-predictive control design trafo)

$$\underline{[x' = v, v' = -b]x \le m} \land v \ge 0 \land A \ge 0 \land b > 0 \rightarrow$$

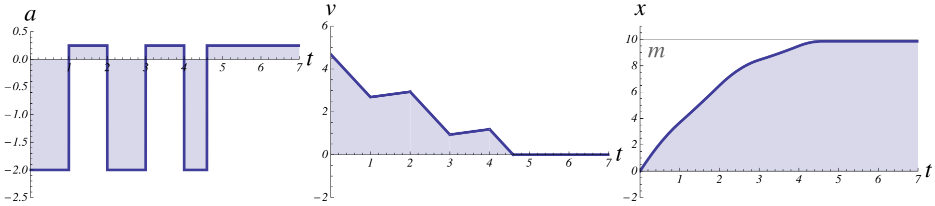
$$\Big[\Big(\Big($$

$$(?\underline{[t := 0; x' = v, v' = A, t' = 1 \,\&\, v \ge 0 \land t \le \varepsilon][x' = v, v' = -b]x \le m};$$

$$a := A)$$

$$\cup\ a := -b);$$

$$t := 0;\ x' = v, v' = a, t' = 1 \,\&\, v \ge 0 \land t \le \varepsilon\Big)^*\Big]\, x \le m$$



Example (d$\mathcal{L}$-based model-predictive control design trafo)

$$\frac{[x' = v, v' = -b]x \le m}{} \land v \ge 0 \land A \ge 0 \land b > 0 \rightarrow$$

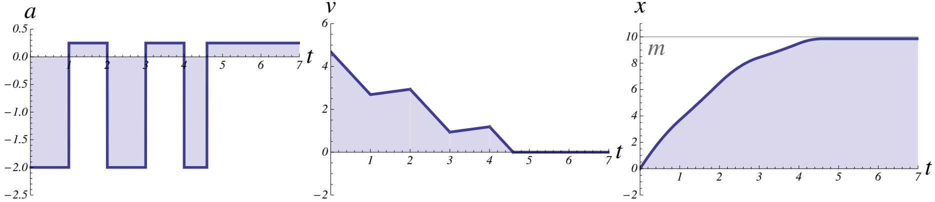
$$\Big[\Big(\Big($$

$$(?\underline{[t := 0; x' = v, v' = A, t' = 1 \,\&\, v \ge 0 \land t \le \varepsilon][x' = v, v' = -b]x \le m} \,;$$

$$a := A)$$

$$\cup\ a := -b);$$

$$t := 0;\ x' = v, v' = a, t' = 1 \,\&\, v \ge 0 \land t \le \varepsilon\Big)^*\Big]\, x \le m$$



Example (dℒ-based model-predictive control design trafo)

$$\underline{v^2 \leq 2b(m-x)} \land v \geq 0 \land A \geq 0 \land b > 0 \rightarrow$$

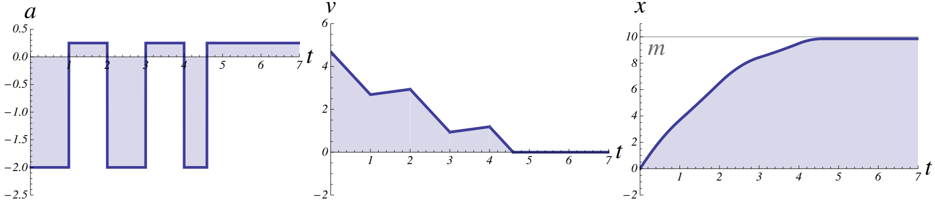
$$\big[\big(\big($$

$$(?\underline{[t := 0; x' = v, v' = A, t' = 1 \,\&\, v \geq 0 \land t \leq \varepsilon][x' = v, v' = -b]x \leq m} \,;$$

$$a := A)$$

$$\cup\, a := -b);$$

$$t := 0;\;\; x' = v, v' = a, t' = 1 \,\&\, v \geq 0 \land t \leq \varepsilon\big)^*\big]\, x \leq m$$



Example (dℒ-based model-predictive control design trafo)

$$\underline{v^2 \leq 2b(m-x)} \land v \geq 0 \land A \geq 0 \land b > 0 \rightarrow$$

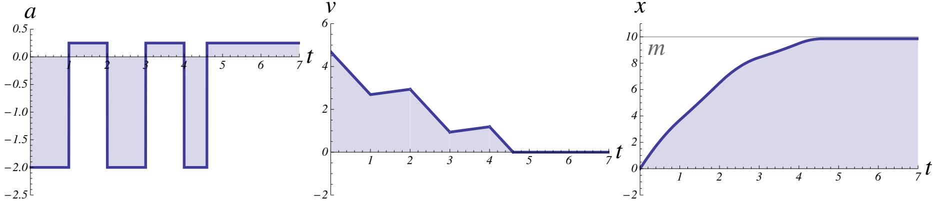
$$\Big[\Big(\big($$

$$(?\underline{[t := 0; x' = v, v' = A, t' = 1 \,\&\, v \geq 0 \land t \leq \varepsilon][x' = v, v' = -b]x \leq m};$$

$$a := A)$$

$$\cup\, a := -b);$$

$$t := 0;\; x' = v, v' = a, t' = 1 \,\&\, v \geq 0 \land t \leq \varepsilon\Big)^*\Big]\, x \leq m$$

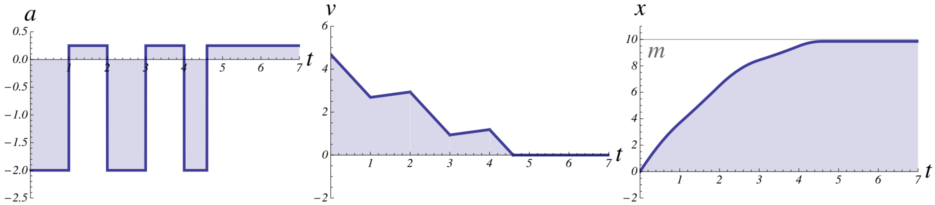


Example (d$\mathcal{L}$-based model-predictive control design trafo)

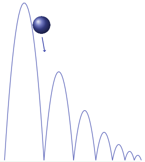
$$\underline{v^2 \le 2b(m-x)} \land v \ge 0 \land A \ge 0 \land b > 0 \rightarrow$$

$$\Big[\Big(\Big(\big(?\underline{2b(m-x) \ge v^2 + (A+b)(A\varepsilon^2 + 2\varepsilon v)}; \; a := A\big) \cup a := -b\Big);$$

$$t := 0;\; x' = v, v' = a, t' = 1 \,\&\, v \ge 0 \land t \le \varepsilon\Big)^*\Big]\, x \le m$$



Ex: Bouncing Ball Properties



$$\texttt{if}(H)\,\alpha\,\texttt{else}\,\beta \equiv (?H;\alpha) \cup (?\neg H;\beta)$$
$$\texttt{while}(H)\,\alpha \equiv (?H;\alpha)^*;?\neg H$$

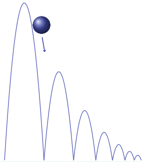
Example (▶ Bouncing ball)

$$\big(\,h' = v, v' = -g \,\&\, h \geq 0;$$
$$\quad \text{if } (h = 0) \text{ then}$$
$$\qquad v := -cv$$
$$\quad \text{fi}\big)^*$$

Example (Bouncing ball height?)

$$h = H \wedge h \geq 0 \wedge g > 0 \rightarrow [ball](0 \leq h \leq H)$$

Ex: Bouncing Ball Properties



$$\texttt{if}(H)\,\alpha\,\texttt{else}\,\beta \equiv (?H;\alpha)\cup(?\neg H;\beta)$$

$$\texttt{while}(H)\,\alpha \equiv (?H;\alpha)^*;?\neg H$$

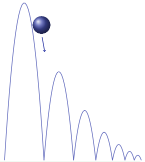
Example (Bouncing ball)

$$\big(\,h' = v, v' = -g \,\&\, h \geq 0;$$
$$\text{if } (h = 0) \text{ then}$$
$$v := -cv$$
$$\text{fi}\big)^*$$

Example (Bouncing ball height?)

$$h = H \wedge h \geq 0 \wedge g > 0 \rightarrow [ball](0 \leq h \leq H)$$

Not if $c > 1$ anti-damping



$$\texttt{if}(H)\,\alpha\,\texttt{else}\,\beta \equiv (?H;\alpha) \cup (?\neg H;\beta)$$

$$\texttt{while}(H)\,\alpha \equiv (?H;\alpha)^*;?\neg H$$

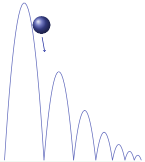
Example (Bouncing ball)

$\big(\, h' = v, v' = -g \,\&\, h \geq 0;$
 if $(h = 0)$ then
 $v := -cv$
 fi$\big)^*$

Example (Bouncing ball height?)

$$1 > c \geq 0 \land h = H \land h \geq 0 \land g > 0 \rightarrow [ball](0 \leq h \leq H)$$

Ex: Bouncing Ball Properties



$$\texttt{if}(H)\,\alpha\,\texttt{else}\,\beta \equiv (?H;\alpha) \cup (?\neg H;\beta)$$

$$\texttt{while}(H)\,\alpha \equiv (?H;\alpha)^*;?\neg H$$

Example (Bouncing ball)

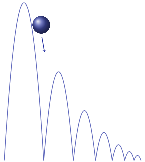
$\big(\, h' = v, v' = -g \,\&\, h \geq 0;$
  if $(h = 0)$ then
    $v := -cv$
  fi$\big)^*$

Example (Bouncing ball height?)

$$1 > c \geq 0 \wedge h = H \wedge h \geq 0 \wedge g > 0 \rightarrow [ball](0 \leq h \leq H)$$

Not if $v > 0$ climbing, initially

Ex: Bouncing Ball Properties



$$\mathtt{if}(H)\,\alpha\,\mathtt{else}\,\beta \equiv (?H;\alpha) \cup (?\neg H;\beta)$$

$$\mathtt{while}(H)\,\alpha \equiv (?H;\alpha)^*;?\neg H$$

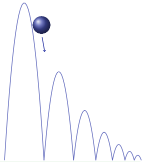
Example (▶ Bouncing ball)

$\big(h' = v, v' = -g \,\&\, h \geq 0;$
  if $(h = 0)$ then
    $v := -cv$
  fi$\big)^*$

Example (Bouncing ball height?)

$$v \leq 0 \land 1 > c \geq 0 \land h = H \land h \geq 0 \land g > 0 \rightarrow [ball](0 \leq h \leq H)$$

Ex: Bouncing Ball Properties



$$\texttt{if}(H)\,\alpha\,\texttt{else}\,\beta \equiv (?H;\alpha) \cup (?\neg H;\beta)$$

$$\texttt{while}(H)\,\alpha \equiv (?H;\alpha)^*; ?\neg H$$

Example (Bouncing ball)

$$\big(\, h' = v, v' = -g \,\&\, h \geq 0;$$
$$\quad \text{if } (h = 0) \text{ then}$$
$$\qquad v := -cv$$
$$\quad \text{fi}\big)^*$$

Example (Bouncing ball height?)

$$v \leq 0 \land 1 > c \geq 0 \land h = H \land h \geq 0 \land g > 0 \to [ball](0 \leq h \leq H)$$

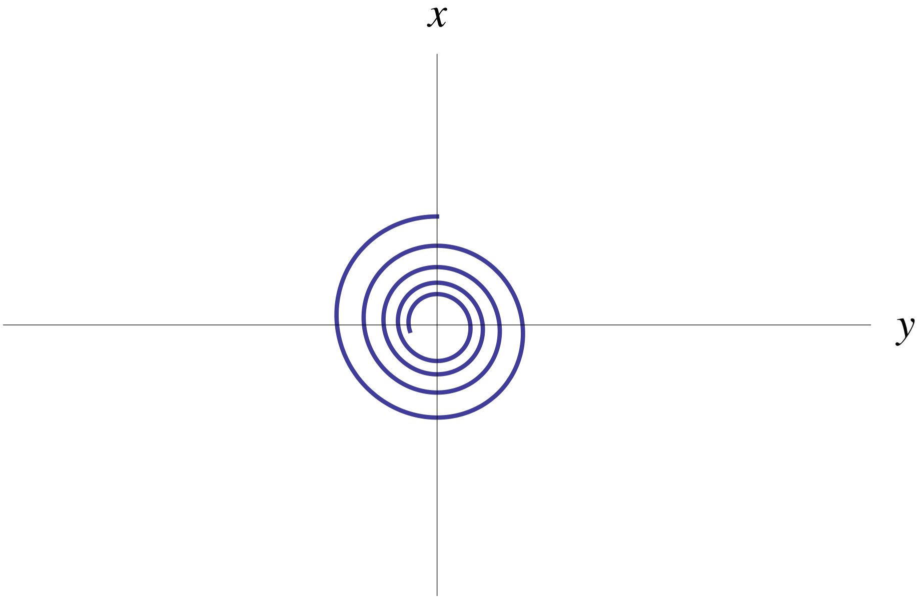
Not if $v \ll 0$ dribbling, initially

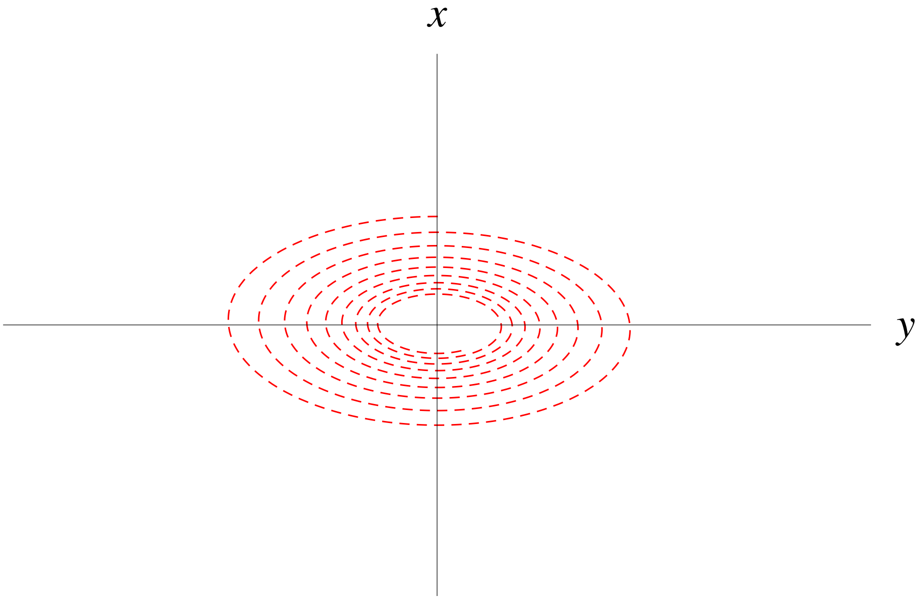
Arbitrarily Nested Modalities and Nested Quantifiers

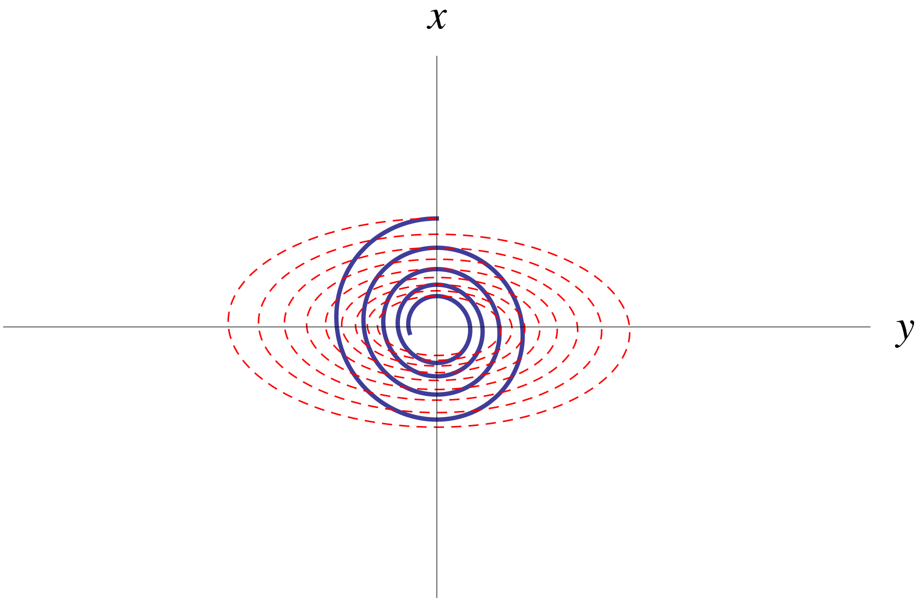
Example (Nest boxes and be happy)

- $[RBC]\text{partitioned} \;\rightarrow\; \exists SB\, \langle \text{Train}\rangle [RBC]\text{safe}$
- $([\text{Train}]\text{safe}) \leftrightarrow \frac{v^2}{2b} \leq m - z \ldots$
- $[\text{rbc}](M \rightarrow [\text{spd}]\langle SB := *\rangle [\text{atp}; \text{drive}]\text{safe})$
- $[\text{aircraft}_1]\langle \text{aircraft}_2\rangle \text{separate}$

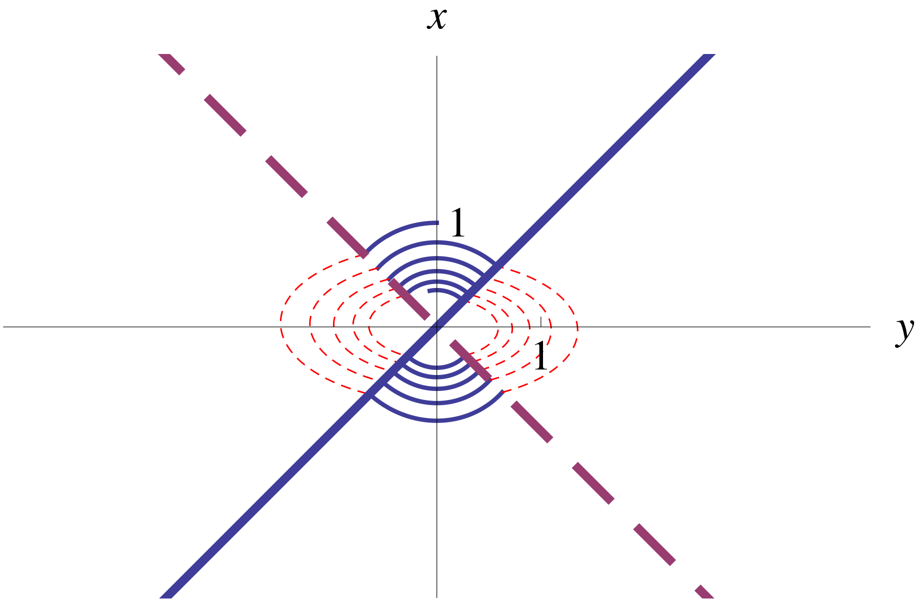
Compositionality in Hybrid Systems



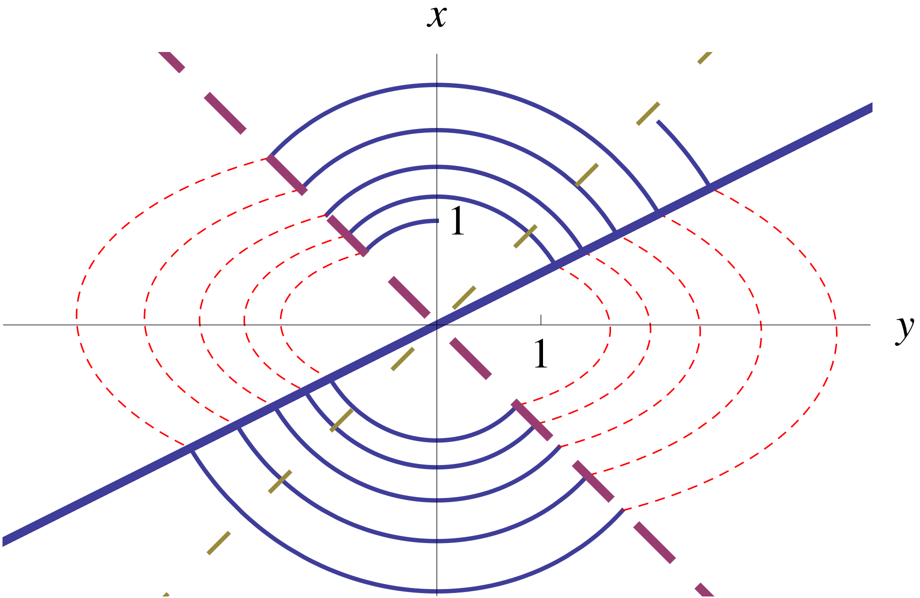

x
y


x
y

Compositionality in Hybrid Systems

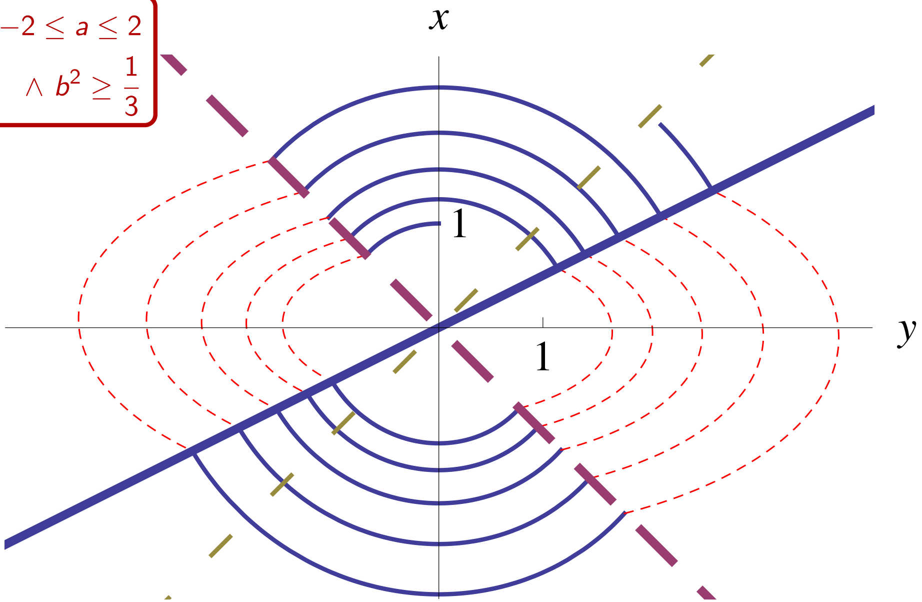


Compositionality in Hybrid Systems



Compositionality in Hybrid Systems

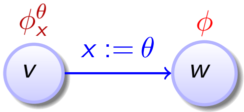
$$-2 \le a \le 2 \;\wedge\; b^2 \ge \frac{1}{3}$$



Outline

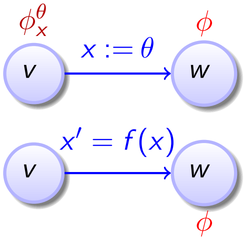
Proof Calculus for Differential Dynamic Logic

$$\frac{\phi_x^\theta}{\langle x := \theta \rangle \phi}$$



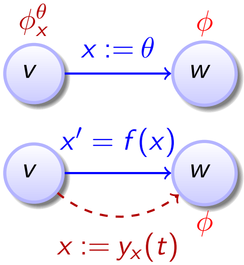
$$\frac{\phi_x^\theta}{\langle x := \theta \rangle \phi}$$

$$\frac{\exists t \geq 0\, \langle x := y_x(t) \rangle \phi}{\langle x' = f(x) \rangle \phi}$$



$$\frac{\phi_x^\theta}{\langle x := \theta\rangle\phi}$$

$$\frac{\exists t{\geq}0\, \langle x := y_x(t)\rangle\phi}{\langle x' = f(x)\rangle\phi}$$

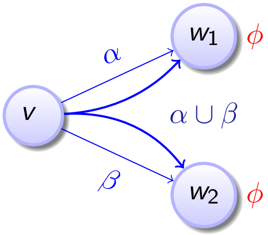


Proof Calculus for Differential Dynamic Logic

compositional semantics $\Rightarrow$ compositional rules!

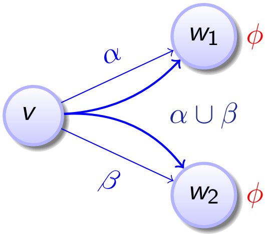
Proof Calculus for Differential Dynamic Logic

$$\frac{[\alpha]\phi \land [\beta]\phi}{[\alpha \cup \beta]\phi}$$

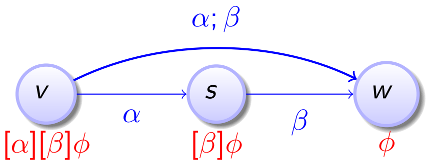


Proof Calculus for Differential Dynamic Logic

$$\frac{[\alpha]\phi \land [\beta]\phi}{[\alpha \cup \beta]\phi}$$

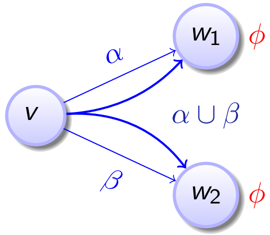


$$\frac{[\alpha][\beta]\phi}{[\alpha;\beta]\phi}$$

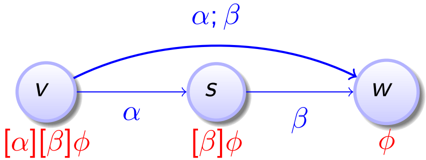


Proof Calculus for Differential Dynamic Logic

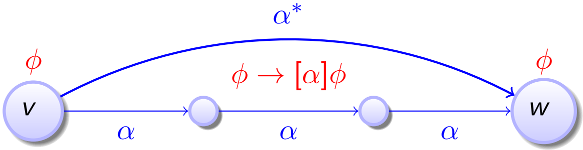
$$\frac{[\alpha]\phi \land [\beta]\phi}{[\alpha \cup \beta]\phi}$$



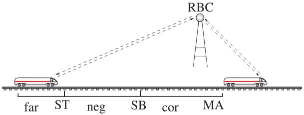
$$\frac{[\alpha][\beta]\phi}{[\alpha;\beta]\phi}$$



$$\frac{\phi \quad (\phi \to [\alpha]\phi)}{[\alpha^*]\phi}$$

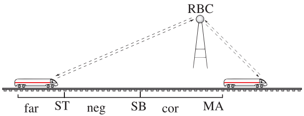


Deduction Modulo Real Arithmetic



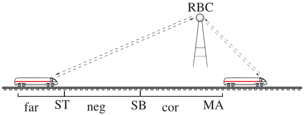
$$v \geq 0 \land z < MA \rightarrow \langle z' = v, v' = -b \rangle\ z > MA$$

Deduction Modulo Real Arithmetic



$$\dfrac{\dfrac{v \geq 0, z < MA \to \exists t{\geq}0\, \langle z := -\frac{b}{2}t^2 + vt + z\rangle z > MA}{v \geq 0, z < MA \to \langle z' = v, v' = -b\rangle z > MA}}{v \geq 0 \land z < MA \to \langle z' = v, v' = -b\rangle\ z > MA}$$

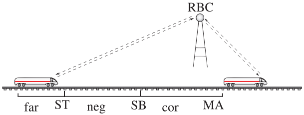
Deduction Modulo Real Arithmetic



Collins/Tarski QE not applicable!

$$\dfrac{\dfrac{v \geq 0, z < MA \rightarrow \exists t{\geq}0\, \langle z := -\frac{b}{2}t^2 + vt + z\rangle z > MA}{v \geq 0, z < MA \rightarrow \langle z' = v, v' = -b\rangle z > MA}}{v \geq 0 \land z < MA \rightarrow \langle z' = v, v' = -b\rangle\ z > MA}$$

Deduction Modulo (Side Deduction)

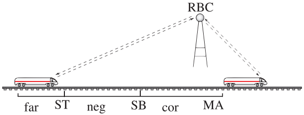


$$\dfrac{}{v \geq 0, z < MA \rightarrow t \geq 0 \land \langle z := -\frac{b}{2}t^2 + vt + z\rangle z > MA}$$

start side

$$\dfrac{\dfrac{\dfrac{}{v \geq 0, z < MA \rightarrow \exists t{\geq}0\, \langle z := -\frac{b}{2}t^2 + vt + z\rangle z > MA}}{v \geq 0, z < MA \rightarrow \langle z' = v, v' = -b\rangle z > MA}}{v \geq 0 \land z < MA \rightarrow \langle z' = v, v' = -b\rangle\ z > MA}$$

Deduction Modulo (Side Deduction)



$$v \geq 0, z < MA \rightarrow -\frac{b}{2}t^2 + vt + z > MA$$

$$v \geq 0, z < MA \rightarrow t \geq 0 \qquad v \geq 0, z < MA \rightarrow \langle z := -\frac{b}{2}t^2 + vt + z\rangle z > M$$

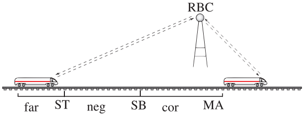
$$v \geq 0, z < MA \rightarrow t \geq 0 \land \langle z := -\frac{b}{2}t^2 + vt + z\rangle z > MA$$

start side

$$v \geq 0, z < MA \rightarrow \exists t{\geq}0\, \langle z := -\frac{b}{2}t^2 + vt + z\rangle z > MA$$

$$v \geq 0, z < MA \rightarrow \langle z' = v, v' = -b\rangle z > MA$$

$$v \geq 0 \land z < MA \rightarrow \langle z' = v, v' = -b\rangle\, z > MA$$



$$v \geq 0, z < MA \rightarrow -\frac{b}{2}t^2 + vt + z > MA$$

$$v \geq 0, z < MA \rightarrow t \geq 0 \qquad v \geq 0, z < MA \rightarrow \langle z := -\frac{b}{2}t^2 + vt + z\rangle z > M$$

$$v \geq 0, z < MA \rightarrow t \geq 0 \wedge \langle z := -\frac{b}{2}t^2 + vt + z\rangle z > MA$$

QE

start side

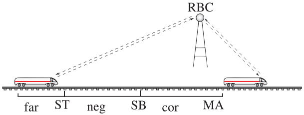
$$v \geq 0, z < MA \rightarrow \mathrm{QE}(\exists t\, (\ldots t \geq 0 \wedge -\frac{b}{2}t^2 + vt + z > MA))$$

$$v \geq 0, z < MA \rightarrow \exists t \geq 0\, \langle z := -\frac{b}{2}t^2 + vt + z\rangle z > MA$$

$$v \geq 0, z < MA \rightarrow \langle z' = v, v' = -b\rangle z > MA$$

$$v \geq 0 \wedge z < MA \rightarrow \langle z' = v, v' = -b\rangle\, z > MA$$

Deduction Modulo (Side Deduction)



$$v \ge 0, z < MA \rightarrow -\frac{b}{2}t^2 + vt + z > MA$$

$$v \ge 0, z < MA \rightarrow t \ge 0 \qquad v \ge 0, z < MA \rightarrow \langle z := -\frac{b}{2}t^2 + vt + z\rangle z > M$$

$$v \ge 0, z < MA \rightarrow t \ge 0 \wedge \langle z := -\frac{b}{2}t^2 + vt + z\rangle z > MA$$

QE

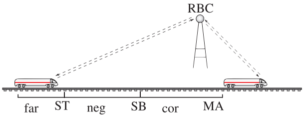
start side

$$v \ge 0, z < MA \rightarrow v^2 > 2b(MA - z)$$

$$v \ge 0, z < MA \rightarrow \exists t \ge 0\, \langle z := -\frac{b}{2}t^2 + vt + z\rangle z > MA$$

$$v \ge 0, z < MA \rightarrow \langle z' = v, v' = -b\rangle z > MA$$

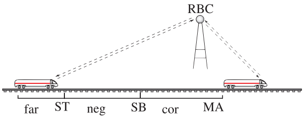
$$v \ge 0 \wedge z < MA \rightarrow \langle z' = v, v' = -b\rangle\, z > MA$$



$$v \geq 0, z < MA \rightarrow \exists t \geq 0 \langle z := -\frac{b}{2}t^2 + vt + z\rangle z > MA$$

$$v \geq 0, z < MA \rightarrow \langle z' = v, v' = -b\rangle z > MA$$

$$v \geq 0 \wedge z < MA \rightarrow \langle z' = v, v' = -b\rangle z > MA$$



$$v \geq 0, z < MA \to -\frac{b}{2}T^2 + vT + z > MA$$

$$v \geq 0, z < MA \to T \geq 0 \qquad v \geq 0, z < MA \to \langle z := -\frac{b}{2}T^2 + vT + z\rangle z > M$$

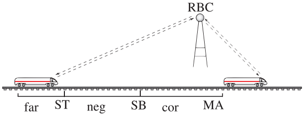
$$v \geq 0, z < MA \to T \geq 0 \land \langle z := -\frac{b}{2}T^2 + vT + z\rangle z > MA$$

$$v \geq 0, z < MA \to \exists t {\geq} 0\, \langle z := -\frac{b}{2}t^2 + vt + z\rangle z > MA$$

$$v \geq 0, z < MA \to \langle z' = v, v' = -b\rangle z > MA$$

$$v \geq 0 \land z < MA \to \langle z' = v, v' = -b\rangle z > MA$$

Deduction Modulo (Free Variables for Automation)



$$v \geq 0, z < MA \to \quad \exists T\, (\ldots T{\geq}0 \land -\tfrac{b}{2} T^2 + vT + z > MA)$$

$$v \geq 0, z < MA \to -\tfrac{b}{2} T^2 + vT + z > MA$$

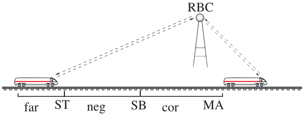
$$v \geq 0, z < MA \to T{\geq}0 \qquad v \geq 0, z < MA \to \langle z := -\tfrac{b}{2} T^2 + vT + z\rangle z > M$$

$$v \geq 0, z < MA \to T \geq 0 \land \langle z := -\tfrac{b}{2} T^2 + vT + z\rangle z > MA$$

$$v \geq 0, z < MA \to \exists t{\geq}0\, \langle z := -\tfrac{b}{2} t^2 + vt + z\rangle z{>}MA$$

$$v \geq 0, z < MA \to \langle z' = v, v' = -b\rangle z > MA$$

$$v \geq 0 \land z < MA \to \langle z' = v, v' = -b\rangle z > MA$$



$$v \geq 0, z < MA \rightarrow \mathrm{QE}\left(\exists T\, (\ldots T \geq 0 \wedge -\tfrac{b}{2} T^2 + vT + z > MA)\right)$$

$$v \geq 0, z < MA \rightarrow -\tfrac{b}{2} T^2 + vT + z > MA$$

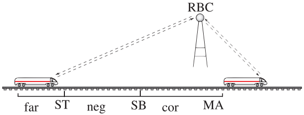
$$v \geq 0, z < MA \rightarrow T \geq 0 \qquad v \geq 0, z < MA \rightarrow \langle z := -\tfrac{b}{2} T^2 + vT + z \rangle z > M$$

$$v \geq 0, z < MA \rightarrow T \geq 0 \wedge \langle z := -\tfrac{b}{2} T^2 + vT + z \rangle z > MA$$

$$v \geq 0, z < MA \rightarrow \exists t \geq 0\, \langle z := -\tfrac{b}{2} t^2 + vt + z \rangle z > MA$$

$$v \geq 0, z < MA \rightarrow \langle z' = v, v' = -b \rangle z > MA$$

$$v \geq 0 \wedge z < MA \rightarrow \langle z' = v, v' = -b \rangle z > MA$$



$$v \geq 0, z < MA \rightarrow v^2 > 2b(MA - z)$$

$$v \geq 0, z < MA \rightarrow -\frac{b}{2}T^2 + vT + z > MA$$

$$v \geq 0, z < MA \rightarrow T \geq 0 \qquad v \geq 0, z < MA \rightarrow \langle z := -\frac{b}{2}T^2 + vT + z\rangle z > M$$

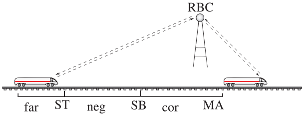
$$v \geq 0, z < MA \rightarrow T \geq 0 \land \langle z := -\frac{b}{2}T^2 + vT + z\rangle z > MA$$

$$v \geq 0, z < MA \rightarrow \exists t \geq 0\, \langle z := -\frac{b}{2}t^2 + vt + z\rangle z > MA$$

$$v \geq 0, z < MA \rightarrow \langle z' = v, v' = -b\rangle z > MA$$

$$v \geq 0 \land z < MA \rightarrow \langle z' = v, v' = -b\rangle z > MA$$

Deduction Modulo (Free Variables for Automation)



- For requantification, not for unification

$$v \geq 0, z < MA \to \mathrm{QE}(\exists T\, (\ldots T{\geq}0 \land -\tfrac{b}{2}T^2 + vT + z > MA))$$

$$\overline{\qquad\qquad v \geq 0, z < MA \to -\tfrac{b}{2}T^2 + vT + z > MA}$$

$$v \geq 0, z < MA \to T{\geq}0 \qquad \overline{v \geq 0, z < MA \to \langle z := -\tfrac{b}{2}T^2 + vT + z\rangle z > M}$$

$$\overline{v \geq 0, z < MA \to T \geq 0 \land \langle z := -\tfrac{b}{2}T^2 + vT + z\rangle z > MA}$$

$$\overline{v \geq 0, z < MA \to \exists t{\geq}0\, \langle z := -\tfrac{b}{2}t^2 + vt + z\rangle z{>}MA}$$

$$\overline{v \geq 0, z < MA \to \langle z' = v, v' = -b\rangle z > MA}$$

$$\overline{v \geq 0 \land z < MA \to \langle z' = v, v' = -b\rangle z > MA}$$

Deduction Modulo (Free Variables for Automation)

$$\dfrac{\dfrac{(X < S)}{\forall s\,(X < s)}}{\exists x\,\forall s\,(x < s)}$$

Deduction Modulo (Free Variables for Automation)

$$\dfrac{\dfrac{\dfrac{\dfrac{\mathrm{QE}(\forall S \exists X (X < S))}{(X < S)}}{\forall s\,(X < s)}}{\exists x\, \forall s\,(x < s)}}{}$$

Deduction Modulo (Free Variables for Automation)

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\mathrm{QE}(\forall S \exists X (X < S))} \qquad \dfrac{}{\mathrm{QE}(\exists X \forall S (X < S))}}{(X < S)}}{\forall s\, (X < s)}}{\exists x\, \forall s\, (x < s)}$$

Deduction Modulo (Free Variables for Automation)

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\textit{true}}{\mathrm{QE}(\forall S \exists X (X < S))} \qquad \dfrac{\textit{false}}{\mathrm{QE}(\exists X \forall S (X < S))}}{(X < S)}}{\forall s\,(X < s)}}{\exists x\, \forall s\,(x < s)}}{\textit{false}!}$$

$$\dfrac{\textit{true}}{\mathrm{QE}(\forall S \exists X (X < S))} \qquad \dfrac{\textit{false}}{\mathrm{QE}(\exists X \forall S (X < S))}$$

$$(X < S)$$

$$\forall s\, (X < s)$$

$$\exists x\, \forall s\, (x < s)$$

false!

Deduction Modulo (Free Variables & Skolemisation)

Skolemisation $S(X)$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\mathit{false}}{\mathrm{QE}(\exists X \forall S\,(X < S))}}{(X < S(X))}}{\forall s\,(X < s)}}{\exists x\, \forall s\,(x < s)}}{\mathit{false}!}$$

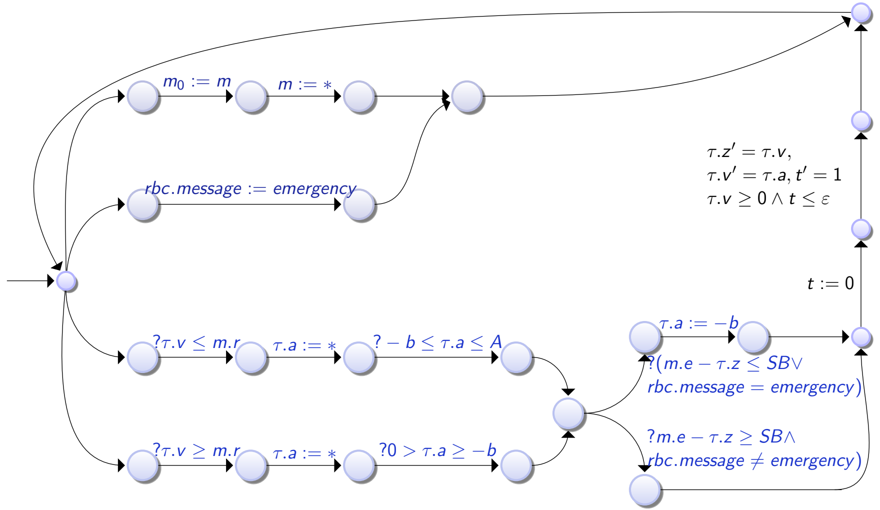
Parametric Skeleton of ETCS

Read from the informal specification...

$$
\begin{array}{ll}
ETCS_{skel} & : (train \cup RBC)^* \\
train & : spd;\ atp;\ drive \\
spd & : \quad (?\tau.v \leq m.r;\ \tau.a := *;\ ?-b \leq \tau.a \leq A) \\
 & \quad \cup(?\tau.v \geq m.r;\ \tau.a := *;\ ?-b \leq \tau.a \leq 0) \\
atp & : \texttt{if}(m.e - \tau.z \leq SB \lor RBC.message = emergency)\, \tau.a := -b \\
drive & : t := 0;\ (\tau.z' = \tau.v, \tau.v' = \tau.a, t' = 1\, \&\, \tau.v \geq 0 \land t \leq \varepsilon) \\
RBC & : (RBC.message := emergency)\ \cup\ (m := *;\ ?m.r > 0)
\end{array}
$$

As transition system...

ETCS Train Control [safety]



Soundness

Theorem (Soundness)

$\mathsf{d}\mathcal{L}$ *calculus is sound, i.e., all provable* $\mathsf{d}\mathcal{L}$ *formulas are valid:*

$$\vdash \phi \textit{ implies } \vDash \phi$$

What about the converse?

Incompleteness

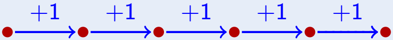
Theorem

Discrete fragment and continuous fragment of $\mathrm{d}\mathcal{L}$ *characterize* $\mathbb{N}$

Proof.

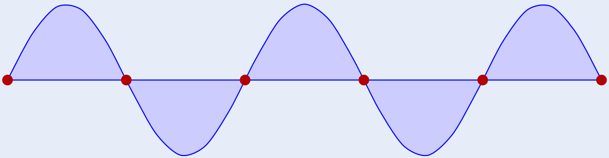
Discrete fragment:

$$\langle (x := x+1)^* \rangle \; x = n$$



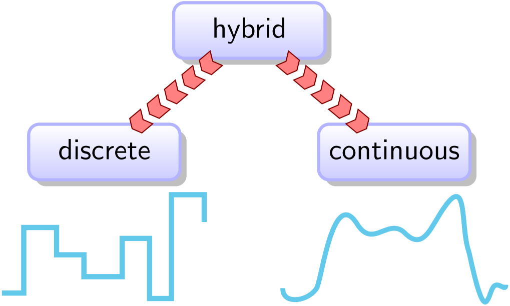
Continuous fragment:

$$\langle s'' = -s, \tau' = 1 \rangle (s = 0 \land \tau = n) \qquad \rightsquigarrow s = \sin$$



∎

Soundness and Completeness



Soundness and Completeness

Theorem (Relative Completeness)

dℒ calculus is a sound & complete axiomatization of hybrid systems relative to differential equations.

Proof Outline 15p

André Platzer.
Differential dynamic logic for hybrid systems.
J. Autom. Reas., 41(2):143–189, 2008.

Soundness and Completeness

Theorem (Relative Completeness)

d$\mathcal{L}$ *calculus is a sound & complete axiomatization of hybrid systems relative to differential equations.* ▸ Proof Outline 15p

Corollary (Proof-theoretical Alignment)

verification of hybrid systems = verification of dynamical systems!

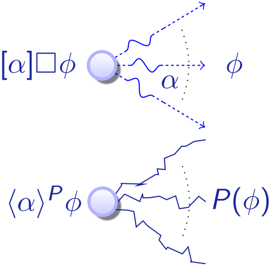
Corollary (Compositionality)

hybrid systems can be verified by recursive decomposition

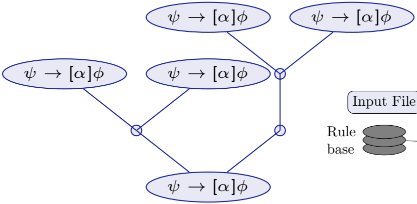
André Platzer.
Differential dynamic logic for hybrid systems.
J. Autom. Reas., 41(2):143–189, 2008.

Outline

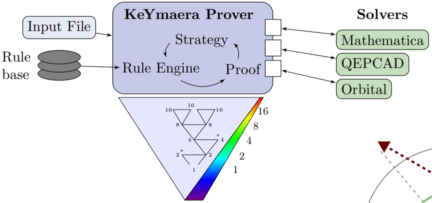
$\neg F$
F
F



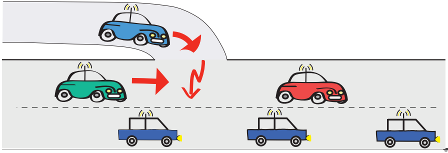
$[\alpha]\Box\phi$
α
ϕ
$\langle\alpha\rangle^P\phi$
$P(\phi)$

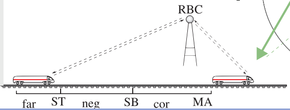


$\psi \rightarrow [\alpha]\phi$
$\psi \rightarrow [\alpha]\phi$
$\psi \rightarrow [\alpha]\phi$
$\psi \rightarrow [\alpha]\phi$
$\psi \rightarrow [\alpha]\phi$

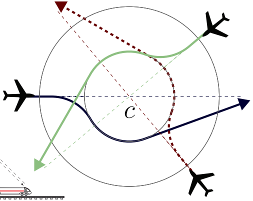


KeYmaera Prover
Input File
Rule base
Strategy
Rule Engine
Proof
Solvers
Mathematica
QEPCAD
Orbital
16
8
4
2
1



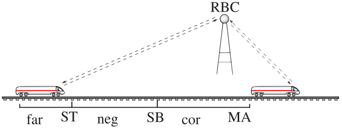


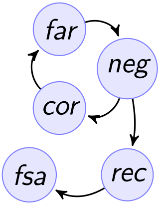
RBC
far
ST
neg
SB
cor
MA

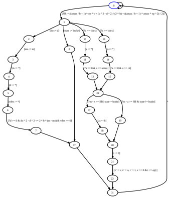


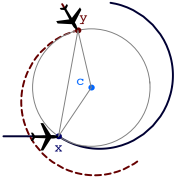
c

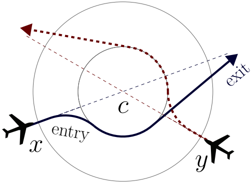
Successful Hybrid Systems Proofs

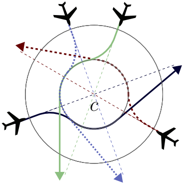


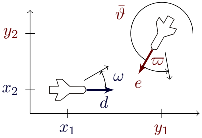


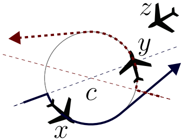


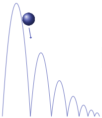


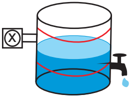




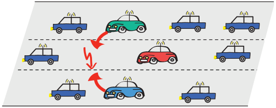
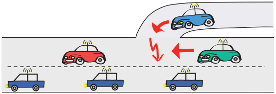
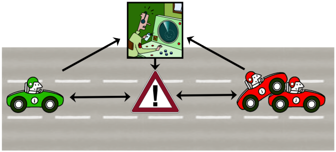
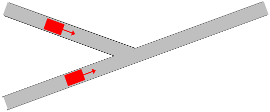
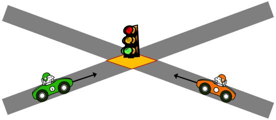
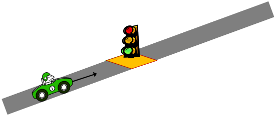
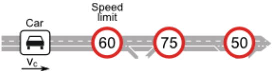


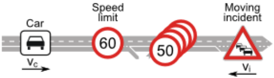


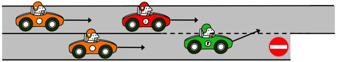
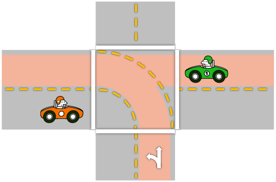
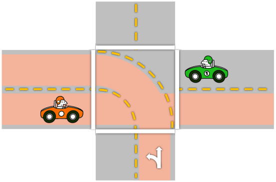
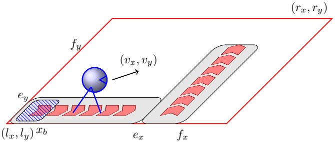




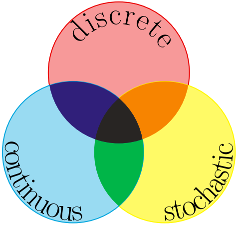
Successful Hybrid Systems Proofs



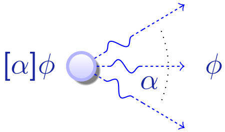





Outline

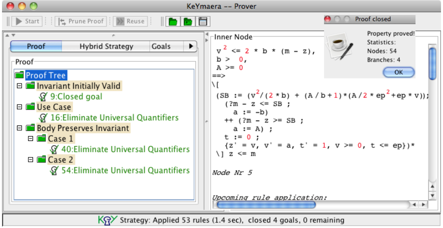


differential dynamic logic

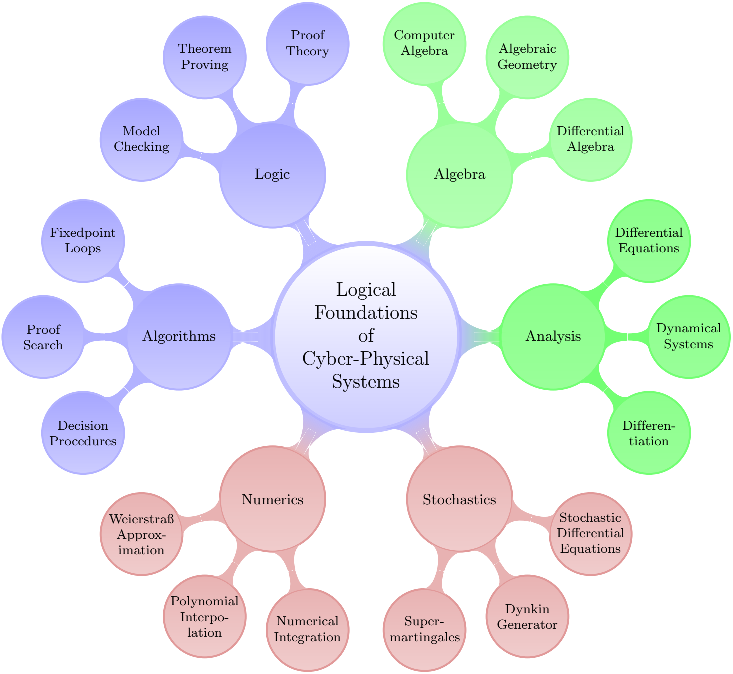
$$d\mathcal{L} = \mathrm{DL} + \mathrm{HP}$$

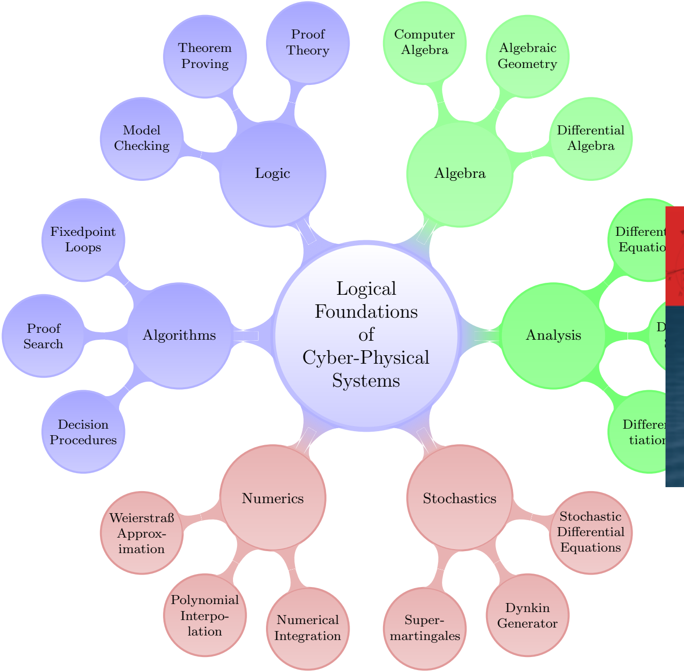


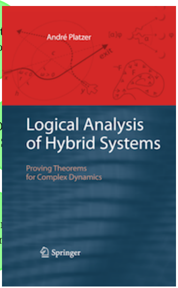
KeYmaera



- Logic for hybrid systems
- Logic + distributed hybrid systems
- Logic + stochastic hybrid systems
- Compositional proofs
- Sound & complete / ODE
- Differential invariants


Logical Foundations of Cyber-Physical Systems
Logic
Model Checking
Theorem Proving
Proof Theory
Algebra
Computer Algebra
Algebraic Geometry
Differential Algebra
Analysis
Differential Equations
Dynamical Systems
Differen-tiation
Stochastics
Stochastic Differential Equations
Dynkin Generator
Super-martingales
Numerics
Numerical Integration
Polynomial Interpo-lation
Weierstraß Approx-imation
Algorithms
Fixedpoint Loops
Proof Search
Decision Procedures


Logical Foundations of Cyber-Physical Systems
Logic
Model Checking
Theorem Proving
Proof Theory
Algebra
Computer Algebra
Algebraic Geometry
Differential Algebra
Algorithms
Fixedpoint Loops
Proof Search
Decision Procedures
Analysis
Numerics
Weierstraß Approx-imation
Polynomial Interpo-lation
Numerical Integration
Stochastics
Stochastic Differential Equations
Dynkin Generator
Super-martingales


André Platzer
Logical Analysis of Hybrid Systems
Proving Theorems for Complex Dynamics
Springer

André Platzer.
Logics of dynamical systems.
In LICS [9], pages 13–24.

André Platzer.
The complete proof theory of hybrid systems.
In LICS [9], pages 541–550.

André Platzer.
Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics.
Springer, Heidelberg, 2010.

André Platzer.
Differential dynamic logic for hybrid systems.
J. Autom. Reas., 41(2):143–189, 2008.

André Platzer.
Differential-algebraic dynamic logic for differential-algebraic programs.
J. Log. Comput., 20(1):309–352, 2010.
Advance Access published on November 18, 2008.

André Platzer and Edmund M. Clarke.
Computing differential invariants of hybrid systems as fixedpoints.
Form. Methods Syst. Des., 35(1):98–120, 2009.
Special issue for selected papers from CAV'08.

André Platzer and Jan-David Quesel.
KeYmaera: A hybrid theorem prover for hybrid systems.
In Alessandro Armando, Peter Baumgartner, and Gilles Dowek, editors, *IJCAR*, volume 5195 of *LNCS*, pages 171–178. Springer, 2008.

André Platzer.
Differential dynamic logic for verifying parametric hybrid systems.
In Nicola Olivetti, editor, *TABLEAUX*, volume 4548 of *LNCS*, pages 216–232. Springer, 2007.

Proceedings of the 27th Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2012, June 25–28, 2012, Dubrovnik, Croatia. IEEE Computer Society, 2012.

João P. Hespanha and Ashish Tiwari, editors.

Hybrid Systems: Computation and Control, 9th International Workshop, HSCC 2006, Santa Barbara, CA, USA, March 29-31, 2006, Proceedings, volume 3927 of *LNCS*. Springer, 2006.

André Platzer.
Quantified differential dynamic logic for distributed hybrid systems.
In Anuj Dawar and Helmut Veith, editors, *CSL*, volume 6247 of *LNCS*, pages 469–483. Springer, 2010.

André Platzer.
A complete axiomatization of quantified differential dynamic logic for distributed hybrid systems.
Logical Methods in Computer Science, 2012.
Special issue for selected papers from CSL'10.

Akash Deshpande, Aleks Göllü, and Pravin Varaiya.
SHIFT: A formalism and a programming language for dynamic networks of hybrid automata.
In Panos J. Antsaklis, Wolf Kohn, Anil Nerode, and Shankar Sastry, editors, *Hybrid Systems*, volume 1273 of *LNCS*, pages 113–133. Springer, 1996.

Fabian Kratz, Oleg Sokolsky, George J. Pappas, and Insup Lee.
R-Charon, a modeling language for reconfigurable hybrid systems.
In Hespanha and Tiwari [10], pages 392–406.

Zhou Chaochen, Wang Ji, and Anders P. Ravn.
A formal description of hybrid systems.
In Rajeev Alur, Thomas A. Henzinger, and Eduardo D. Sontag, editors, *Hybrid Systems*, volume 1066 of *LNCS*, pages 511–530. Springer, 1995.

Pieter J. L. Cuijpers and Michel A. Reniers.
Hybrid process algebra.
J. Log. Algebr. Program., 62(2):191–245, 2005.

D. A. van Beek, Ka L. Man, Michel A. Reniers, J. E. Rooda, and Ramon R. H. Schiffelers.
Syntax and consistent equation semantics of hybrid Chi.
J. Log. Algebr. Program., 68(1-2):129–210, 2006.

William C. Rounds.
A spatial logic for the hybrid π-calculus.

In Rajeev Alur and George J. Pappas, editors, *HSCC*, volume 2993 of *LNCS*, pages 508–522. Springer, 2004.

Jan A. Bergstra and C. A. Middelburg.
Process algebra for hybrid systems.
Theor. Comput. Sci., 335(2-3):215–280, 2005.

José Meseguer and Raman Sharykin.
Specification and analysis of distributed object-based stochastic hybrid systems.
In Hespanha and Tiwari [10], pages 460–475.

André Platzer.
Stochastic differential dynamic logic for stochastic hybrid programs.
In Nikolaj Bjørner and Viorica Sofronie-Stokkermans, editors, *CADE*, volume 6803 of *LNCS*, pages 431–445. Springer, 2011.

André Platzer and Edmund M. Clarke.
The image computation problem in hybrid systems model checking.
In Alberto Bemporad, Antonio Bicchi, and Giorgio Buttazzo, editors, *HSCC*, volume 4416 of *LNCS*, pages 473–486. Springer, 2007.

Outline Background

Outline Background

	Op	Par	T	Cl	Tec	Aut	Cex	Dim	
HenzingerH94, HyTech	✓	×	✓	×	✓	✓	✓		LHA
LafferrierePY99	✓	×	✓	×	✓		✓		forgetful reset
Fränzle99	✓	×	✓	×	✓		✓	×	robust systems
CKrogh03, CheckMate	✓	×	✓	×	✓	✓	✓		polyhedral
Frehse05, PHAVer	✓	×	✓	×	✓	✓	✓	8	LHA (+affine)
MysorePM05	✓	×	✓	×	✓	●	✓	4	bounded prefix
TomlinPS98,MBT05	○	×	×	×	○	○	●	4	HJB numPDE
RatschanS07, HSolver	✓	×		×	✓	✓	×	4	interval
MannaS98, STeP	✓			×	✓	○	×	7	inv$\mapsto$VCG, flat
ÁbrahámSH01, PVS	●			×	●	○	×	$\approx$9	HA$\hookrightarrow$PVS, -“-
ZhouRH92, EDC	×	●	✓	..	×	×	×	×	no maths
DavorenN00, Lμ	×	×		✓	○	×	×	×	prop. H-semantics
RönkköRS03, HGC	✓	×	×	×	×	×	×	×	HGC$\hookrightarrow$HOL
SSManna04	●	○		×	✓		×	4/1	equational system
CTiwari05	●	○		×	✓		×	6/0	linear, -”-
PrajnaJP07, barrier	●	×		×	●		×	3	needs 10000-dim
d$\mathcal{L}$ & dTL	✓	✓	✓	✓	✓	●	×	28	expr., compos.

	Dom	Op	Base	Modal	Quant	Cmpl	Aut
DL	$\mathbb{N}$		$\text{FOL}_{(\mathbb{N})}$		FV+unify	$/\mathbb{N}$	
$d\mathcal{L}$	$\mathbb{R}$	x'	$\text{FOL}_{\mathbb{R}}$	ODE	FV+requant+QE	/ODE	IBC

Outline Background

6. Formal Details
   - Soundness Proof
   - Completeness Proof
7. Differential Algebraic Dynamic Logic DAL (Excerpt)
   - Air Traffic Control
   - Structure of Differential Invariants
   - Computing Differential Invariants as Fixedpoints
   - Derivations and Differentiation
   - Differential Variants
8. Differential Temporal Dynamic Logic dTL (Excerpt)
9. Deduction Modulo Real Algebraic and Computer Algebraic Constraints
10. European Train Control System
11. Collision Avoidance Maneuvers in Air Traffic Control
12. Hybrid Automata Embedding
13. Distributed Hybrid Systems
14. Car Control Verification
15. Stochastic Hybrid Systems

Soundness

Proof (Soundness).

- $x' = f(x)$
- Side deductions
- Free variables & Skolemisation

□

Return

Incompleteness

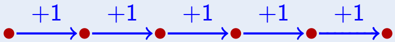
Theorem

Discrete fragment and continuous fragment of $\mathrm{d}\mathcal{L}$ *characterize* $\mathbb{N}$

Proof.

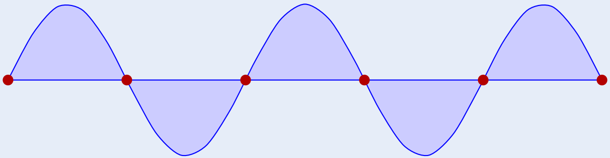
Discrete fragment:

$$\langle (x := x+1)^* \rangle\ x = n$$



Continuous fragment:

$$\langle s'' = -s, \tau' = 1 \rangle (s = 0 \land \tau = n) \qquad \leadsto s = \sin$$



Outline Background

Incomplete! But are we missing proof rules?

Incomplete! But are we missing proof rules?

Relativity

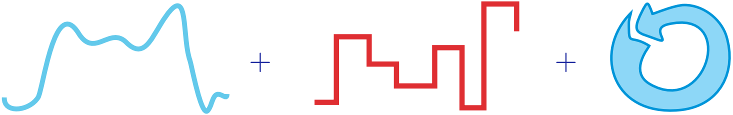
Cook,Harel: discrete-DL/$\text{data}_{\mathbb{N}}$ hybrid-d$\mathcal{L}$/$\text{data}_{\mathbb{R}}$??

Sources of Incompleteness

Sources of Incompleteness

continuous

Sources of Incompleteness

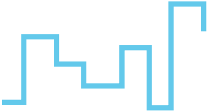


continuous discrete

Sources of Incompleteness

continuous

+

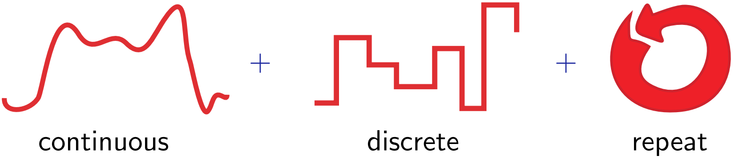


discrete

+

repeat

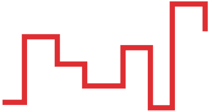
Sources of Incompleteness



Relative Completeness

continuous

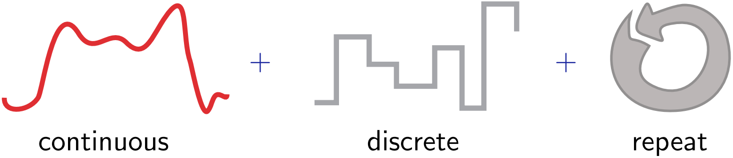
+



discrete

+

repeat


continuous
+
discrete
+
repeat

Relative Completeness

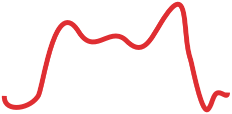
Theorem (Relative Completeness)

d$\mathcal{L}$ calculus is complete relative to first-order logic of differential equations.

$$\vDash \phi \quad \text{iff} \quad \mathit{Taut}_{\mathrm{FOD}} \vdash \phi$$

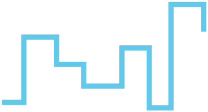
where $\mathrm{FOD} = \mathrm{FOL}_{\mathbb{R}} + [x_1' = \theta_1, \ldots, x_n' = \theta_n]F$

Proof Outline 15p



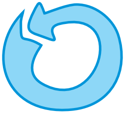
continuous

$+$



discrete

$+$



repeat

$\Downarrow$

Theorem (Relative Completeness)

d$\mathcal{L}$ calculus is complete relative to first-order logic of differential equations.

$$\vDash \phi \quad \text{iff} \quad Taut_{\text{FOD}} \vdash \phi$$

where $\text{FOD} = \text{FOL}_{\mathbb{R}} + [x_1' = \theta_1, \ldots, x_n' = \theta_n]F$

Proof Outline 15p

$\Downarrow$

Relativity

Cook,Harel: discrete-DL/data P.: hybrid-d$\mathcal{L}$/differential equations

Relative Completeness

Theorem (Relative Completeness)

d$\mathcal{L}$ calculus is complete relative to first-order logic of differential equations.

$$\vDash \phi \quad \text{iff} \quad Taut_{\mathrm{FOD}} \vdash \phi$$

where $\quad \mathrm{FOD} = \mathrm{FOL}_{\mathbb{R}} + [x_1' = \theta_1, \ldots, x_n' = \theta_n]F$

▸ Proof Outline 15p

$\Downarrow$

Corollary (Proof-theoretical Alignment)

verification of hybrid systems = verification of dynamical systems!

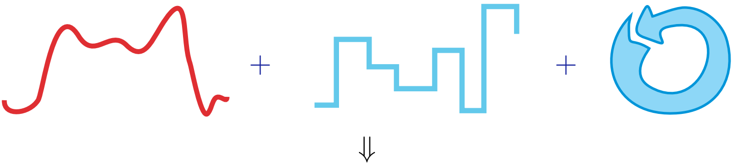
Theorem (Relative Completeness)

d$\mathcal{L}$ calculus is complete relative to first-order logic of differential equations.

$$\vDash \phi \quad \text{iff} \quad Taut_{\text{FOD}} \vdash \phi$$

where $\quad \text{FOD} = \text{FOL}_{\mathbb{R}} + [x_1' = \theta_1, \ldots, x_n' = \theta_n]F$

▸ Proof Outline 15p



Corollary (Deductive Power)

d$\mathcal{L}$ calculus is *supremal hybrid* verification technique

Relative Completeness Proof

$$\vDash \phi \quad \text{iff} \quad Taut_{\mathsf{FOD}} \vdash \phi$$

$$\text{where} \quad \mathsf{FOD} = \mathsf{FOL}_{\mathbb{R}} + [x_1' = \theta_1, \dots, x_n' = \theta_n]F$$

Proof (Relative Completeness, 10 pages)

◂ Return.

1. Strong invariants and variants expressible in d$\mathcal{L}$
2. d$\mathcal{L}$ expressible in FOD
3. valid d$\mathcal{L}$ formulas d$\mathcal{L}$-derivable from corresponding FOD axioms
4. finite FOD formula characterising unbounded hybrid repetition
5. FOD characterises $\mathbb{R}$-Gödel encoding
6. First-order expressible & program rendition: $\forall\phi\ \exists F \in \mathsf{FOD} \quad \vDash \phi \leftrightarrow F$
7. Propositionally & first-order complete
8. Relative complete for first-order safety $F \rightarrow [\alpha]G$
9. Relative complete for first-order liveness $F \rightarrow \langle\alpha\rangle G$

□

Relative Completeness Proof

$$\vDash \phi \quad \text{iff} \quad Taut_{\mathrm{FOD}} \vdash \phi$$

$$\text{where} \quad \mathrm{FOD} = \mathrm{FOL}_{\mathbb{R}} + [x_1' = \theta_1, \ldots, x_n' = \theta_n]F$$

Proof (Relative Completeness, 10 pages)

Return

1. Strong invariants and variants expressible in d$\mathcal{L}$
2. d$\mathcal{L}$ expressible in FOD
3. valid d$\mathcal{L}$ formulas d$\mathcal{L}$-derivable from corresponding FOD axioms
4. finite FOD formula characterising unbounded hybrid repetition
5. FOD characterises $\mathbb{R}$-Gödel encoding
6. First-order expressible & program rendition: $\forall \phi\ \exists F \in \mathrm{FOD} \quad \vDash \phi \leftrightarrow F$
7. Propositionally & first-order complete
8. Relative complete for first-order safety $F \to [\alpha]G$
9. Relative complete for first-order liveness $F \to \langle \alpha \rangle G$

□

Relative Completeness Proof

$$\vDash \phi \quad \text{iff} \quad Taut_{\mathrm{FOD}} \vdash \phi$$

$$\text{where} \quad \mathrm{FOD} = \mathrm{FOL}_{\mathbb{R}} + [x_1' = \theta_1, \dots, x_n' = \theta_n]F$$

Proof (Relative Completeness, 10 pages)

Return

1. Strong invariants and variants expressible in d$\mathcal{L}$
2. d$\mathcal{L}$ expressible in FOD
3. valid d$\mathcal{L}$ formulas d$\mathcal{L}$-derivable from corresponding FOD axioms
4. finite FOD formula characterising unbounded hybrid repetition
5. FOD characterises $\mathbb{R}$-Gödel encoding
6. First-order expressible & program rendition: $\forall\phi\ \exists F \in \mathrm{FOD} \quad \vDash \phi \leftrightarrow F$
7. Propositionally & first-order complete
8. Relative complete for first-order safety $F \to [\alpha]G$
9. Relative complete for first-order liveness $F \to \langle\alpha\rangle G$

□

Relative Completeness Proof

$$\vDash \phi \quad \text{iff} \quad Taut_{\mathrm{FOD}} \vdash \phi$$

$$\text{where} \quad \mathrm{FOD} = \mathrm{FOL}_{\mathbb{R}} + [x_1' = \theta_1, \dots, x_n' = \theta_n]F$$

Proof (Relative Completeness, 10 pages)

Return.

1. Strong invariants and variants expressible in $\mathsf{d}\mathcal{L}$
2. $\mathsf{d}\mathcal{L}$ expressible in FOD
3. valid $\mathsf{d}\mathcal{L}$ formulas $\mathsf{d}\mathcal{L}$-derivable from corresponding FOD axioms
4. finite FOD formula characterising unbounded hybrid repetition
5. FOD characterises $\mathbb{R}$-Gödel encoding
6. First-order expressible & program rendition: $\forall \phi \; \exists F \in \mathrm{FOD} \quad \vDash \phi \leftrightarrow F$
7. Propositionally & first-order complete
8. Relative complete for first-order safety $F \rightarrow [\alpha]G$
9. Relative complete for first-order liveness $F \rightarrow \langle\alpha\rangle G$

□

Relative Completeness Proof

$$\vDash \phi \quad \text{iff} \quad Taut_{\mathrm{FOD}} \vdash \phi$$

$$\text{where} \quad \mathrm{FOD} = \mathrm{FOL}_{\mathbb{R}} + [x_1' = \theta_1, \ldots, x_n' = \theta_n]F$$

Proof (Relative Completeness, 10 pages)

Return.

1. Strong invariants and variants expressible in $d\mathcal{L}$
2. $d\mathcal{L}$ expressible in FOD
3. valid $d\mathcal{L}$ formulas $d\mathcal{L}$-derivable from corresponding FOD axioms
4. finite FOD formula characterising unbounded hybrid repetition
5. FOD characterises $\mathbb{R}$-Gödel encoding
6. First-order expressible & program rendition: $\forall \phi \ \exists F \in \mathrm{FOD} \quad \vDash \phi \leftrightarrow F$
7. Propositionally & first-order complete
8. Relative complete for first-order safety $F \rightarrow [\alpha]G$
9. Relative complete for first-order liveness $F \rightarrow \langle \alpha \rangle G$

□

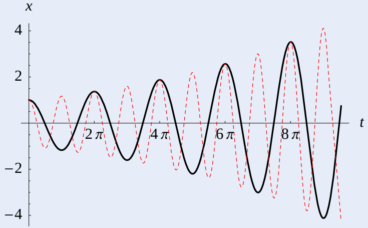
Relative Completeness Proof

where $\quad \text{FOD} = \text{FOL}_{\mathbb{R}} + [x_1' = \theta_1, \ldots, x_n' = \theta_n]F$

Proof ($\mathbb{R}$-Gödel encoding)

Return

FOD characterises constructive bijection $\mathbb{R} \to \mathbb{R}^2$



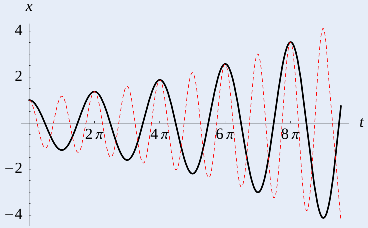
Relative Completeness Proof

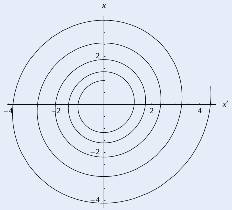
where $\quad \mathrm{FOD} = \mathrm{FOL}_{\mathbb{R}} + [x_1' = \theta_1, \ldots, x_n' = \theta_n]F$

Proof ($\mathbb{R}$-Gödel encoding)

Return

FOD characterises constructive bijection $\mathbb{R} \to \mathbb{R}^2$



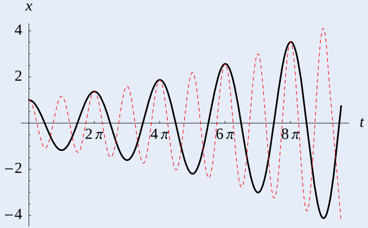


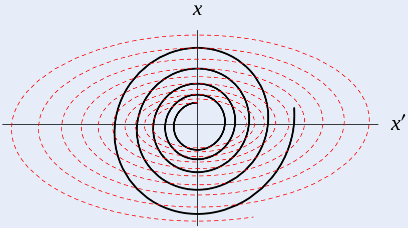
where $\quad \mathrm{FOD} = \mathrm{FOL}_{\mathbb{R}} + [x_1' = \theta_1, \ldots, x_n' = \theta_n]F$

Proof ($\mathbb{R}$-Gödel encoding)

Return.

FOD characterises constructive bijection $\mathbb{R} \to \mathbb{R}^2$





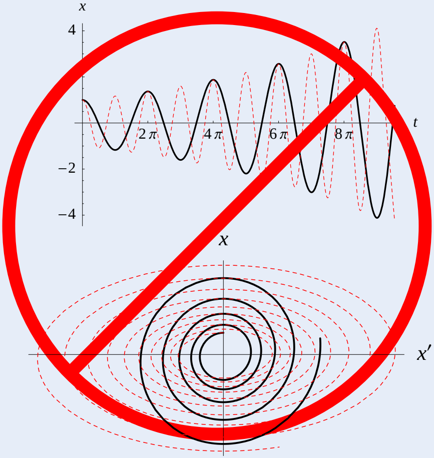
Relative Completeness Proof

where $\text{FOD} = \text{FOL}_{\mathbb{R}} + [x_1' = \theta_1, \dots, x_n' = \theta_n]F$

Proof ($\mathbb{R}$-Gödel encoding)

Return

FOD characterises constructive bijection $\mathbb{R} \to \mathbb{R}^2$ not differentiable!



where $\quad \text{FOD} = \text{FOL}_{\mathbb{R}} + [x_1' = \theta_1, \ldots, x_n' = \theta_n]F$

Proof ($\mathbb{R}$-Gödel encoding)

Return

FOD characterises constructive bijection $\mathbb{R} \to \mathbb{R}^2$

$$\sum_{i=1}^{\infty} \frac{a_i}{2^i} = 0.a_1 a_2 \ldots$$

$$\sum_{i=1}^{\infty} \frac{b_i}{2^i} = 0.b_1 b_2 \ldots$$

$$\sum_{i=0}^{\infty} \left(\frac{a_i}{2^{2i+1}} + \frac{b_i}{2^{2i+2}} \right) = 0.a_1 b_1 a_2 b_2 \ldots$$

□

Relative Completeness Proof

where FOD $= \text{FOL}_{\mathbb{R}} + [x_1' = \theta_1, \ldots, x_n' = \theta_n]F$

Proof ($\mathbb{R}$-Gödel encoding)

◂ Return

FOD characterises constructive bijection $\mathbb{R} \to \mathbb{R}^2$

$$\sum_{i=1}^{\infty} \frac{a_i}{2^i} = 0.a_1 a_2 \ldots$$

$$\sum_{i=1}^{\infty} \frac{b_i}{2^i} = 0.b_1 b_2 \ldots$$

$$\sum_{i=0}^{\infty} \left(\frac{a_i}{2^{2i+1}} + \frac{b_i}{2^{2i+2}} \right) = 0.a_1 b_1 a_2 b_2 \ldots$$

$$2^n = z \quad \leftrightarrow \quad \langle x := 1; \tau := 0; x' = x \ln 2 \land \tau' = 1 \rangle (\tau = n \land x = z)$$

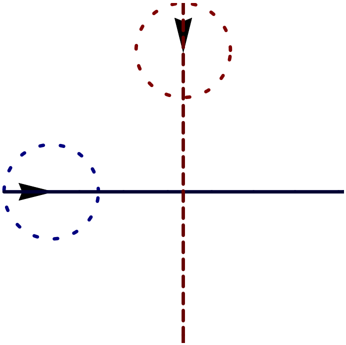
$$\ln 2 = z \quad \leftrightarrow \quad \langle x := 1; \tau := 0; x' = x \land \tau' = 1 \rangle (x = 2 \land \tau = z)$$

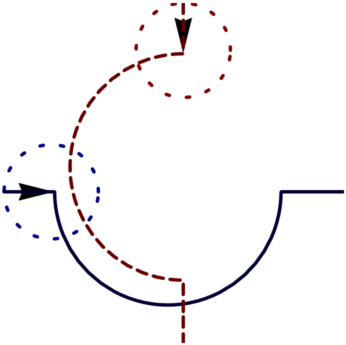
□

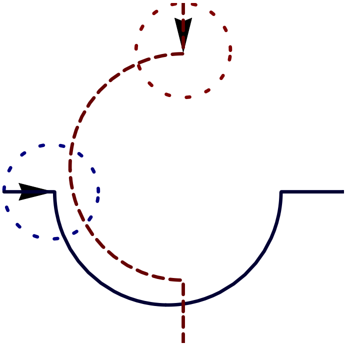
Outline Background

Outline Background

Air Traffic Control

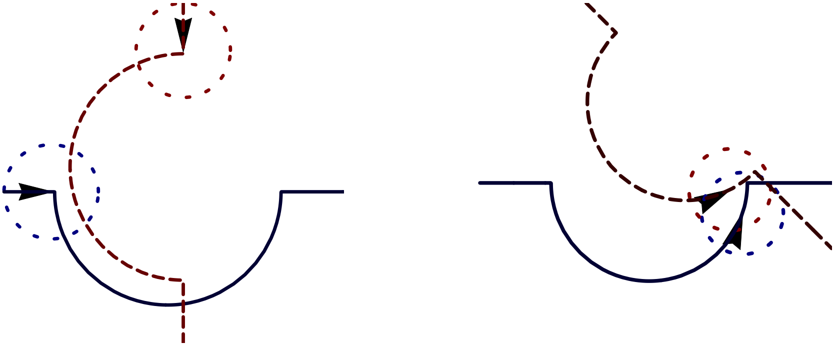






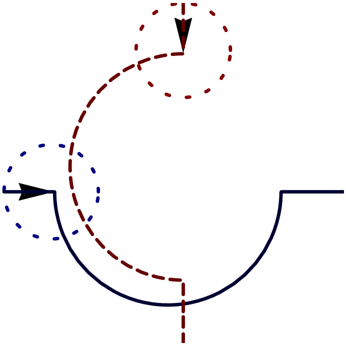
Verification?

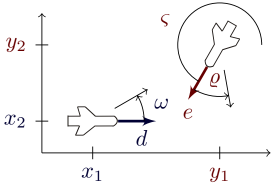
looks correct



Verification?

looks correct NO!

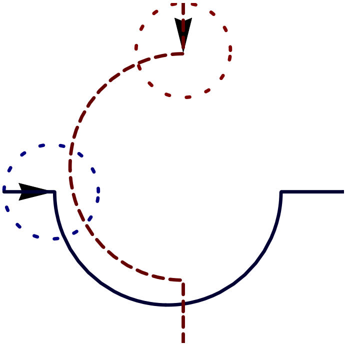


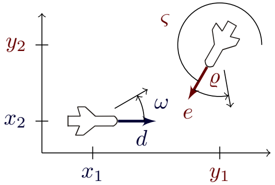


$$\begin{bmatrix} x_1' = -v_1 + v_2 \cos\vartheta + \omega x_2 \\ x_2' = v_2 \sin\vartheta - \omega x_1 \\ \vartheta' = \varpi - \omega \end{bmatrix}$$

Verification?

looks correct NO!

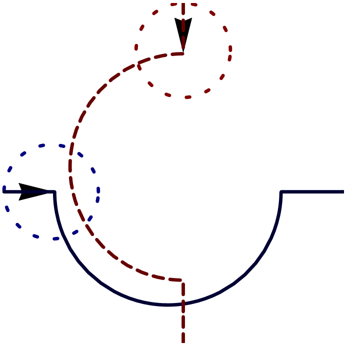


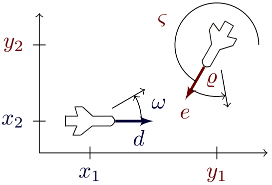


$$\begin{bmatrix} x_1' = -v_1 + v_2 \cos\vartheta + \omega x_2 \\ x_2' = v_2 \sin\vartheta - \omega x_1 \\ \vartheta' = \varpi - \omega \end{bmatrix}$$

Example (“Solving” differential equations)

$$x_1(t) = \frac{1}{\omega\varpi}\big(x_1\omega\varpi \cos t\omega - v_2\omega \cos t\omega \sin\vartheta + v_2\omega \cos t\omega \cos t\varpi \sin\vartheta - v_1\varpi \sin t\omega$$
$$+ x_2\omega\varpi \sin t\omega - v_2\omega \cos\vartheta \cos t\varpi \sin t\omega - v_2\omega\sqrt{1 - \sin\vartheta^2} \sin t\omega$$
$$+ v_2\omega \cos\vartheta \cos t\omega \sin t\varpi + v_2\omega \sin\vartheta \sin t\omega \sin t\varpi\big) \ldots$$





$$\begin{bmatrix} x_1' = -v_1 + v_2 \cos\vartheta + \omega x_2 \\ x_2' = v_2 \sin\vartheta - \omega x_1 \\ \vartheta' = \varpi - \omega \end{bmatrix}$$

Example ("Solving" differential equations)

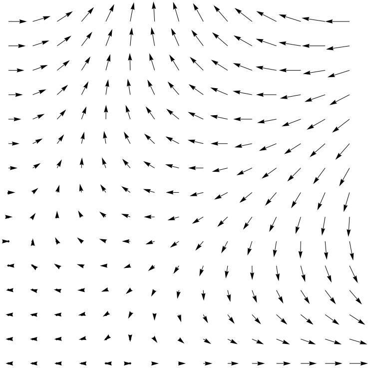
$$\forall t{\geq}0 \quad \frac{1}{\omega\varpi}\Big(x_1\omega\varpi \cos t\omega - v_2\omega \cos t\omega \sin\vartheta + v_2\omega \cos t\omega \cos t\varpi \sin\vartheta - v_1\varpi \sin t\omega$$
$$+ x_2\omega\varpi \sin t\omega - v_2\omega \cos\vartheta \cos t\varpi \sin t\omega - v_2\omega\sqrt{1 - \sin\vartheta^2} \sin t\omega$$
$$+ v_2\omega \cos\vartheta \cos t\omega \sin t\varpi + v_2\omega \sin\vartheta \sin t\omega \sin t\varpi\Big) \ldots$$

Differential Invariants for Differential Equations

"Definition" (Differential Invariant)

Details

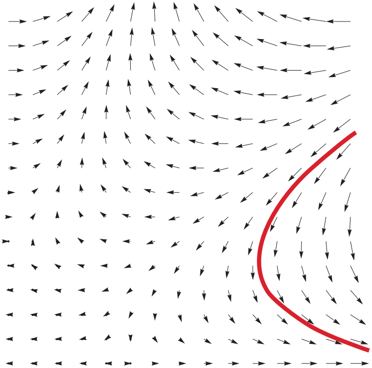
"Formula that remains true in the direction of the dynamics"



"Definition" (Differential Invariant)

Details

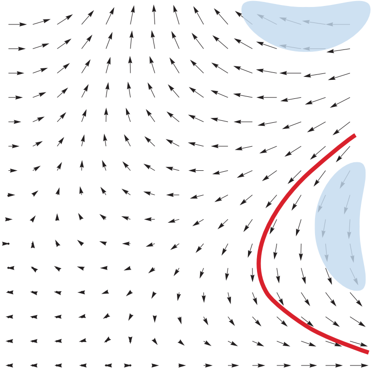
"Formula that remains true in the direction of the dynamics"



"Definition" (Differential Invariant)

▸ Details

"Formula that remains true in the direction of the dynamics"



Differential Induction: Local Dynamics w/o Solutions

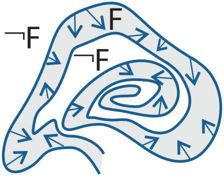
Definition (Differential Invariant) ▸ Details

F closed under total differentiation with respect to differential constraints

André Platzer.
Differential-algebraic dynamic logic for differential-algebraic programs.
J. Log. Comput., 35(1): 309–352, 2010.

Definition (Differential Invariant) ▸ Details

F closed under total differentiation with respect to differential constraints



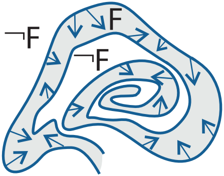
$$\frac{(\chi \to F')}{\chi \to F \to [x' = \theta \,\&\, \chi]F}$$

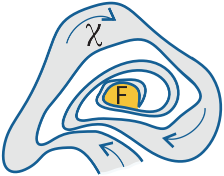
$$\frac{F \to [\alpha]F}{F \to [\alpha^*]F}$$

Definition (Differential Invariant)

Details

F closed under total differentiation with respect to differential constraints

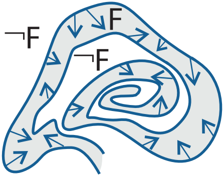


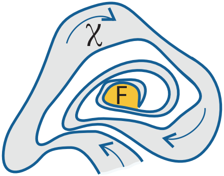


$$\frac{(\chi \rightarrow F')}{\chi \rightarrow F \rightarrow [x' = \theta \,\&\, \chi] F}$$

Definition (Differential Invariant) ▸ Details

F closed under total differentiation with respect to differential constraints



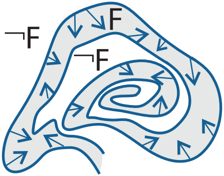


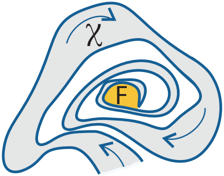
$$\frac{(\chi \to F')}{\chi \to F \to [x' = \theta \,\&\, \chi]F}$$

$$\frac{(\neg F \wedge \chi \to F'_{\gg})}{[x' = \theta \,\&\, \neg F]\chi \to \langle x' = \theta \,\&\, \chi\rangle F}$$

Definition (Differential Invariant) ▸ Details

F closed under total differentiation with respect to differential constraints





$$\frac{(\chi \to F')}{\chi \to F \to [x' = \theta \,\&\, \chi]F}$$

$$\frac{(\neg F \wedge \chi \to F'_{\gg})}{[x' = \theta \,\&\, \neg F]\chi \to \langle x' = \theta \,\&\, \chi\rangle F}$$

Total differential F' of *formulas*?

$$\overline{x^3 \geq -1 \rightarrow [x' = (x-3)^4 + a \,\&\, a \geq 0] x^3 \geq -1}$$

Ex: Nonlinear Dynamics

$$\dfrac{\overline{a \geq 0 \rightarrow 2x^2 x' \geq 0}}{x^3 \geq -1 \rightarrow [x' = (x-3)^4 + a \,\&\, a \geq 0] x^3 \geq -1}$$

$$\dfrac{\dfrac{a \geq 0 \rightarrow 2x^2((x-3)^4 + a) \geq 0}{a \geq 0 \rightarrow 2x^2 x' \geq 0}}{x^3 \geq -1 \rightarrow [x' = (x-3)^4 + a \,\&\, a \geq 0] x^3 \geq -1}$$

$$\dfrac{\dfrac{\dfrac{*}{a \geq 0 \rightarrow 2x^2((x-3)^4 + a) \geq 0}}{a \geq 0 \rightarrow 2x^2 x' \geq 0}}{x^3 \geq -1 \rightarrow [x' = (x-3)^4 + a \,\&\, a \geq 0] x^3 \geq -1}$$

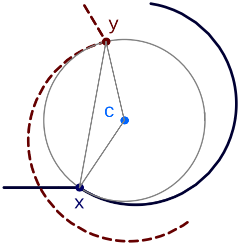
$$\overline{2x^3 \geq \frac{1}{4} \rightarrow [x' = x^2 + x^4] 2x^3 \geq \frac{1}{4}}$$

$$\dfrac{\overline{\quad 6x^2x' \geq 0 \quad}}{2x^3 \geq \frac{1}{4} \rightarrow [x' = x^2 + x^4] 2x^3 \geq \frac{1}{4}}$$

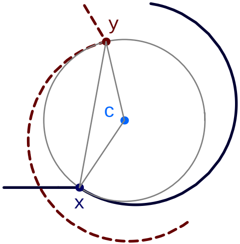
$$\cfrac{\cfrac{\overline{6x^2(x^2+x^4)\geq 0}}{6x^2x'\geq 0}}{2x^3\geq\frac{1}{4}\rightarrow[x'=x^2+x^4]2x^3\geq\frac{1}{4}}$$

$$\dfrac{\dfrac{\dfrac{*}{6x^2(x^2+x^4)\geq 0}}{6x^2x'\geq 0}}{2x^3\geq \frac{1}{4}\rightarrow[x'=x^2+x^4]2x^3\geq\frac{1}{4}}$$

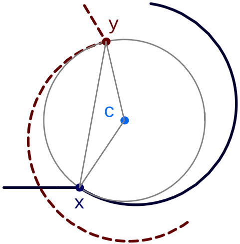
$$\frac{}{[x_1' = d_1, d_1' = -\omega d_2, x_2' = d_2, d_2' = \omega d_1, ..](x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2}$$



$$\frac{\frac{\partial\|x-y\|^2}{\partial x_1}x_1' + \frac{\partial\|x-y\|^2}{\partial y_1}y_1' + \frac{\partial\|x-y\|^2}{\partial x_2}x_2' + \frac{\partial\|x-y\|^2}{\partial y_2}y_2' \geq \frac{\partial p^2}{\partial x_1}x_1' \ldots}{[x_1' = d_1, d_1' = -\omega d_2, x_2' = d_2, d_2' = \omega d_1, ..](x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2}$$

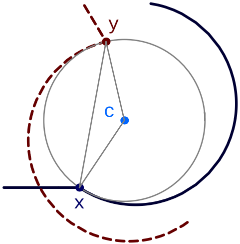


$$\frac{\frac{\partial\|x-y\|^2}{\partial x_1}x_1' + \frac{\partial\|x-y\|^2}{\partial y_1}y_1' + \frac{\partial\|x-y\|^2}{\partial x_2}x_2' + \frac{\partial\|x-y\|^2}{\partial y_2}y_2' \geq \frac{\partial p^2}{\partial x_1}x_1' \ldots}{[x_1' = d_1, d_1' = -\omega d_2, x_2' = d_2, d_2' = \omega d_1, ..](x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2}$$



$$\frac{\phantom{\frac{\partial\|x-y\|^2}{\partial x_1}}}{\frac{\partial\|x-y\|^2}{\partial x_1}d_1+\frac{\partial\|x-y\|^2}{\partial y_1}e_1+\frac{\partial\|x-y\|^2}{\partial x_2}d_2+\frac{\partial\|x-y\|^2}{\partial y_2}e_2\geq\frac{\partial p^2}{\partial x_1}d_1\ldots}$$

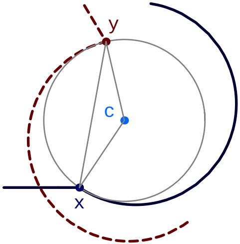
$$[x_1'=d_1,d_1'=-\omega d_2,x_2'=d_2,d_2'=\omega d_1,..](x_1-y_1)^2+(x_2-y_2)^2\geq p^2$$

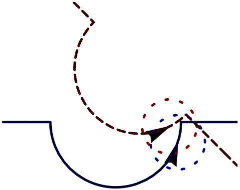


$$2(x_1 - y_1)(d_1 - e_1) + 2(x_2 - y_2)(d_2 - e_2) \geq 0$$

$$\frac{\partial\|x-y\|^2}{\partial x_1} d_1 + \frac{\partial\|x-y\|^2}{\partial y_1} e_1 + \frac{\partial\|x-y\|^2}{\partial x_2} d_2 + \frac{\partial\|x-y\|^2}{\partial y_2} e_2 \geq \frac{\partial p^2}{\partial x_1} d_1 \ldots$$

$$[x_1' = d_1, d_1' = -\omega d_2, x_2' = d_2, d_2' = \omega d_1, ..](x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2$$

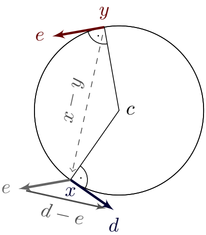


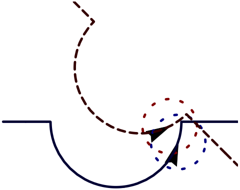


$$2(x_1 - y_1)(d_1 - e_1) + 2(x_2 - y_2)(d_2 - e_2) \geq 0$$

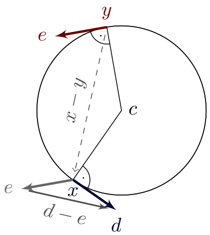
$$\frac{\partial\|x-y\|^2}{\partial x_1}d_1 + \frac{\partial\|x-y\|^2}{\partial y_1}e_1 + \frac{\partial\|x-y\|^2}{\partial x_2}d_2 + \frac{\partial\|x-y\|^2}{\partial y_2}e_2 \geq \frac{\partial p^2}{\partial x_1}d_1 \dots$$

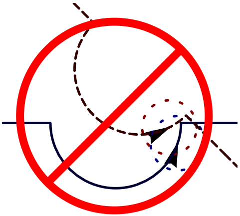
$$[x_1' = d_1, d_1' = -\omega d_2, x_2' = d_2, d_2' = \omega d_1, ..](x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2$$





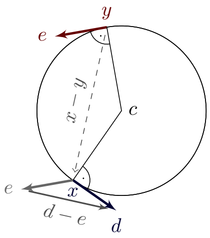
$$\dfrac{\dfrac{\dfrac{2(x_1-y_1)(d_1-e_1)+2(x_2-y_2)(d_2-e_2)\geq 0}{\frac{\partial\|x-y\|^2}{\partial x_1}d_1+\frac{\partial\|x-y\|^2}{\partial y_1}e_1+\frac{\partial\|x-y\|^2}{\partial x_2}d_2+\frac{\partial\|x-y\|^2}{\partial y_2}e_2\geq\frac{\partial p^2}{\partial x_1}d_1\dots}}{[x_1'=d_1,d_1'=-\omega d_2,x_2'=d_2,d_2'=\omega d_1,..](x_1-y_1)^2+(x_2-y_2)^2\geq p^2}}{}$$





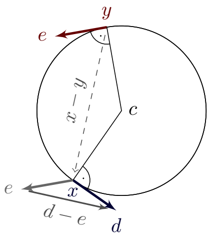
$$\overline{..\rightarrow[d_1'=-\omega d_2,e_1'=-\omega e_2,x_2'=d_2,d_2'=\omega d_1,..]d_1-e_1=-\omega(x_2-y_2)}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{[x_1' = d_1, d_1' = -\omega d_2, x_2' = d_2, d_2' = \omega d_1, ..](x_1-y_1)^2 + (x_2-y_2)^2 \geq p^2}}{\frac{\partial\|x-y\|^2}{\partial x_1} d_1 + \frac{\partial\|x-y\|^2}{\partial y_1} e_1 + \frac{\partial\|x-y\|^2}{\partial x_2} d_2 + \frac{\partial\|x-y\|^2}{\partial y_2} e_2 \geq \frac{\partial p^2}{\partial x_1} d_1 \ldots}}{2(x_1-y_1)(d_1-e_1) + 2(x_2-y_2)(d_2-e_2) \geq 0}}{2(x_1-y_1)(-\omega(x_2-y_2)) + 2(x_2-y_2)\omega(x_1-y_1) \geq 0}$$



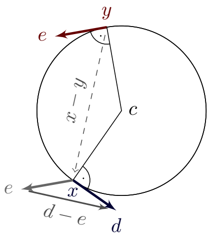
$$\overline{.. \rightarrow [d_1' = -\omega d_2, e_1' = -\omega e_2, x_2' = d_2, d_2' = \omega d_1, ..] d_1 - e_1 = -\omega(x_2 - y_2)}$$

$$\frac{\dfrac{\dfrac{2(x_1-y_1)(-\omega(x_2-y_2))+2(x_2-y_2)\omega(x_1-y_1)\geq 0}{2(x_1-y_1)(d_1-e_1)+2(x_2-y_2)(d_2-e_2)\geq 0}}{\frac{\partial\|x-y\|^2}{\partial x_1}d_1+\frac{\partial\|x-y\|^2}{\partial y_1}e_1+\frac{\partial\|x-y\|^2}{\partial x_2}d_2+\frac{\partial\|x-y\|^2}{\partial y_2}e_2\geq\frac{\partial p^2}{\partial x_1}d_1\ldots}}{[x_1'=d_1,d_1'=-\omega d_2,x_2'=d_2,d_2'=\omega d_1,..](x_1-y_1)^2+(x_2-y_2)^2\geq p^2}$$



$$\frac{\frac{\partial(d_1-e_1)}{\partial d_1}d_1'+\frac{\partial(d_1-e_1)}{\partial e_1}e_1'=-\frac{\partial\omega(x_2-y_2)}{\partial x_2}x_2'-\frac{\partial\omega(x_2-y_2)}{\partial y_2}y_2'}{..\to[d_1'=-\omega d_2,e_1'=-\omega e_2,x_2'=d_2,d_2'=\omega d_1,..]\,d_1-e_1=-\omega(x_2-y_2)}$$

$$\dfrac{\dfrac{\dfrac{2(x_1-y_1)(-\omega(x_2-y_2))+2(x_2-y_2)\omega(x_1-y_1)\geq 0}{2(x_1-y_1)(d_1-e_1)+2(x_2-y_2)(d_2-e_2)\geq 0}}{\frac{\partial\|x-y\|^2}{\partial x_1}d_1+\frac{\partial\|x-y\|^2}{\partial y_1}e_1+\frac{\partial\|x-y\|^2}{\partial x_2}d_2+\frac{\partial\|x-y\|^2}{\partial y_2}e_2\geq\frac{\partial p^2}{\partial x_1}d_1\dots}}{[x_1'=d_1,d_1'=-\omega d_2,x_2'=d_2,d_2'=\omega d_1,..](x_1-y_1)^2+(x_2-y_2)^2\geq p^2}$$



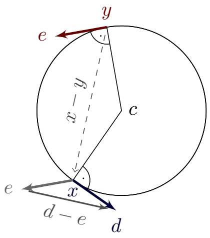
$$\dfrac{\dfrac{}{\frac{\partial(d_1-e_1)}{\partial d_1}d_1'+\frac{\partial(d_1-e_1)}{\partial e_1}e_1'=-\frac{\partial\omega(x_2-y_2)}{\partial x_2}x_2'-\frac{\partial\omega(x_2-y_2)}{\partial y_2}y_2'}}{..\rightarrow[d_1'=-\omega d_2,e_1'=-\omega e_2,x_2'=d_2,d_2'=\omega d_1,..]d_1-e_1=-\omega(x_2-y_2)}$$

$$2(x_1-y_1)(-\omega(x_2-y_2))+2(x_2-y_2)\omega(x_1-y_1)\geq 0$$

$$2(x_1-y_1)(d_1-e_1)+2(x_2-y_2)(d_2-e_2)\geq 0$$

$$\frac{\partial\|x-y\|^2}{\partial x_1}d_1+\frac{\partial\|x-y\|^2}{\partial y_1}e_1+\frac{\partial\|x-y\|^2}{\partial x_2}d_2+\frac{\partial\|x-y\|^2}{\partial y_2}e_2\geq\frac{\partial p^2}{\partial x_1}d_1\dots$$

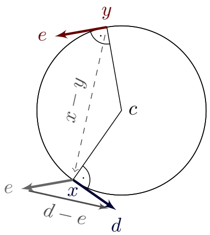
$$[x_1'=d_1,d_1'=-\omega d_2,x_2'=d_2,d_2'=\omega d_1,..](x_1-y_1)^2+(x_2-y_2)^2\geq p^2$$



$$\frac{\partial(d_1-e_1)}{\partial d_1}(-\omega d_2)+\frac{\partial(d_1-e_1)}{\partial e_1}(-\omega e_2)=-\frac{\partial\omega(x_2-y_2)}{\partial x_2}d_2-\frac{\partial\omega(x_2-y_2)}{\partial y_2}e_2$$

$$..\rightarrow[d_1'=-\omega d_2,e_1'=-\omega e_2,x_2'=d_2,d_2'=\omega d_1,..]d_1-e_1=-\omega(x_2-y_2)$$

$$\cfrac{\cfrac{\cfrac{2(x_1-y_1)(-\omega(x_2-y_2))+2(x_2-y_2)\omega(x_1-y_1)\geq 0}{2(x_1-y_1)(d_1-e_1)+2(x_2-y_2)(d_2-e_2)\geq 0}}{\frac{\partial\|x-y\|^2}{\partial x_1}d_1+\frac{\partial\|x-y\|^2}{\partial y_1}e_1+\frac{\partial\|x-y\|^2}{\partial x_2}d_2+\frac{\partial\|x-y\|^2}{\partial y_2}e_2\geq\frac{\partial p^2}{\partial x_1}d_1\dots}}{[x_1'=d_1,d_1'=-\omega d_2,x_2'=d_2,d_2'=\omega d_1,..](x_1-y_1)^2+(x_2-y_2)^2\geq p^2}$$



$$\cfrac{\cfrac{-\omega d_2+\omega e_2=-\omega(d_2-e_2)}{\frac{\partial(d_1-e_1)}{\partial d_1}(-\omega d_2)+\frac{\partial(d_1-e_1)}{\partial e_1}(-\omega e_2)=-\frac{\partial\omega(x_2-y_2)}{\partial x_2}d_2-\frac{\partial\omega(x_2-y_2)}{\partial y_2}e_2}}{..\to[d_1'=-\omega d_2,e_1'=-\omega e_2,x_2'=d_2,d_2'=\omega d_1,..]d_1-e_1=-\omega(x_2-y_2)}$$

$$\cfrac{\cfrac{\cfrac{2(x_1 - y_1)(-\omega(x_2 - y_2)) + 2(x_2 - y_2)\omega(x_1 - y_1) \geq 0}{2(x_1 - y_1)(d_1 - e_1) + 2(x_2 - y_2)(d_2 - e_2) \geq 0}}{\frac{\partial\|x-y\|^2}{\partial x_1} d_1 + \frac{\partial\|x-y\|^2}{\partial y_1} e_1 + \frac{\partial\|x-y\|^2}{\partial x_2} d_2 + \frac{\partial\|x-y\|^2}{\partial y_2} e_2 \geq \frac{\partial p^2}{\partial x_1} d_1 \ldots}}{[x_1' = d_1, d_1' = -\omega d_2, x_2' = d_2, d_2' = \omega d_1, ..](x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2}$$

Proposition (Differential cut saturation)

F differential invariant of $[x' = \theta \,\&\, H]\phi$, then

$$[x' = \theta \,\&\, H]\phi \quad \text{iff} \quad [x' = \theta \,\&\, H \land F]\phi$$

$$\cfrac{\cfrac{-\omega d_2 + \omega e_2 = -\omega(d_2 - e_2)}{\frac{\partial(d_1 - e_1)}{\partial d_1}(-\omega d_2) + \frac{\partial(d_1 - e_1)}{\partial e_1}(-\omega e_2) = -\frac{\partial\omega(x_2 - y_2)}{\partial x_2} d_2 - \frac{\partial\omega(x_2 - y_2)}{\partial y_2} e_2}}{.. \to [d_1' = -\omega d_2, e_1' = -\omega e_2, x_2' = d_2, d_2' = \omega d_1, ..]\, d_1 - e_1 = -\omega(x_2 - y_2)}$$

$$\dfrac{\dfrac{\dfrac{2(x_1-y_1)(-\omega(x_2-y_2))+2(x_2-y_2)\omega(x_1-y_1)\geq 0}{2(x_1-y_1)(d_1-e_1)+2(x_2-y_2)(d_2-e_2)\geq 0}}{\frac{\partial\|x-y\|^2}{\partial x_1}d_1+\frac{\partial\|x-y\|^2}{\partial y_1}e_1+\frac{\partial\|x-y\|^2}{\partial x_2}d_2+\frac{\partial\|x-y\|^2}{\partial y_2}e_2\geq\frac{\partial p^2}{\partial x_1}d_1\ldots}}{[x_1'=d_1,d_1'=-\omega d_2,x_2'=d_2,d_2'=\omega d_1,..](x_1-y_1)^2+(x_2-y_2)^2\geq p^2}$$

refine dynamics

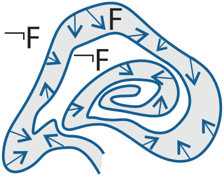
by differential cut

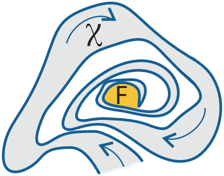
$$\dfrac{\dfrac{-\omega d_2+\omega e_2=-\omega(d_2-e_2)}{\frac{\partial(d_1-e_1)}{\partial d_1}(-\omega d_2)+\frac{\partial(d_1-e_1)}{\partial e_1}(-\omega e_2)=-\frac{\partial\omega(x_2-y_2)}{\partial x_2}d_2-\frac{\partial\omega(x_2-y_2)}{\partial y_2}e_2}}{..\to[d_1'=-\omega d_2,e_1'=-\omega e_2,x_2'=d_2,d_2'=\omega d_1,..]d_1-e_1=-\omega(x_2-y_2)}$$

Definition (Differential Invariant)

Details

F closed under total differentiation with respect to differential constraints

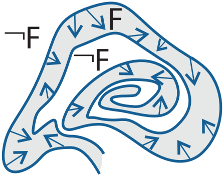


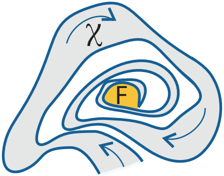


$$d_1 \geq d_2 \rightarrow [x := a^2 + 1;$$
$$d_1' = -\omega d_2, d_2' = \omega d_1$$
$$]\, d_1 \geq d_2$$

Definition (Differential Invariant) Details

F closed under total differentiation with respect to differential constraints

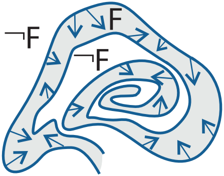


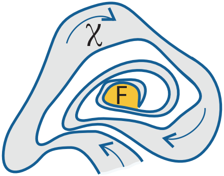


$$d_1 \geq d_2 \rightarrow [x := a^2 + 1; \; (d_1' = -\omega d_2 \wedge d_2' = \omega d_1) \vee (d_1' \leq 2d_1) \;] \, d_1 \geq d_2$$

Definition (Differential Invariant) ▸ Details

F closed under total differentiation with respect to differential constraints



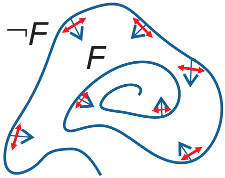


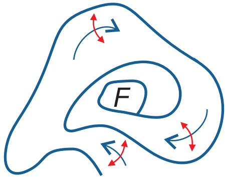
$$d_1 \geq d_2 \rightarrow [x := a^2 + 1;$$
$$\exists \omega \, (\omega \leq 1 \land d_1' = -\omega d_2 \land d_2' = \omega d_1) \lor (d_1' \leq 2 d_1)$$
$$]\, d_1 \geq d_2$$

Definition (Differential Invariant)

Details

F closed under total differentiation with respect to differential constraints





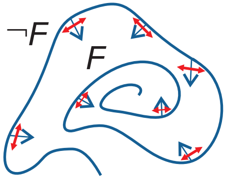
$$d_1 \geq d_2 \rightarrow [x := a^2 + 1;$$
$$\exists \omega\, (\omega \leq 1 \land d_1' = -\omega d_2 \land d_2' = \omega d_1) \lor (d_1' \leq 2 d_1)$$
$$]\, d_1 \geq d_2$$

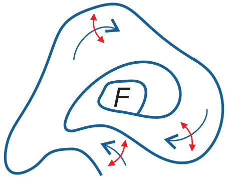
- quantified nondeterminism/disturbance

Definition (Differential Invariant)

Details

F closed under total differentiation with respect to differential constraints





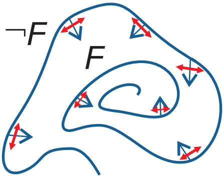
$$d_1 \geq d_2 \rightarrow [x := a^2 + 1;\\ \exists \omega\, (\omega \leq 1 \wedge d_1' = -\omega d_2 \wedge d_2' = \omega d_1) \vee (d_1' \leq 2 d_1)\\ ]\, d_1 \geq d_2$$

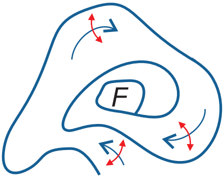
- quantified nondeterminism/disturbance

Definition (Differential Invariant)

Details

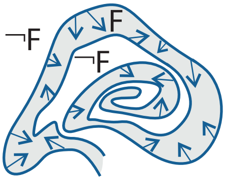
F closed under total differentiation with respect to differential constraints

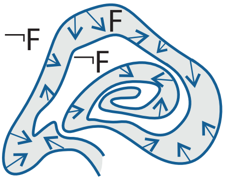




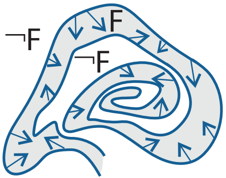
$$d_1 \geq d_2 \rightarrow [x > 0 \rightarrow \exists a\,(a < 5 \wedge x := a^2 + 1);\ \exists \omega\,(\omega \leq 1 \wedge d_1' = -\omega d_2 \wedge d_2' = \omega d_1) \vee (d_1' \leq 2d_1)\ ]\, d_1 \geq d_2$$

- discrete quantified nondeterminism/disturbance

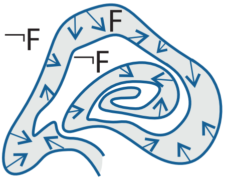




$$\frac{(H \to F')}{(H \to F) \to [x' = \theta \,\&\, H]F}$$

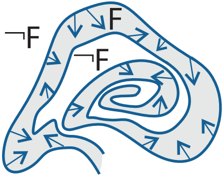


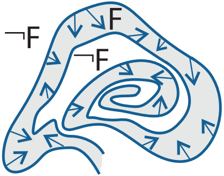
$$\frac{(H \to F')}{(H \to F) \to [x' = \theta \,\&\, H]F}$$



$$\frac{({\color{red}F} \land H \to F')}{(H \to F) \to [x' = \theta \,\&\, H]F}$$

Assuming Differential Invariance





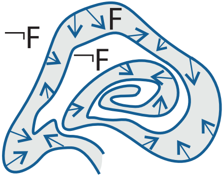
$$\frac{(H \to F')}{(H \to F) \to [x' = \theta \,\&\, H]F}$$

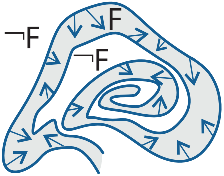
$$\frac{(F \land H \to F')}{(H \to F) \to [x' = \theta \,\&\, H]F}$$

Example (Restrictions)

$$\frac{}{x^2 - 6x + 9 = 0 \to [x' = y, y' = -x]x^2 - 6x + 9 = 0}$$

Assuming Differential Invariance





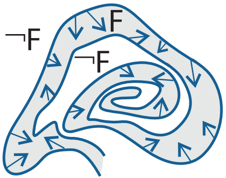
$$\frac{(H \rightarrow F')}{(H \rightarrow F) \rightarrow [x' = \theta \,\&\, H]F}$$

$$\frac{(F \land H \rightarrow F')}{(H \rightarrow F) \rightarrow [x' = \theta \,\&\, H]F}$$

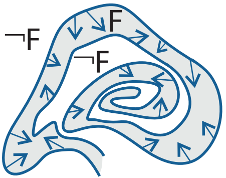
Example (Restrictions)

$$\frac{\dfrac{}{x^2 - 6x + 9 = 0 \rightarrow y\frac{\partial(x^2-6x+9)}{\partial x} - x\frac{\partial(x^2-6x+9)}{\partial y} = 0}}{x^2 - 6x + 9 = 0 \rightarrow [x' = y, y' = -x]x^2 - 6x + 9 = 0}$$

Assuming Differential Invariance



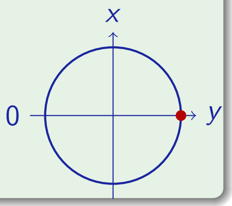
$$\frac{(H \to F')}{(H \to F) \to [x' = \theta \,\&\, H]F}$$

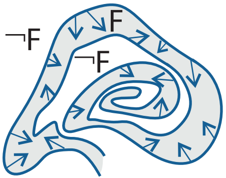


$$\frac{(F \land H \to F')}{(H \to F) \to [x' = \theta \,\&\, H]F}$$

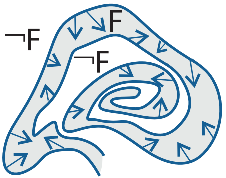
Example (Restrictions)

$$\frac{\dfrac{x^2 - 6x + 9 = 0 \to y2x - 6y = 0}{x^2 - 6x + 9 = 0 \to y\frac{\partial(x^2-6x+9)}{\partial x} - x\frac{\partial(x^2-6x+9)}{\partial y} = 0}}{x^2 - 6x + 9 = 0 \to [x' = y, y' = -x]x^2 - 6x + 9 = 0}$$





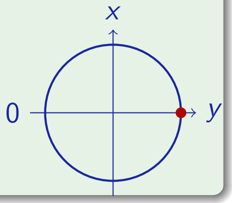
$$\frac{(H \to F')}{(H \to F) \to [x' = \theta \,\&\, H]F}$$

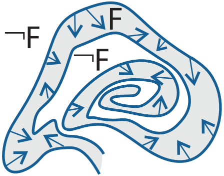


$$\frac{(F \land H \to F')}{(H \to F) \to [x' = \theta \,\&\, H]F}$$

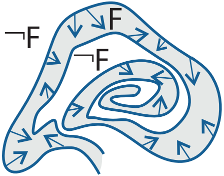
Example (Restrictions are unsound!)

$$\frac{\dfrac{x^2 - 6x + 9 = 0 \to y2x - 6y = 0}{x^2 - 6x + 9 = 0 \to y\frac{\partial(x^2-6x+9)}{\partial x} - x\frac{\partial(x^2-6x+9)}{\partial y} = 0}}{x^2 - 6x + 9 = 0 \to [x' = y, y' = -x]x^2 - 6x + 9 = 0}$$





$$\frac{(H \to F')}{(H \to F)\to[x' = \theta \,\&\, H]F}$$

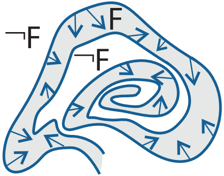


$$\frac{(F \land H \to F')}{(H \to F)\to[x' = \theta \,\&\, H]F}$$

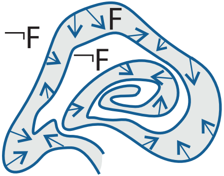
Example (Restrictions)

$$\frac{(x^2 \leq 0 \to 2x \cdot 1 \leq 0)}{x^2 \leq 0 \to [x' = 1]x^2 \leq 0}$$

Assuming Differential Invariance



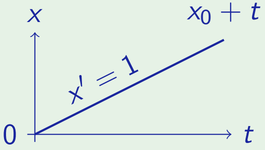
$$\frac{(H \to F')}{(H \to F) \to [x' = \theta \,\&\, H]F}$$



$$\frac{(F \land H \to F')}{(H \to F) \to [x' = \theta \,\&\, H]F}$$

Example (Restrictions are unsound!)

$$\frac{(x^2 \leq 0 \to 2x \cdot 1 \leq 0)}{x^2 \leq 0 \to [x' = 1]x^2 \leq 0}$$



Differential Invariance of Negative Equations

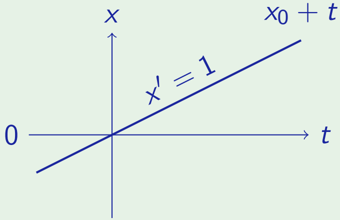
Example (Negative equations)

$$\dfrac{\dfrac{*}{\forall x\,(1 \neq 0)}}{x \neq 0 \rightarrow [x' = 1]x \neq 0}$$

Differential Invariance of Negative Equations

Example (Negative equations)

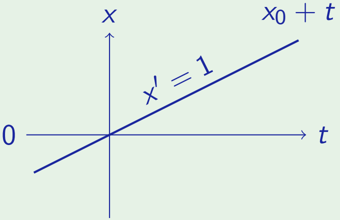
$$\dfrac{\dfrac{*}{\forall x\,(1 \neq 0)}}{x \neq 0 \rightarrow [x' = 1]x \neq 0}$$



Differential Invariance of Negative Equations

Example (Negative equations are unsound!)

$$\dfrac{\dfrac{*}{\forall x\,(1 \neq 0)}}{x \neq 0 \rightarrow [x' = 1]x \neq 0}$$



Disjunctive Differential Invariants

$$F \land G' \equiv$$

Disjunctive Differential Invariants

$$F \land G' \equiv F' \land G'$$

Disjunctive Differential Invariants

$$F \land G' \equiv F' \land G'$$
$$F \lor G' \equiv$$

Disjunctive Differential Invariants

$$F \wedge G' \equiv F' \wedge G'$$
$$F \vee G' \equiv F' \vee G' \; ?$$

Disjunctive Differential Invariants

$$F \wedge G' \equiv F' \wedge G'$$
$$F \vee G' \equiv F' \vee G' \ ?$$

Example (Provable)

$$d_1^2 + d_2^2 = v^2 \rightarrow [d_1' = -\omega d_2, d_2' = \omega d_1]\, d_1^2 + d_2^2 = v^2$$

Disjunctive Differential Invariants

$$F \wedge G' \equiv F' \wedge G'$$
$$F \vee G' \equiv F' \vee G' \ ?$$

Example (Provable)

$$d_1^2 + d_2^2 = v^2 \rightarrow [d_1' = -\omega d_2, d_2' = \omega d_1]\, d_1^2 + d_2^2 = v^2$$

Example (Consequence)

$$x_1 \geq 0 \vee d_1^2 + d_2^2 = v^2 \rightarrow [d_1' = -\omega d_2, d_2' = \omega d_1](x_1 \geq 0 \vee d_1^2 + d_2^2 = v^2)$$

Disjunctive Differential Invariants

$$F \wedge G' \equiv F' \wedge G'$$
$$F \vee G' \equiv F' \vee G' \; ?$$

Example (Provable)

$$d_1^2 + d_2^2 = v^2 \rightarrow [d_1' = -\omega d_2, d_2' = \omega d_1]\, d_1^2 + d_2^2 = v^2$$

Example (Unsound!)

$$x_1 \geq 0 \vee d_1^2 + d_2^2 = v^2 \rightarrow [d_1' = -\omega d_2, d_2' = \omega d_1](x_1 \geq 0 \vee d_1^2 + d_2^2 = v^2)$$

Disjunctive Differential Invariants

$$F \land G' \equiv F' \land G'$$
$$F \lor G' \equiv F' \land G' \;!$$

Example (Provable)

$$d_1^2 + d_2^2 = v^2 \to [d_1' = -\omega d_2, d_2' = \omega d_1]\, d_1^2 + d_2^2 = v^2$$

Example (Unsound!)

$$x_1 \geq 0 \lor d_1^2 + d_2^2 = v^2 \to [d_1' = -\omega d_2, d_2' = \omega d_1](x_1 \geq 0 \lor d_1^2 + d_2^2 = v^2)$$

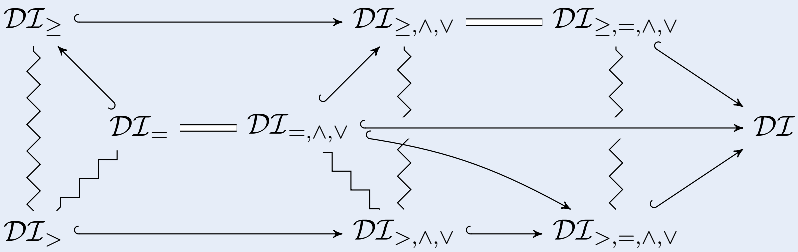
Outline Background

The Structure of Differential Invariants

Theorem (Closure properties of differential invariants)

Closed under conjunction, differentiation, and propositional equivalences.

Theorem (Differential Invariance Chart)



André Platzer.
The structure of differential invariants and differential cut elimination.
Logical Methods in Computer Science, 2012.

Differential Cuts

$$\frac{F \rightarrow [x' = \theta \,\&\, H]C \qquad F \rightarrow [x' = \theta \,\&\, (H \wedge C)]F}{F \rightarrow [x' = \theta \,\&\, H]F}$$

André Platzer.
The structure of differential invariants and differential cut elimination.
Logical Methods in Computer Science, 2012.

Ex: Differential Cuts

$$\frac{}{x^3 \geq -1 \land y^5 \geq 0 \rightarrow [x' = (x-3)^4 + y^5, y' = y^2] x^3 \geq -1}$$

Ex: Differential Cuts

$$\frac{}{x^3 \geq -1 \land y^5 \geq 0 \rightarrow [x' = (x-3)^4 + y^5, y' = y^2] x^3 \geq -1}$$

$$\frac{}{y^5 \geq 0 \rightarrow [x' = (x-3)^4 + y^5, y' = y^2] y^5 \geq 0}$$

$$\frac{}{x^3 \geq -1 \land y^5 \geq 0 \rightarrow [x' = (x-3)^4 + y^5, y' = y^2] x^3 \geq -1}$$

$$\frac{\overline{5y^4 y' \geq 0}}{y^5 \geq 0 \rightarrow [x' = (x-3)^4 + y^5, y' = y^2] y^5 \geq 0}$$

$$\overline{x^3 \geq -1 \land y^5 \geq 0 \rightarrow [x' = (x-3)^4 + y^5, y' = y^2] x^3 \geq -1}$$

$$\dfrac{\dfrac{\overline{5y^4 y^2 \geq 0}}{5y^4 y' \geq 0}}{y^5 \geq 0 \rightarrow [x' = (x-3)^4 + y^5, y' = y^2] y^5 \geq 0}$$

Ex: Differential Cuts

$$\overline{x^3 \geq -1 \land y^5 \geq 0 \rightarrow [x' = (x-3)^4 + y^5, y' = y^2] x^3 \geq -1}$$

$$\dfrac{\dfrac{\dfrac{*}{5y^4 y^2 \geq 0}}{5y^4 y' \geq 0}}{y^5 \geq 0 \rightarrow [x' = (x-3)^4 + y^5, y' = y^2] y^5 \geq 0}$$

$$\dfrac{x^3 \geq -1 \rightarrow [x' = (x-3)^4 + y^5, y' = y^2 \,\&\, y^5 \geq 0] x^3 \geq -1 \quad \triangleright}{x^3 \geq -1 \land y^5 \geq 0 \rightarrow [x' = (x-3)^4 + y^5, y' = y^2] x^3 \geq -1}$$

$$\dfrac{\dfrac{\dfrac{*}{5y^4 {\color{red}y^2} \geq 0}}{5y^4 {\color{red}y'} \geq 0}}{y^5 \geq 0 \rightarrow [x' = (x-3)^4 + y^5, y' = y^2] y^5 \geq 0}$$

$$\dfrac{\dfrac{\dfrac{}{y^5 \geq 0 \rightarrow 2x^2 x' \geq 0}}{x^3 \geq -1 \rightarrow [x' = (x-3)^4 + y^5, y' = y^2 \,\&\, y^5 \geq 0]x^3 \geq -1} \triangleright}{x^3 \geq -1 \land y^5 \geq 0 \rightarrow [x' = (x-3)^4 + y^5, y' = y^2]x^3 \geq -1}$$

$$\dfrac{\dfrac{\dfrac{*}{5y^4 y^2 \geq 0}}{5y^4 y' \geq 0}}{y^5 \geq 0 \rightarrow [x' = (x-3)^4 + y^5, y' = y^2]y^5 \geq 0}$$

$$\dfrac{\dfrac{\dfrac{\overline{y^5 \geq 0 \rightarrow 2x^2((x-3)^4 + y^5) \geq 0}}{y^5 \geq 0 \rightarrow 2x^2 x' \geq 0}}{x^3 \geq -1 \rightarrow [x' = (x-3)^4 + y^5, y' = y^2 \,\&\, y^5 \geq 0]x^3 \geq -1} \quad \triangleright}{x^3 \geq -1 \land y^5 \geq 0 \rightarrow [x' = (x-3)^4 + y^5, y' = y^2]x^3 \geq -1}$$

$$\dfrac{\dfrac{\dfrac{*}{5y^4 y^2 \geq 0}}{5y^4 y' \geq 0}}{y^5 \geq 0 \rightarrow [x' = (x-3)^4 + y^5, y' = y^2]y^5 \geq 0}$$

$$\dfrac{\dfrac{\dfrac{*}{y^5 \geq 0 \to 2x^2((x-3)^4 + y^5) \geq 0}}{y^5 \geq 0 \to 2x^2 x' \geq 0}}{\dfrac{x^3 \geq -1 \to [x' = (x-3)^4 + y^5, y' = y^2 \,\&\, y^5 \geq 0]x^3 \geq -1 \quad \triangleright}{x^3 \geq -1 \land y^5 \geq 0 \to [x' = (x-3)^4 + y^5, y' = y^2]x^3 \geq -1}}$$

$$\dfrac{\dfrac{\dfrac{*}{5y^4 y^2 \geq 0}}{5y^4 y' \geq 0}}{y^5 \geq 0 \to [x' = (x-3)^4 + y^5, y' = y^2]y^5 \geq 0}$$

Differential Cuts

$$\frac{F \rightarrow [x' = \theta \,\&\, H]C \qquad F \rightarrow [x' = \theta \,\&\, (H \wedge C)]F}{F \rightarrow [x' = \theta \,\&\, H]F}$$

André Platzer.
The structure of differential invariants and differential cut elimination.
Logical Methods in Computer Science, 2012.

Differential Cuts

$$\frac{F \rightarrow [x' = \theta \,\&\, H]C \qquad F \rightarrow [x' = \theta \,\&\, (H \land C)]F}{F \rightarrow [x' = \theta \,\&\, H]F}$$

Theorem (Gentzen's Cut Elimination)

$$\frac{A \rightarrow B \lor C \qquad A \land C \rightarrow B}{A \rightarrow B}$$ *cut can be eliminated*

André Platzer.
The structure of differential invariants and differential cut elimination.
Logical Methods in Computer Science, 2012.

Differential Cuts

$$\frac{F \rightarrow [x' = \theta \,\&\, H]C \qquad F \rightarrow [x' = \theta \,\&\, (H \land C)]F}{F \rightarrow [x' = \theta \,\&\, H]F}$$

Theorem (Gentzen's Cut Elimination)

$$\frac{A \rightarrow B \lor C \quad A \land C \rightarrow B}{A \rightarrow B}$$ *cut can be eliminated*

Theorem (No Differential Cut Elimination)

Deductive power with differential cut exceeds deductive power without.

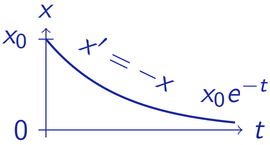
$$\mathcal{DCI} > \mathcal{DI}$$

André Platzer.
The structure of differential invariants and differential cut elimination.
Logical Methods in Computer Science, 2012.

Ex: Exponentials

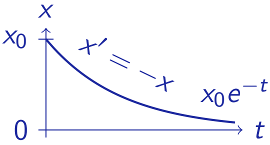
Counterexample ()

$$\overline{x > 0 \rightarrow [x' = -x]x > 0}$$



Counterexample ()

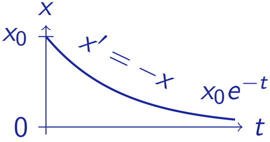
$$\dfrac{\overline{\quad x' > 0 \quad}}{x > 0 \rightarrow [x' = -x]x > 0}$$



Ex: Exponentials

Counterexample ()

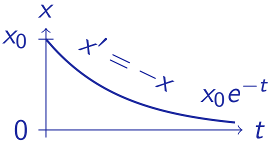
$$\cfrac{\cfrac{\cfrac{}{-x > 0}}{x' > 0}}{x > 0 \to [x' = -x]x > 0}$$



Ex: Exponentials

Counterexample (Cannot prove)

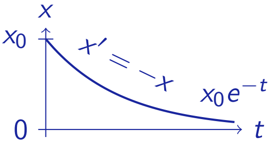
$$\dfrac{\dfrac{\dfrac{\text{not valid}}{-x > 0}}{x' > 0}}{x > 0 \rightarrow [x' = -x]x > 0}$$



Differential Auxiliaries

Example (Successful proof)

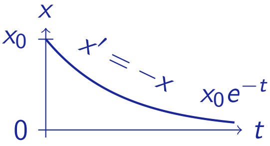
$$\frac{}{x > 0 \rightarrow [x' = -x]x > 0}$$



Differential Auxiliaries

Example (Successful proof)

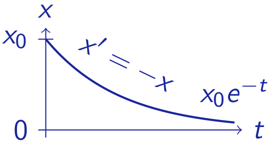
$$\dfrac{\dfrac{}{x > 0 \leftrightarrow \exists y\, xy^2 = 1} \qquad \dfrac{}{xy^2 = 1 \rightarrow [x' = -x, y' = \frac{y}{2}]xy^2 = 1}}{x > 0 \rightarrow [x' = -x]x > 0}$$



Differential Auxiliaries

Example (Successful proof)

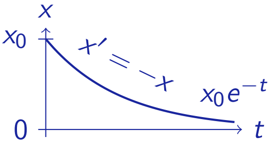
$$\dfrac{\dfrac{*}{x > 0 \leftrightarrow \exists y\, xy^2 = 1} \qquad \dfrac{}{xy^2 = 1 \rightarrow [x' = -x, y' = \frac{y}{2}]xy^2 = 1}}{x > 0 \rightarrow [x' = -x]x > 0}$$



Differential Auxiliaries

Example (Successful proof)

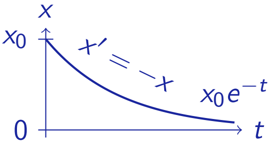
$$\dfrac{\dfrac{*}{x > 0 \leftrightarrow \exists y\, xy^2 = 1} \qquad \dfrac{\dfrac{}{x'y^2 + x2yy' = 0}}{xy^2 = 1 \rightarrow [x' = -x, y' = \frac{y}{2}]xy^2 = 1}}{x > 0 \rightarrow [x' = -x]x > 0}$$



Differential Auxiliaries

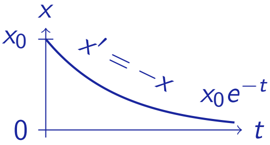
Example (Successful proof)

$$\dfrac{\dfrac{*}{x>0 \leftrightarrow \exists y\, xy^2=1} \quad \dfrac{\dfrac{\dfrac{}{-xy^2+2xy\frac{y}{2}=0}}{x'y^2+x2yy'=0}}{xy^2=1 \rightarrow [x'=-x,y'=\frac{y}{2}]xy^2=1}}{x>0 \rightarrow [x'=-x]x>0}$$



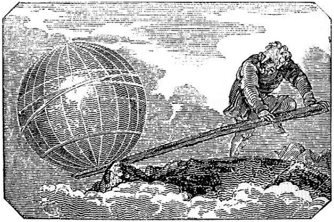
Example (Successful proof)

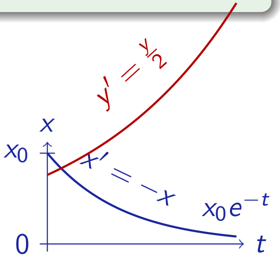
$$
\dfrac{\dfrac{*}{x > 0 \leftrightarrow \exists y\, xy^2 = 1} \qquad \dfrac{\dfrac{\dfrac{*}{-xy^2 + 2xy\frac{y}{2} = 0}}{x'y^2 + x2yy' = 0}}{xy^2 = 1 \rightarrow [x' = -x, y' = \frac{y}{2}]xy^2 = 1}}{x > 0 \rightarrow [x' = -x]x > 0}
$$



Example (Successful proof)

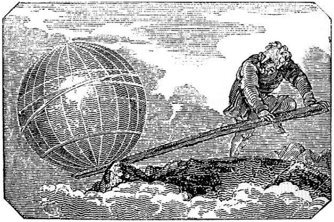
$$
\dfrac{\dfrac{*}{x > 0 \leftrightarrow \exists y\, xy^2 = 1} \qquad \dfrac{\dfrac{\dfrac{*}{-xy^2 + 2xy\frac{y}{2} = 0}}{x'y^2 + x2yy' = 0}}{xy^2 = 1 \rightarrow [x' = -x, y' = \frac{y}{2}]xy^2 = 1}}{x > 0 \rightarrow [x' = -x]x > 0}
$$

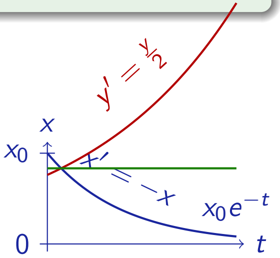




Example (Successful proof)

$$\dfrac{\dfrac{*}{x > 0 \leftrightarrow \exists y\, xy^2 = 1} \qquad \dfrac{\dfrac{\dfrac{*}{-xy^2 + 2xy\frac{y}{2} = 0}}{x'y^2 + x2yy' = 0}}{xy^2 = 1 \rightarrow [x' = -x, y' = \frac{y}{2}]xy^2 = 1}}{x > 0 \rightarrow [x' = -x]x > 0}$$





Differential Auxiliaries

$$\frac{\phi \leftrightarrow \exists y\, \psi \quad \psi \rightarrow [x' = \theta, y' = \vartheta \,\&\, H]\psi}{\phi \rightarrow [x' = \theta \,\&\, H]\phi}$$

if $y' = \vartheta$ has solution $y : [0, \infty) \rightarrow \mathbb{R}^n$

Theorem (Auxiliary Differential Variables)

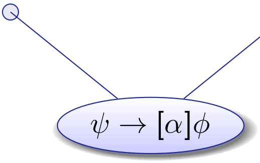
Deductive power with differential auxiliaries exceeds deductive power without.

$$\mathcal{DCI} + DA > \mathcal{DCI}$$

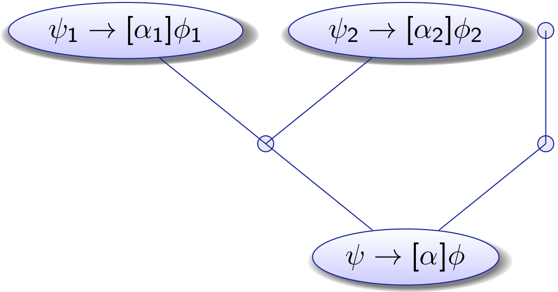
André Platzer.
The structure of differential invariants and differential cut elimination.
Logical Methods in Computer Science, 2012.

Outline Background

Differential Invariants as Fixedpoints

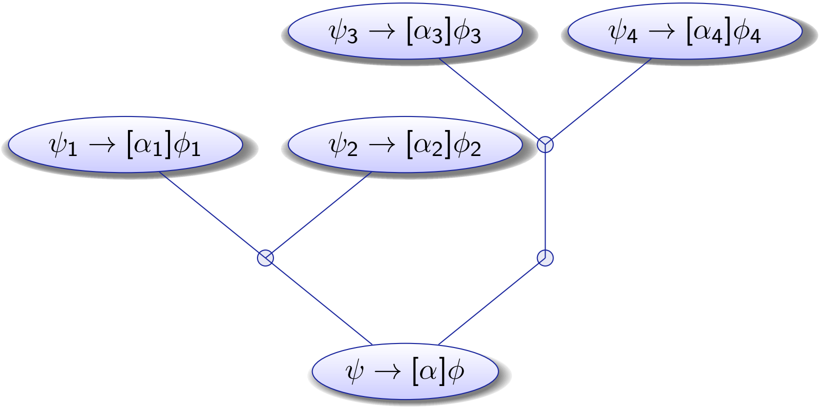


Details



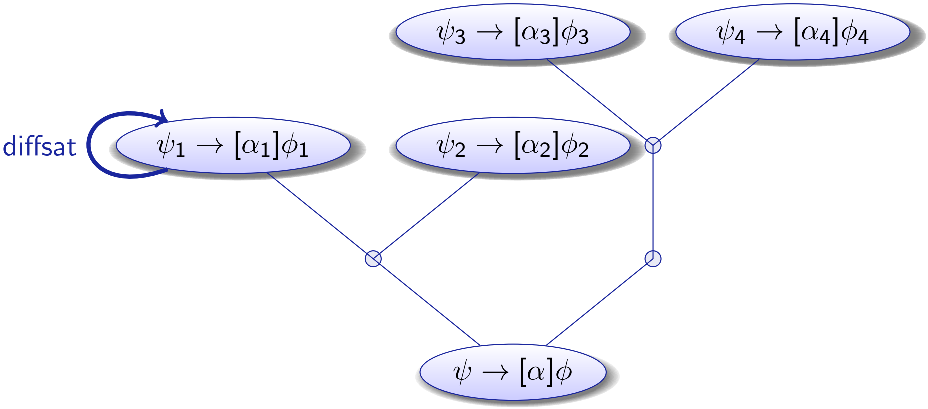
for $\cup\,, ;\,, :=$ do decompose

Details



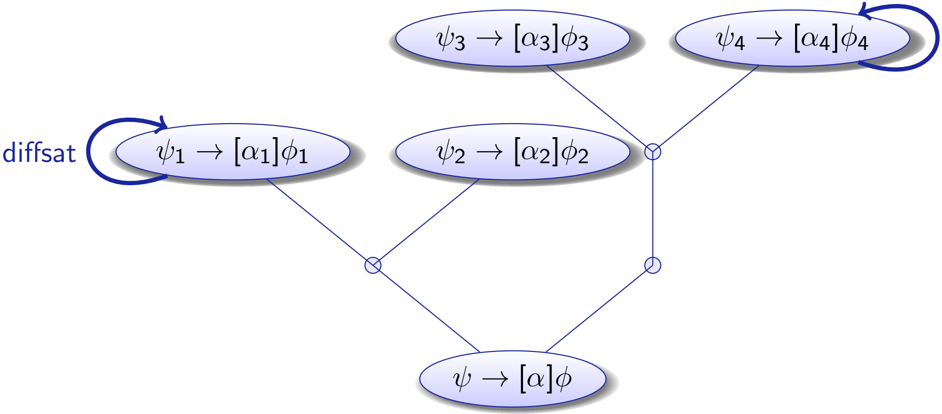
for $\cup\, ,\, ;\, ,\, :=$ do decompose

Details



for $\cup\,,;\,,:=$ do decompose
for $x' = \dots$ do diffsat

Details

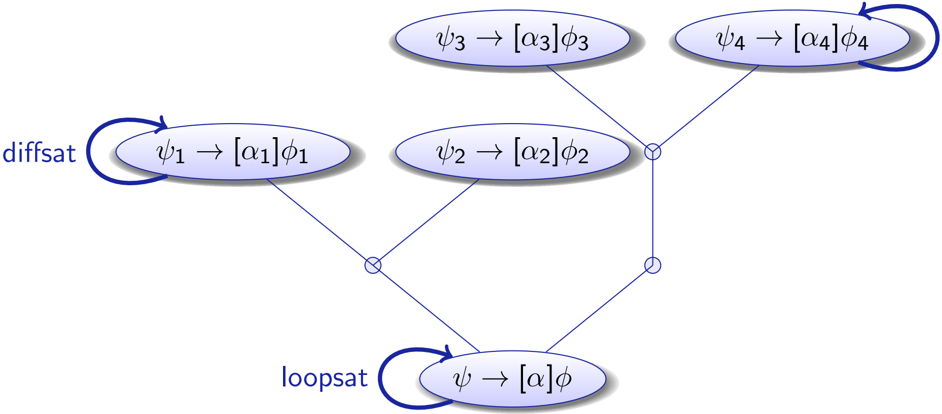


for $\cup$, ; , := do decompose

for $x' = \dots$ do diffsat

Details

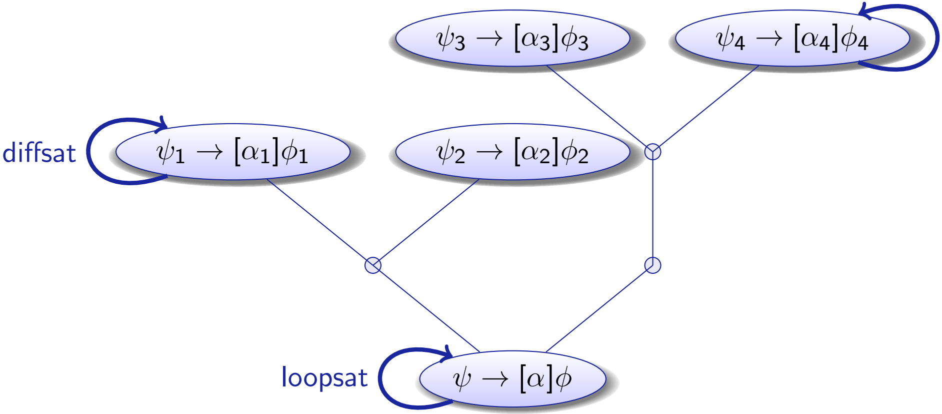
Differential Invariants as Fixedpoints



for $\cup, ;, :=$	do decompose
for $x' = \dots$	do diffsat
for α^*	do loopsat

Details

Differential Invariants as Fixedpoints



for $\cup\,,;\,,:=$	do decompose	repeat until fixedpoint
for $x' = \dots$	do diffsat	
for α^*	do loopsat	

Details

Outline Background

Definition (Syntactic total derivation $D : \mathrm{Trm} \to \mathrm{Trm}$)

$$
\begin{aligned}
D(r) &= 0 && \text{if } r \text{ is a (rigid) number symbol}\\
D(x^{(n)}) &= x^{(n+1)} && \text{if } x \in \Sigma \text{ is flexible, } n \geq 0\\
D(a+b) &= D(a) + D(b)\\
D(a \cdot b) &= D(a) \cdot b + a \cdot D(b)\\
D(a/b) &= (D(a) \cdot b - a \cdot D(b))/b^2\\
D(F) &\equiv \bigwedge_{i=1}^{m} D(F_i) && \{F_1, \dots, F_m\} \text{ all literals of } F\\
D(a \geq b) &\equiv D(a) \geq D(b) && \text{accordingly for } <, >, \leq, =
\end{aligned}
$$

$$
\begin{aligned}
\mathcal{P} &\equiv (x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2\\
\Rightarrow D(\mathcal{P}) &\equiv 2(x_1 - y_1)(x_1' - y_1') + 2(x_2 - y_2)(x_2' - y_2') \geq 0
\end{aligned}
$$

Derivations and Differentiation

Definition (Syntactic total derivation $D : \mathrm{Trm} \to \mathrm{Trm}$)

$$
\begin{aligned}
D(r) &= 0 && \text{if } r \text{ is a (rigid) number symbol}\\
D(x^{(n)}) &= x^{(n+1)} && \text{if } x \in \Sigma \text{ is flexible, } n \geq 0\\
D(a+b) &= D(a) + D(b)\\
D(a \cdot b) &= D(a) \cdot b + a \cdot D(b)\\
D(a/b) &= (D(a) \cdot b - a \cdot D(b))/b^2\\
D(F) &\equiv \bigwedge_{i=1}^{m} D(F_i) && \{F_1, \dots, F_m\} \text{ all literals of } F\\
D(a \geq b) &\equiv D(a) \geq D(b) && \text{accordingly for } <, >, \leq, =
\end{aligned}
$$

$$
\begin{aligned}
\mathcal{P} &\equiv (x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2\\
\Rightarrow D(\mathcal{P}) &\equiv 2(x_1 - y_1)(x_1' - y_1') + 2(x_2 - y_2)(x_2' - y_2') \geq 0
\end{aligned}
$$

Derivations and Differentiation

Syntactic derivation $D(\cdot)$ coincides with analytic differentiation:

Lemma (Derivation lemma)

Valuation is differential homomorphism: for all flows φ *all* $\zeta \in [0, r]$

$$\frac{\mathrm{d}\,[\![\theta]\!]_{\varphi(t)}}{\mathrm{d}t}(\zeta) = [\![D(\theta)]\!]_{\bar{\varphi}(\zeta)}$$

Theorem (Differential Invariant)

$$\frac{\chi \rightarrow F'}{\chi \rightarrow F \rightarrow [x' = \theta \,\&\, \chi]F} \quad \textit{sound for } F' \equiv D(F)^{\theta}_{x'}$$

Derivations and Differentiation

Syntactic derivation $D(\cdot)$ coincides with analytic differentiation:

Lemma (Derivation lemma)

Valuation is differential homomorphism: for all flows φ *all* $\zeta \in [0, r]$

$$\frac{\mathrm{d}\,[\![\theta]\!]_{\varphi(t)}}{\mathrm{d}t}(\zeta) = [\![D(\theta)]\!]_{\bar{\varphi}(\zeta)}$$

Locally understand differential equations by substitution:

Lemma (Differential substitution principle)

If $\varphi \models x_i' = \theta_i \land \chi$, *then* $\varphi \models \mathcal{D} \leftrightarrow (\chi \to \mathcal{D}_{x_i'}^{\theta_i})$ *for all* $\mathcal{D}$.

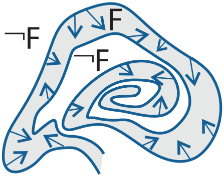
Theorem (Differential Invariant)

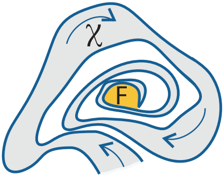
$$\frac{\chi \to F'}{\chi \to F \to [x' = \theta \,\&\, \chi]F} \quad \textit{sound for } F' \equiv D(F)_{x'}^{\theta}$$

Outline Background

Definition (Differential Invariant) ▸ Details

F closed under total differentiation with respect to differential constraints





$$\frac{(\chi \to F')}{\chi \to F \to [x' = \theta \,\&\, \chi]F}$$

$$\frac{(\neg F \land \chi \to F'_{\gg})}{[x' = \theta \,\&\, \neg F]\chi \to \langle x' = \theta \,\&\, \chi\rangle F}$$

$$\frac{}{\langle x' = a \rangle x \geq b}$$

Ex: Differential Variant for Progress Discovery

$$\cfrac{\overline{\exists \varepsilon > 0\, \forall x\, (x \leq b \rightarrow x' \geq \varepsilon}}{\langle x' = a \rangle x \geq b}$$

Ex: Differential Variant for Progress Discovery

$$\cfrac{\cfrac{}{\exists\varepsilon{>}0\,\forall x\,(x \leq b \rightarrow {\color{red}a} \geq \varepsilon)}}{\cfrac{\exists\varepsilon{>}0\,\forall x\,(x \leq b \rightarrow {\color{red}x'} \geq \varepsilon}{\langle x' = a\rangle x \geq b}}$$

Ex: Differential Variant for Progress Discovery

$$a > 0$$

$$\exists \varepsilon{>}0\, \forall x\, (x \leq b \rightarrow a \geq \varepsilon)$$

$$\exists \varepsilon{>}0\, \forall x\, (x \leq b \rightarrow x' \geq \varepsilon$$

$$\langle x' = a \rangle x \geq b$$

$$
\begin{array}{c}
b > 0 \\ \hline
\mathrm{QE}(\exists d\,((\|d\|^2 \le b^2) \land (d_1 > 0 \land d_2 > 0))) \\ \hline
\begin{array}{cc}
 & \begin{array}{c} d_1 > 0 \land d_2 > 0 \\ \hline \exists \epsilon{>}0\, \forall x_1, x_2\, (x_1 < p_1 \lor x_2 < p_2 \to d_1 \ge \epsilon \land d_2 \ge \epsilon) \\ \hline \langle \mathcal{F}(0) \rangle (x_1 \ge p_1 \land x_2 \ge p_2) \end{array} \\
\|d\|^2 \le b^2 &
\end{array} \\ \hline
\|d\|^2 \le b^2 \land \langle \mathcal{F}(0) \rangle (x_1 \ge p_1 \land x_2 \ge p_2) \\ \hline
\exists d\,(\|d\|^2 \le b^2 \land \langle \mathcal{F}(0) \rangle (x_1 \ge p_1 \land x_2 \ge p_2)) \\ \hline
\forall p\, \exists d\,(\|d\|^2 \le b^2 \land \langle \mathcal{F}(0) \rangle (x_1 \ge p_1 \land x_2 \ge p_2))
\end{array}
$$

$$
\begin{aligned}
\mathcal{F}(0) &\equiv x_1' = d_1 \land x_2' = d_2 \\
F &\equiv x_1 \ge p_1 \land x_2 \ge p_2
\end{aligned}
$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{b > 0}{\mathrm{QE}(\exists d\,((\|d\|^2 \le b^2) \land (d_1 > 0 \land d_2 > 0)))}}{\|d\|^2 \le b^2 \qquad \dfrac{\dfrac{d_1 > 0 \land d_2 > 0}{\exists \epsilon{>}0\, \forall x_1, x_2\, (x_1 < p_1 \lor x_2 < p_2 \rightarrow d_1 \ge \epsilon \land d_2 \ge \epsilon)}}{\langle \mathcal{F}(0) \rangle (x_1 \ge p_1 \land x_2 \ge p_2)}}}{\|d\|^2 \le b^2 \land \langle \mathcal{F}(0) \rangle (x_1 \ge p_1 \land x_2 \ge p_2)}}{\exists d\, (\|d\|^2 \le b^2 \land \langle \mathcal{F}(0) \rangle (x_1 \ge p_1 \land x_2 \ge p_2))}}{\forall p\, \exists d\, (\|d\|^2 \le b^2 \land \langle \mathcal{F}(0) \rangle (x_1 \ge p_1 \land x_2 \ge p_2))}$$

$$\begin{aligned} \mathcal{F}(0) &\equiv x_1' = d_1 \land x_2' = d_2 \\ F &\equiv x_1 \ge p_1 \land x_2 \ge p_2 \\ F' &\equiv x_1' \ge 0 \land x_2' \ge 0 \end{aligned}$$

$$
\dfrac{\dfrac{\dfrac{\dfrac{b > 0}{\text{QE}(\exists d\,((\|d\|^2 \le b^2) \land (d_1 > 0 \land d_2 > 0)))}}{\|d\|^2 \le b^2 \qquad \dfrac{\dfrac{d_1 > 0 \land d_2 > 0}{\exists \epsilon{>}0\, \forall x_1, x_2\, (x_1 < p_1 \lor x_2 < p_2 \rightarrow d_1 \ge \epsilon \land d_2 \ge \epsilon)}}{\langle \mathcal{F}(0) \rangle (x_1 \ge p_1 \land x_2 \ge p_2)}}}{\|d\|^2 \le b^2 \land \langle \mathcal{F}(0) \rangle (x_1 \ge p_1 \land x_2 \ge p_2)}}{\dfrac{\exists d\,(\|d\|^2 \le b^2 \land \langle \mathcal{F}(0) \rangle (x_1 \ge p_1 \land x_2 \ge p_2))}{\forall p\, \exists d\,(\|d\|^2 \le b^2 \land \langle \mathcal{F}(0) \rangle (x_1 \ge p_1 \land x_2 \ge p_2))}}
$$

$$
\begin{aligned}
\mathcal{F}(0) &\equiv x_1' = d_1 \land x_2' = d_2 \\
F &\equiv x_1 \ge p_1 \land x_2 \ge p_2 \\
F' &\equiv x_1' \ge 0 \land x_2' \ge 0 \\
F' \ge \epsilon &\equiv x_1' \ge \epsilon \land x_2' \ge \epsilon
\end{aligned}
$$

$$\dfrac{\dfrac{b > 0}{\mathrm{QE}(\exists d\,((\|d\|^2 \le b^2) \land (d_1 > 0 \land d_2 > 0)))}}{\dfrac{\|d\|^2 \le b^2 \quad \dfrac{\dfrac{d_1 > 0 \land d_2 > 0}{\exists \epsilon{>}0\, \forall x_1, x_2\, (x_1 < p_1 \lor x_2 < p_2 \to d_1 \ge \epsilon \land d_2 \ge \epsilon)}}{\langle \mathcal{F}(0) \rangle (x_1 \ge p_1 \land x_2 \ge p_2)}}{\dfrac{\|d\|^2 \le b^2 \land \langle \mathcal{F}(0) \rangle (x_1 \ge p_1 \land x_2 \ge p_2)}{\dfrac{\exists d\,(\|d\|^2 \le b^2 \land \langle \mathcal{F}(0) \rangle (x_1 \ge p_1 \land x_2 \ge p_2))}{\forall p\, \exists d\,(\|d\|^2 \le b^2 \land \langle \mathcal{F}(0) \rangle (x_1 \ge p_1 \land x_2 \ge p_2))}}}}$$

$$\begin{aligned} \mathcal{F}(0) &\equiv x_1' = d_1 \land x_2' = d_2 \\ F &\equiv x_1 \ge p_1 \land x_2 \ge p_2 \\ F' &\equiv x_1' \ge 0 \land x_2' \ge 0 \\ F' \ge \epsilon &\equiv x_1' \ge \epsilon \land x_2' \ge \epsilon \end{aligned}$$

$$
\begin{array}{c}
b > 0 \\
\hline
\mathrm{QE}(\exists d\,((\|d\|^2 \le b^2) \land (d_1 > 0 \land d_2 > 0))) \\
\hline
\|d\|^2 \le b^2 \qquad
\begin{array}{l}
d_1 > 0 \land d_2 > 0 \\
\hline
\exists \epsilon{>}0\, \forall x_1, x_2\, (x_1 < p_1 \lor x_2 < p_2 \to d_1 \ge \epsilon \land d_2 \ge \epsilon) \\
\hline
\langle \mathcal{F}(0) \rangle (x_1 \ge p_1 \land x_2 \ge p_2)
\end{array} \\
\hline
\|d\|^2 \le b^2 \land \langle \mathcal{F}(0) \rangle (x_1 \ge p_1 \land x_2 \ge p_2) \\
\hline
\exists d\, (\|d\|^2 \le b^2 \land \langle \mathcal{F}(0) \rangle (x_1 \ge p_1 \land x_2 \ge p_2)) \\
\hline
\forall p\, \exists d\, (\|d\|^2 \le b^2 \land \langle \mathcal{F}(0) \rangle (x_1 \ge p_1 \land x_2 \ge p_2))
\end{array}
$$

$$
\begin{aligned}
\mathcal{F}(0) &\equiv x_1' = d_1 \land x_2' = d_2 \\
F &\equiv x_1 \ge p_1 \land x_2 \ge p_2 \\
F' &\equiv d_1 \ge 0 \land d_2 \ge 0 \\
F' \ge \epsilon &\equiv d_1 \ge \epsilon \land d_2 \ge \epsilon
\end{aligned}
$$

Differential Variants for Progress

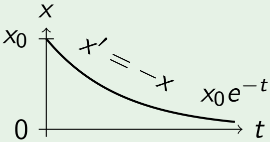
Example (Progress)

$$\frac{\forall x\,(x > 0 \rightarrow -x < 0)}{\langle x' = -x\rangle x \leq 0}$$

Differential Variants for Progress

Example (Progress)

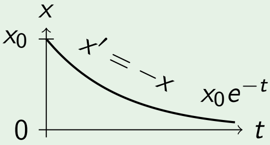
$$\frac{\forall x\,(x > 0 \rightarrow -x < 0)}{\langle x' = -x \rangle x \leq 0}$$



Differential Variants for Progress

Example (Unsound without minimal progress!)

$$\frac{\forall x\,(x > 0 \to -x < 0)}{\langle x' = -x \rangle x \le 0}$$



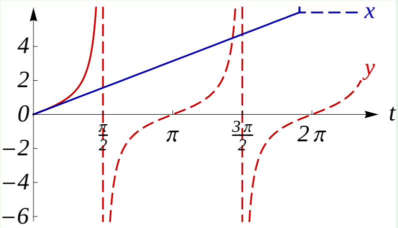
Differential Variants for Progress

Example (Mixed dynamics)

$$\dfrac{\dfrac{*}{\exists\varepsilon{>}0\,\forall x\forall y\,(x<6\rightarrow 1\geq\varepsilon)}}{\langle x'=1\land y'=1+y^2\rangle x\geq 6}$$

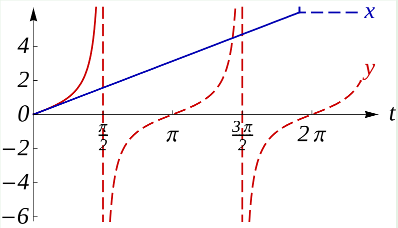
Example (Mixed dynamics)

$$\dfrac{\dfrac{*}{\exists\varepsilon{>}0\,\forall x\forall y\,(x<6\rightarrow 1\geq\varepsilon)}}{\langle x'=1\land y'=1+y^2\rangle x\geq 6}$$



Example (Unsound without Lipschitz-continuity!)

$$\dfrac{\dfrac{*}{\exists \varepsilon{>}0\, \forall x \forall y\, (x < 6 \rightarrow 1 \geq \varepsilon)}}{\langle x' = 1 \land y' = 1 + y^2 \rangle x \geq 6}$$



Temporal Modalities + Dynamic Modalities

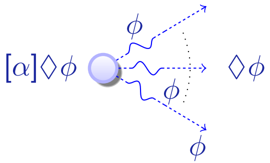
problem	technique	Op	Par	T	closed
$ETCS \models z < MA$	TL-MC	✓	×	✓	×
$\models (\text{Ax}(ETCS) \rightarrow z < MA)$	TL-calculus	×	...	✓	...
$\models [ETCS]\, z < MA$	DL-calculus	✓	✓	×	✓
$\models [ETCS]\Box\, z < MA$	dTL-calculus	✓	✓	✓	✓

Temporal Modalities + Dynamic Modalities

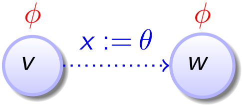
problem	technique	Op	Par	T	closed
$ETCS \models z < MA$	TL-MC	✓	×	✓	×
$\models (Ax(ETCS) \to z < MA)$	TL-calculus	×	...	✓	...
$\models [ETCS]\, z < MA$	DL-calculus	✓	✓	×	✓
$\models [ETCS]\Box\, z < MA$	dTL-calculus	✓	✓	✓	✓

differential temporal dynamic logic

$$dTL = TL + DL + HP$$

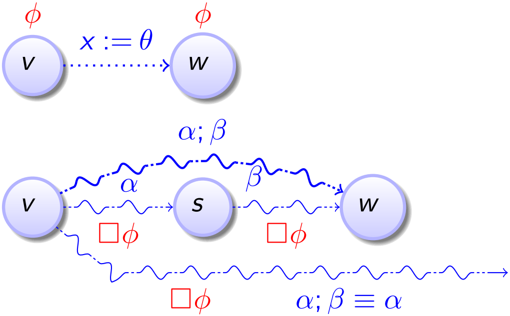


$$\frac{\phi \land [x := \theta]\phi}{[x := \theta]\Box\phi}$$

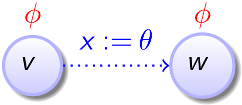


$$\frac{\phi \wedge [x := \theta]\phi}{[x := \theta]\Box\phi}$$

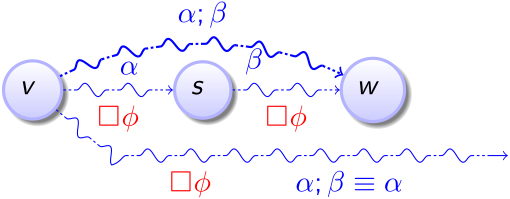
$$\frac{[\alpha]\Box\phi \wedge [\alpha][\beta]\Box\phi}{[\alpha;\beta]\Box\phi}$$



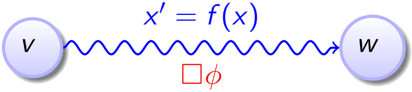
$$\frac{\phi \land [x := \theta]\phi}{[x := \theta]\Box\phi}$$



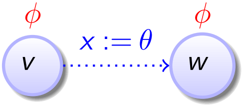
$$\frac{[\alpha]\Box\phi \land [\alpha][\beta]\Box\phi}{[\alpha;\beta]\Box\phi}$$



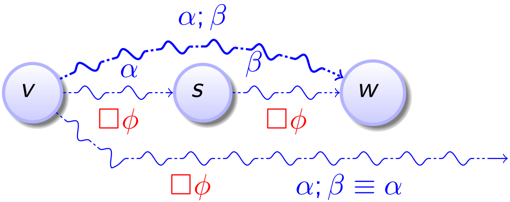
$$\frac{[x' = \theta]\phi}{[x' = \theta]\Box\phi}$$



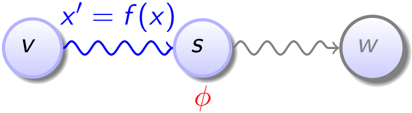
$$\frac{\phi \land [x := \theta]\phi}{[x := \theta]\Box\phi}$$



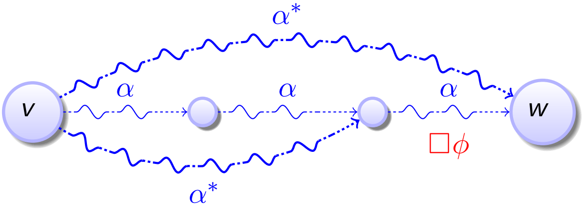
$$\frac{[\alpha]\Box\phi \land [\alpha][\beta]\Box\phi}{[\alpha;\beta]\Box\phi}$$



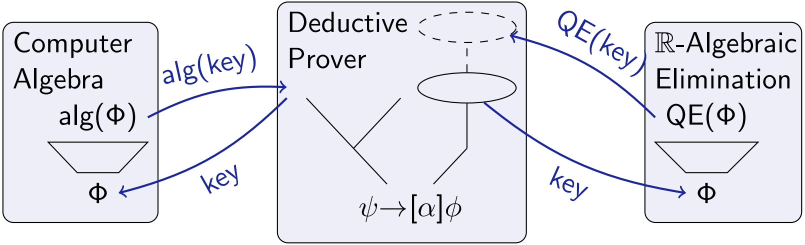
$$\frac{[x' = \theta]\phi}{[x' = \theta]\Box\phi}$$



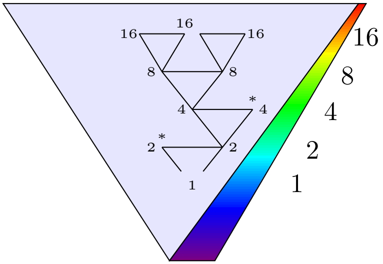
$$\frac{[\alpha^*][\alpha]\Box\phi}{[\alpha^*]\Box\phi}$$



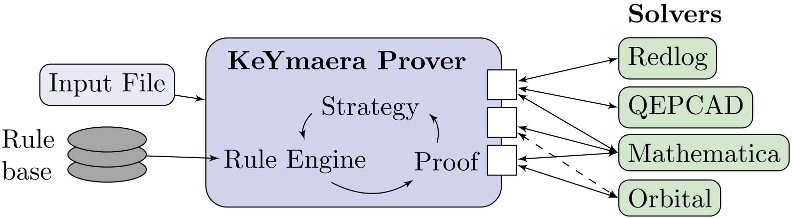
Outline Background

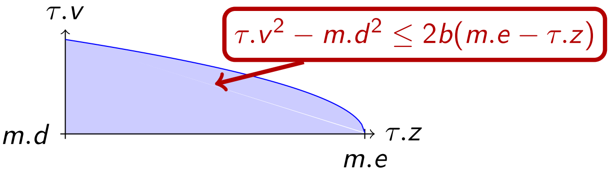


56 interactions?



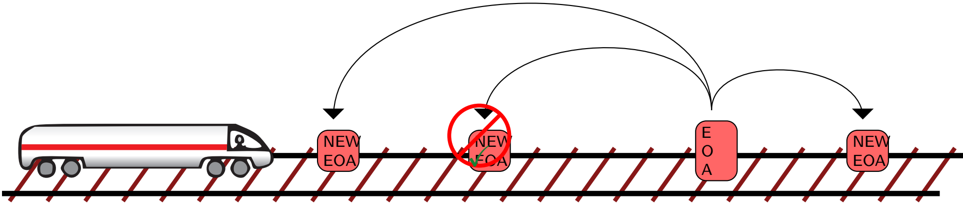
0–1 interactions!


Solvers
KeYmaera Prover
Input File
Strategy
Rule
base
Rule Engine
Proof
Redlog
QEPCAD
Mathematica
Orbital



Proposition (Controllability)

$$[\tau.z' = \tau.v, \tau.v' = -b \,\&\, \tau.v \geq 0](\tau.z \geq m.e \rightarrow \tau.v \leq m.d)$$
$$\equiv \tau.v^2 - m.d^2 \leq 2b(m.e - \tau.z)$$



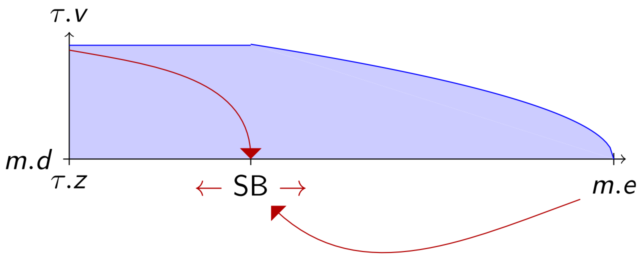
Proposition (RBC Controllability)

$m.d \geq 0 \land b > 0 \rightarrow [m_0 := m;\ RBC] \Big($

$m_0.d^2 - m.d^2 \leq 2b(m.e - m_0.e) \land m_0.d \geq 0 \land m.d \geq 0 \leftrightarrow \forall \tau$

$((\langle m := m_0 \rangle \tau.v^2 - m.d^2 \leq 2b(m.e - \tau.z)) \rightarrow \tau.v^2 - m.d^2 \leq 2b(m.e - \tau.z)) \Big)$

ETCS Reactivity

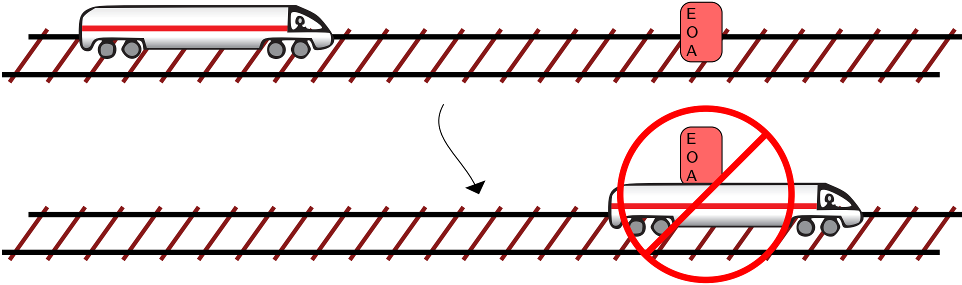


Proposition (Reactivity)

$$\Big(\forall m.e\, \forall \tau.z\, \big(m.e - \tau.z \geq SB \land \tau.v^2 - m.d^2 \leq 2b(m.e - \tau.z) \rightarrow [\tau.a := A;\ drive]\, \tau.v^2 - m.d^2 \leq 2b(m.e - \tau.z)\big)\Big)$$

$$\equiv SB \geq \frac{\tau.v^2 - m.d^2}{2b} + \left(\frac{A}{b} + 1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon\, \tau.v\right)$$

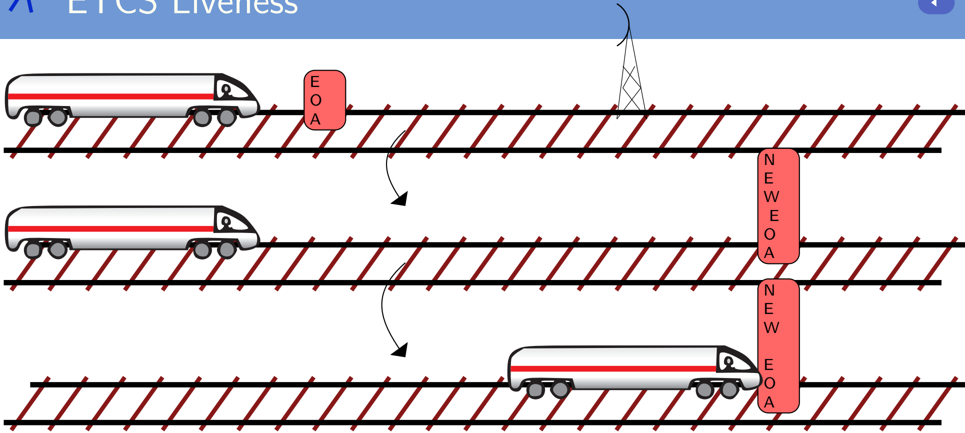
ETCS Safety



Proposition (Safety)

$$\tau.v^2 - m.d^2 \le 2b(m.e - \tau.z) \rightarrow$$
$$[ETCS](\tau.z \ge m.e \rightarrow \tau.v \le m.d)$$

ETCS Liveness



Proposition (Liveness)

$$\tau.v > 0 \land \varepsilon > 0 \rightarrow \forall P\, \langle ETCS \rangle\, \tau.z \geq P$$

Safety Despite Disturbances

So far: no wind, friction, etc.

Direct control of the acceleration

Safety Despite Disturbances

So far: no wind, friction, etc.

Direct control of the acceleration

Issue

This is unrealistic!

Safety Despite Disturbances

So far: no wind, friction, etc.

Direct control of the acceleration

Issue

This is unrealistic!

Solution Take disturbances into account.

Theorem

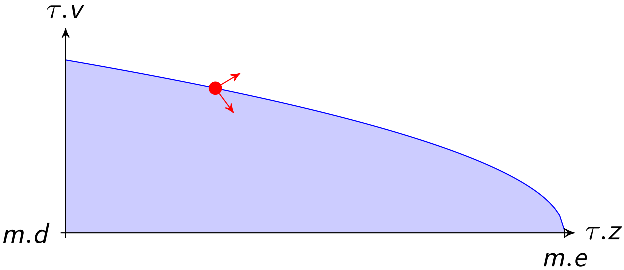
ETCS is controllable, reactive, and safe in the presence of disturbances.

So far: no wind, friction, etc.
Direct control of the acceleration

Issue
This is unrealistic!

Solution Take disturbances into account.

Theorem
ETCS is controllable, reactive, and safe in the presence of disturbances.



Safety Despite Disturbances

So far: no wind, friction, etc.

Direct control of the acceleration

Issue

This is unrealistic!

Solution Take disturbances into account.

Theorem

ETCS is controllable, reactive, and safe in the presence of disturbances.

Proof sketch

The system now contains $\tau.a - l \leq \tau.v' \leq \tau.a + u$ instead of $\tau.v' = \tau.a$.

$\leadsto$ We cannot solve the differential equations anymore.

$\leadsto$ Use differential invariants for approximation. For details see paper.

Platzer, A.:
Differential-algebraic dynamic logic for differential-algebraic programs.
J. Log. Comput., 35(1): 309–352, 2010.

So far

Almost completely non-deterministic control.

Smooth Speed Control

So far

Almost completely non-deterministic control.

Issue

This is unrealistic!

Smooth Speed Control

So far

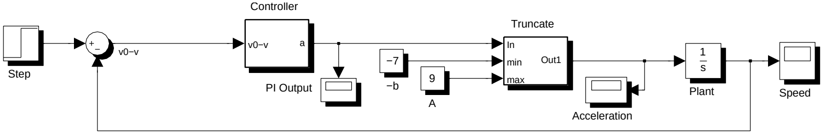
Almost completely non-deterministic control.

Issue

This is unrealistic!

Solution

Verify proportional-integral (PI) controllers used in trains.



Smooth Speed Control

So far

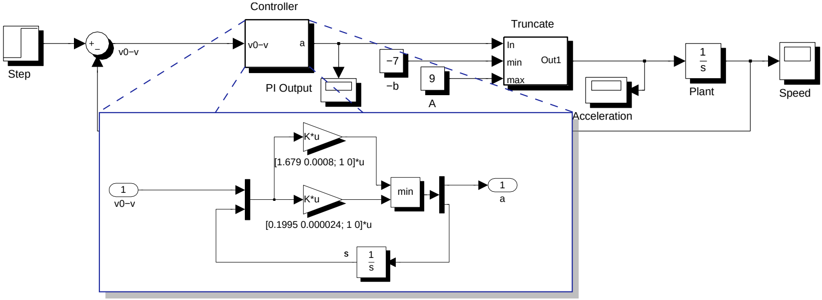
Almost completely non-deterministic control.

Issue

This is unrealistic!

Solution

Verify proportional-integral (PI) controllers used in trains.



Smooth Speed Control

So far

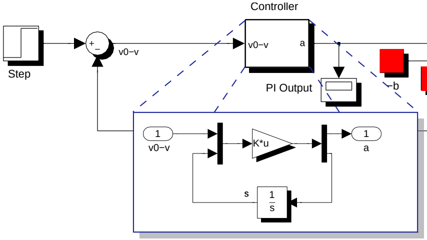
Almost completely non-deterministic control.

Issue

This is unrealistic!

Solution

Verify proportional-integral (PI) controllers used in trains.



Differential equation system

$$\tau.v' = \min\Big(A, \max\big(-b,\ \ell(\tau.v - m.r) - i\, s - c\, m.r\big)\Big) \land s' = \tau.v - m.r$$

Smooth Speed Control

So far

Almost completely non-deterministic control.

Issue

This is unrealistic!

Solution Verify proportional-integral (PI) controllers used in trains.

Theorem

The ETCS system remains safe when speed is controlled by a PI controller.

Proof sketch

Cannot solve differential equations really. Use differential invariants! For details see paper.

Platzer, A.:
Differential-algebraic dynamic logic for differential-algebraic programs.
J. Log. Comput., 35(1): 309–352, 2010.

Experimental Results (ETCS)

Case Study		Int	Time(s)	Mem(Mb)	Steps	Dim
controllability	train	0	0.6	6.9	14	5
controllability	RBC	0	0.5	6.4	42	12
controllability	RBC	0	0.9	6.5	82	12
reactivity		13	279.1	98.3	265	14
reactivity		0	103.9	61.7	47	14
safety		0	2052.4	204.3	153	14
liveness	essentials	4	35.2	92.2	62	10
liveness	simplified	6	9.6	23.5	134	13
controllability	disturbance	0	2.8	8.3	26	7
reactivity	disturbance	1	23.7	47.6	76	15
safety	disturbance	1	5805.2	34	218	16

provable automatically!

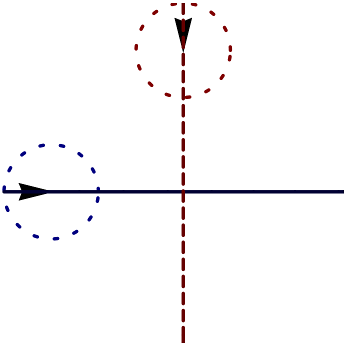
$$
\begin{aligned}
\text{spec} &: \tau.v^2 - \mathbf{m}.d^2 \le 2b(\mathbf{m}.e - \tau.p) \land \tau.v \ge 0 \land \mathbf{m}.d \ge 0 \land b > 0\\
&\quad \to \; [\text{ETCS}](\tau.p \ge \mathbf{m}.e \to \tau.v \le \mathbf{m}.d)\\
\text{ETCS} &: (\text{train} \cup \text{rbc})^*\\
\text{train} &: \text{spd};\ \text{atp};\ \text{move}\\
\text{spd} &: \ (?\tau.v \le \mathbf{m}.r;\ \tau.a := *;\ ?-b \le \tau.a \le A)\\
&\quad \cup (?\tau.v \ge \mathbf{m}.r;\ \tau.a := *;\ ?0 > \tau.a \ge -b)\\
\text{atp} &: SB := \frac{\tau.v^2 - \mathbf{m}.d^2}{2b} + \left(\frac{A}{b} + 1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon\, \tau.v\right);\\
&\quad (?(\mathbf{m}.e - \tau.p \le SB \lor rbc.message = emergency);\ \tau.a := -b)\\
&\quad \cup (?\mathbf{m}.e - \tau.p \ge SB \land rbc.message \ne emergency)\\
\text{move} &: t := 0;\ (\tau.p' = \tau.v, \tau.v' = \tau.a, t' = 1 \,\&\, \tau.v \ge 0 \land t \le \varepsilon)\\
\text{rbc} &: \ (rbc.message := emergency)\\
&\quad \cup \big(\mathbf{m}_0 := \mathbf{m}; \mathbf{m} := *;\\
&\qquad ?\mathbf{m}.r \ge 0 \land \mathbf{m}.d \ge 0 \land \mathbf{m}_0.d^2 - \mathbf{m}.d^2 \le 2b(\mathbf{m}.e - \mathbf{m}_0.e)\big)
\end{aligned}
$$

1 Branch of ETCS Proof

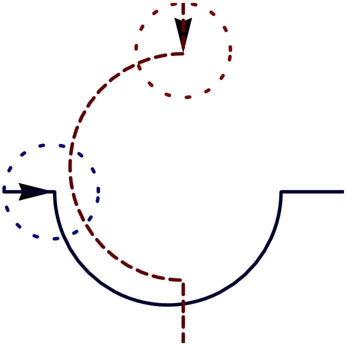
```
 state = 0,
 2 * b * (m - z) >= v ^ 2 - d ^ 2,
 v >= 0, d >= 0, v >= 0, ep >  0, b >  0, amax >  0, d >= 0
==>
    v <= vdes
 -> \forall R a_3;
      (   a_3 >= 0 & a_3 <= amax
       ->   (       m - z
                <= (amax / b + 1) * ep * v
                 + (v ^ 2 - d ^ 2) / (2 * b)
                 + (amax / b + 1) * amax * ep ^ 2 / 2
            -> \forall R t0;
                 (   t0 >= 0
                  -> \forall R ts0;  (0 <= ts0 & ts0 <= t0 -> -b * ts0 + v >= 0 & ts0 + 0 <= ep)
                  ->      2 * b * (m - 1 / 2 * (-b * t0 ^ 2 + 2 * t0 * v + 2 * z))
                       >= (-b * t0 + v) ^ 2
                        - d ^ 2
                     & -b * t0 + v >= 0
                     & d >= 0))
         & (       m - z
                >  (amax / b + 1) * ep * v
                 + (v ^ 2 - d ^ 2) / (2 * b)
                 + (amax / b + 1) * amax * ep ^ 2 / 2
            -> \forall R t2;
                 (   t2 >= 0
                  -> \forall R ts2;  (0 <= ts2 & ts2 <= t2 -> a_3 * ts2 + v >= 0 & ts2 + 0 <= ep)
                  ->      2 * b * (m - 1 / 2 * (a_3 * t2 ^ 2 + 2 * t2 * v + 2 * z))
                       >= (a_3 * t2 + v) ^ 2
                        - d ^ 2
                     & a_3 * t2 + v >= 0
                     & d >= 0)))
```

Outline Background

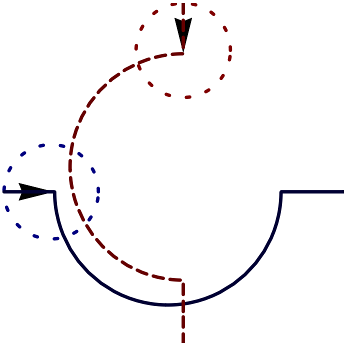
Air Traffic Control



Air Traffic Control



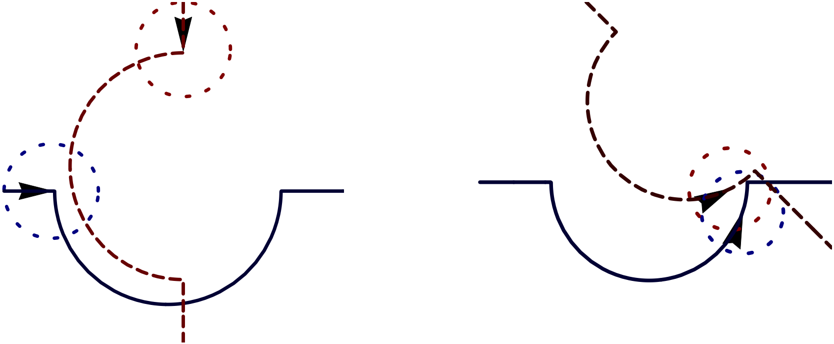
Air Traffic Control



Verification?

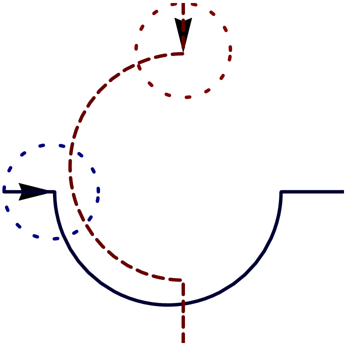
looks correct

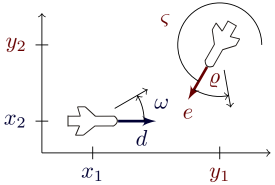
Air Traffic Control



Verification?

looks correct NO!



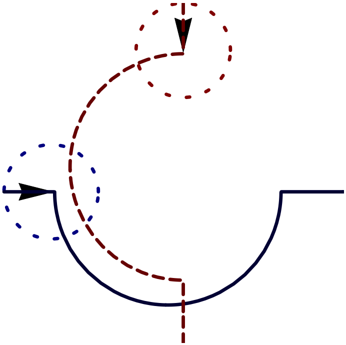


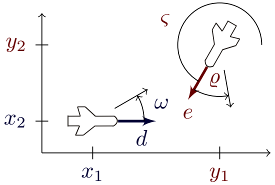
$$\begin{bmatrix} x_1' = -v_1 + v_2 \cos\vartheta + \omega x_2 \\ x_2' = v_2 \sin\vartheta - \omega x_1 \\ \vartheta' = \varpi - \omega \end{bmatrix}$$

Verification?

looks correct NO!

Air Traffic Control



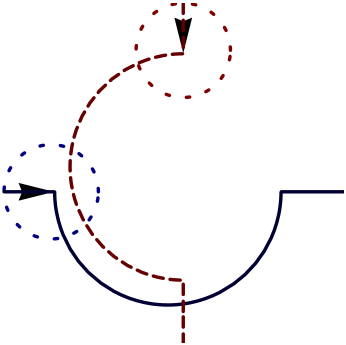


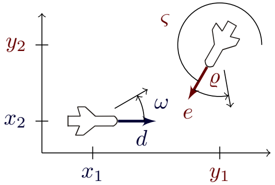
$$\begin{bmatrix} x_1' = -v_1 + v_2 \cos\vartheta + \omega x_2 \\ x_2' = v_2 \sin\vartheta - \omega x_1 \\ \vartheta' = \varpi - \omega \end{bmatrix}$$

Example ("Solving" differential equations)

$$x_1(t) = \frac{1}{\omega\varpi}\big(x_1\omega\varpi \cos t\omega - v_2\omega \cos t\omega \sin\vartheta + v_2\omega \cos t\omega \cos t\varpi \sin\vartheta - v_1\varpi \sin t\omega$$
$$+ x_2\omega\varpi \sin t\omega - v_2\omega \cos\vartheta \cos t\varpi \sin t\omega - v_2\omega\sqrt{1 - \sin\vartheta^2} \sin t\omega$$
$$+ v_2\omega \cos\vartheta \cos t\omega \sin t\varpi + v_2\omega \sin\vartheta \sin t\omega \sin t\varpi\big) \ldots$$

Air Traffic Control





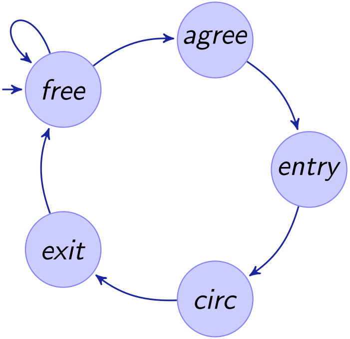
$$\begin{bmatrix} x_1' = -v_1 + v_2 \cos\vartheta + \omega x_2 \\ x_2' = v_2 \sin\vartheta - \omega x_1 \\ \vartheta' = \varpi - \omega \end{bmatrix}$$

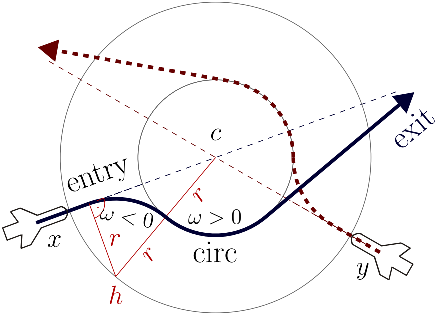
Example ("Solving" differential equations)

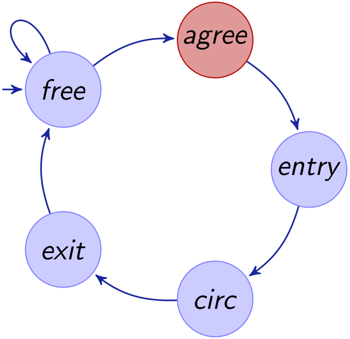
$$\forall t \geq 0 \quad \frac{1}{\omega\varpi}\big(x_1\omega\varpi \cos t\omega - v_2\omega \cos t\omega \sin\vartheta + v_2\omega \cos t\omega \cos t\varpi \sin\vartheta - v_1\varpi \sin t\omega$$

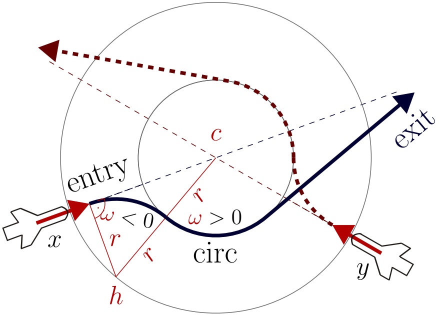
$$+ x_2\omega\varpi \sin t\omega - v_2\omega \cos\vartheta \cos t\varpi \sin t\omega - v_2\omega\sqrt{1 - \sin\vartheta^2} \sin t\omega$$

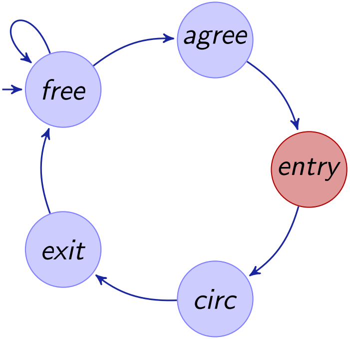
$$+ v_2\omega \cos\vartheta \cos t\omega \sin t\varpi + v_2\omega \sin\vartheta \sin t\omega \sin t\varpi\big) \ldots$$

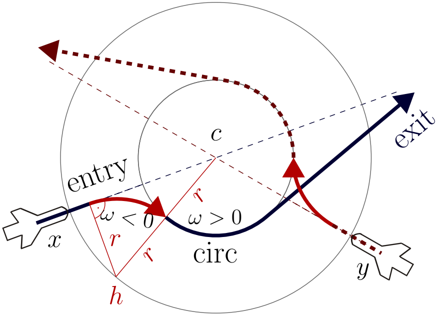

agree
free
entry
exit
circ


c
entry
exit
$\omega < 0$
$\omega > 0$
r
r
r
x
y
circ
h

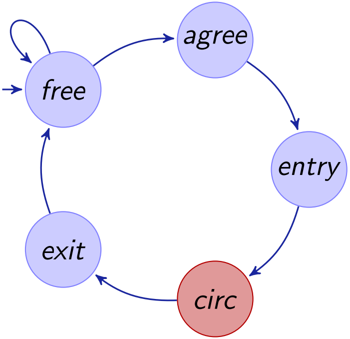

agree
free
entry
exit
circ

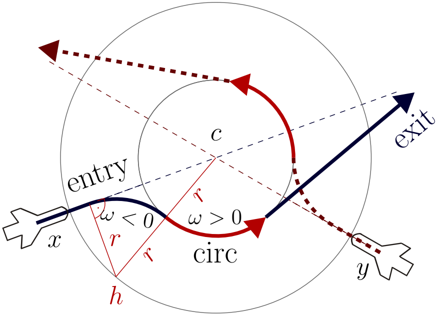

c
entry
exit
r
$\omega < 0$
$\omega > 0$
x
circ
y
h

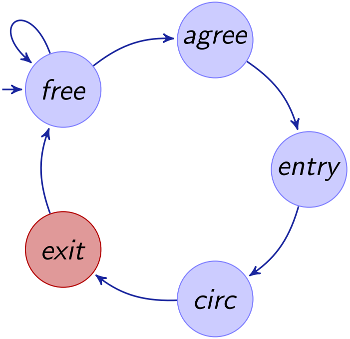

agree
free
entry
exit
circ

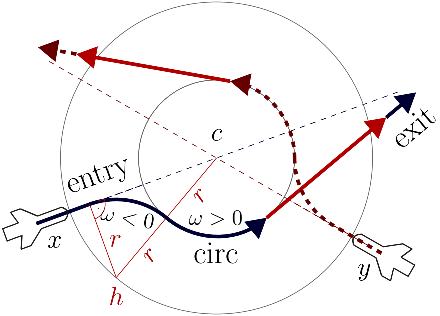

c
entry
exit
r
$\omega < 0$
$\omega > 0$
x
y
circ
h

Flyable Roundabout Maneuver: Overview

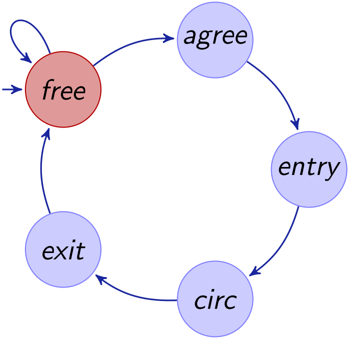


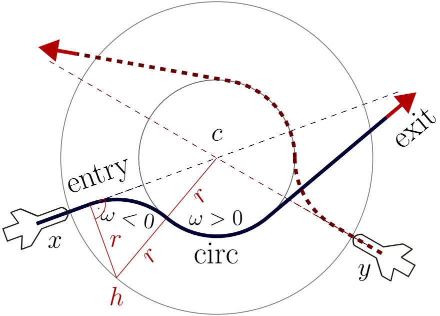


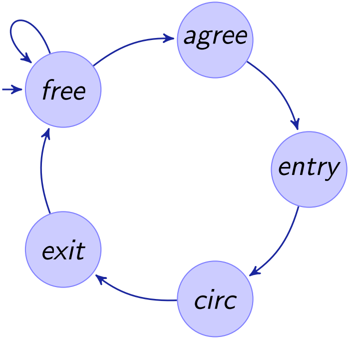

agree
free
entry
exit
circ

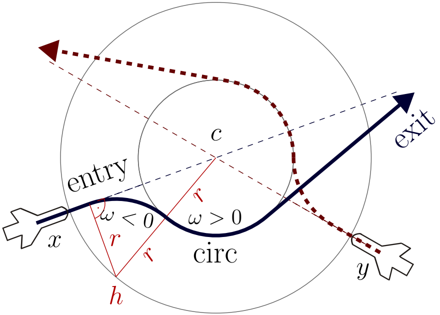

c
entry
$\omega < 0$
$\omega > 0$
r
r
r
x
circ
h
y
exit

Flyable Roundabout Maneuver: Overview

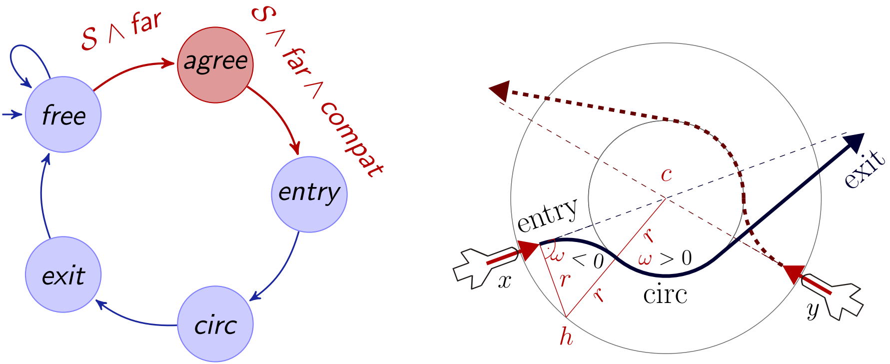





agree
free
entry
exit
circ

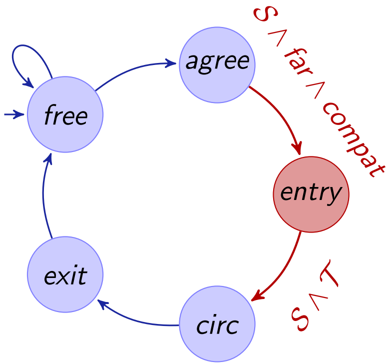

c
entry
exit
$\omega < 0$
$\omega > 0$
r
r
r
x
y
circ
h

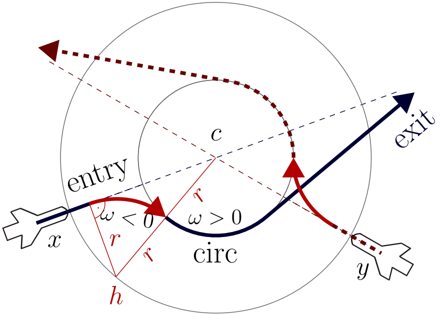
Fixedpoint Iterations for Air Traffic Control



Example (d$\mathcal{L}$ formula of verification subgoal)

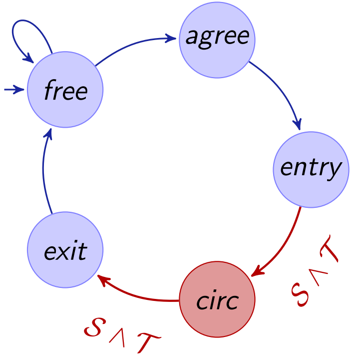
$$safe \wedge far \rightarrow [agree](safe \wedge far \wedge compatible)$$

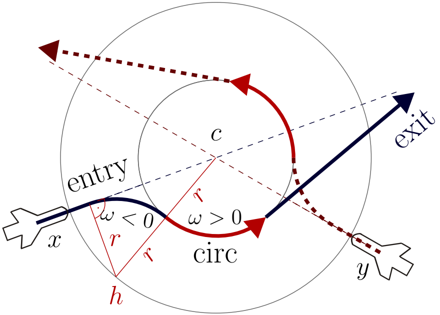




Example (d$\mathcal{L}$ formula of verification subgoal)

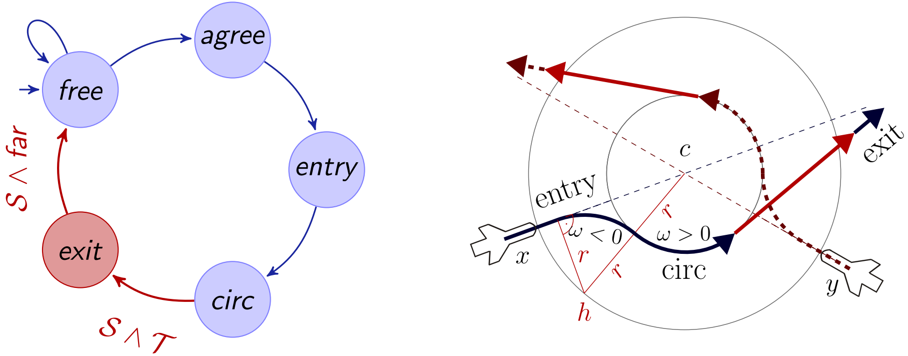
$$\textit{safe} \land \textit{far} \land \textit{compatible} \;\rightarrow\; [\textit{entry}](\textit{safe} \land \textit{tangential})$$





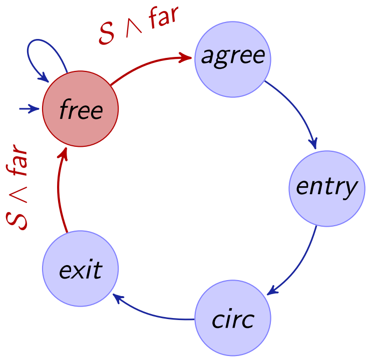
Example (d$\mathcal{L}$ formula of verification subgoal)

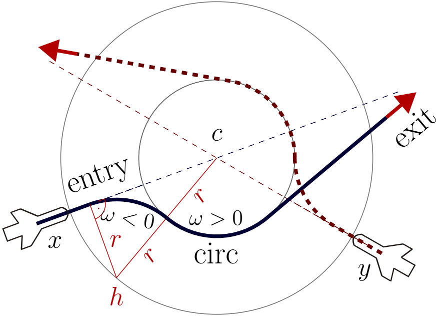
$$\textit{safe} \wedge \textit{tangential} \rightarrow [\textit{circ}](\textit{safe} \wedge \textit{tangential})$$



Example (d$\mathcal{L}$ formula of verification subgoal)

$$\textit{safe} \land \textit{tangential} \rightarrow [\textit{exit}](\textit{safe} \land \textit{far})$$

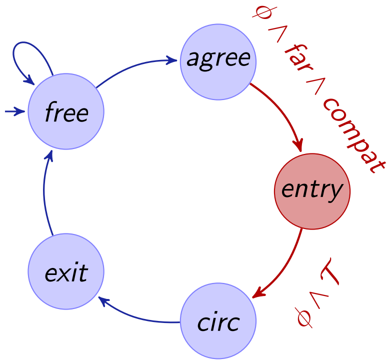


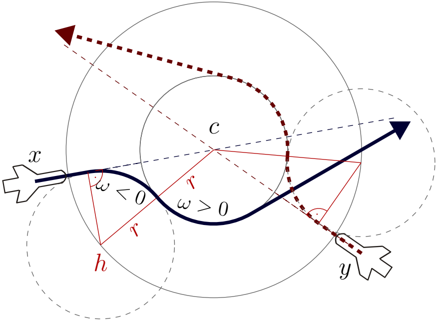


Example (d$\mathcal{L}$ formula of verification subgoal)

$$safe \land far \rightarrow [free](safe \land far)$$

Flyable Roundabout Maneuver: Entry

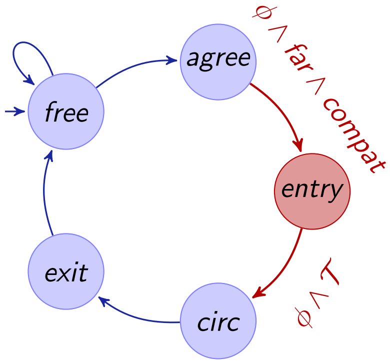


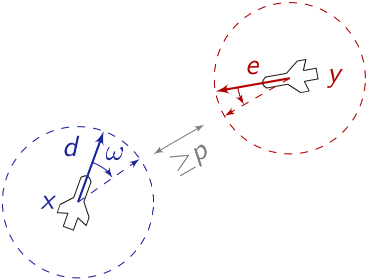


Example (d$\mathcal{L}$ formula of verification subgoal)

$$(r\omega)^2 = \|d\|^2 \land \|x-c\| = \sqrt{3}r \land \exists \lambda{\geq}0\,(x+\lambda d = c) \land$$
$$\|h-c\| = 2r \land d = -\omega(x-h)^\perp$$
$$\to [\mathcal{F}(-\omega)\,\&\,\|x-c\| \geq r]\,\big(\|x-c\| \leq r \to d = \omega(x-c)^\perp\big)$$

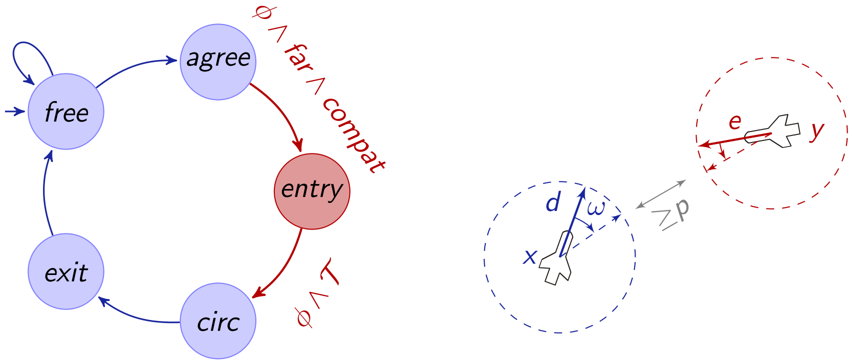
Flyable Roundabout Maneuver: Entry





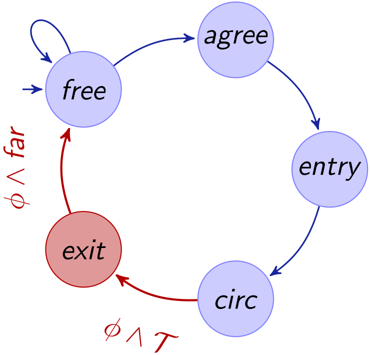
Example (d$\mathcal{L}$ formula of verification subgoal)

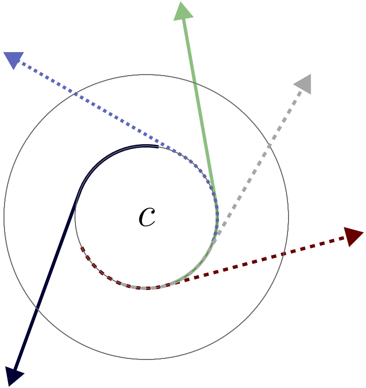
$$\|x - y\| \geq \sqrt{2}(p + 2bT) \wedge p \geq 0 \wedge \|d\|^2 \leq \|e\|^2 \leq b^2 \wedge b \geq 0 \wedge T \geq 0 \\ \rightarrow [entry]\,(\|x - y\| \geq p)$$



Example (d$\mathcal{L}$ formula of verification subgoal)

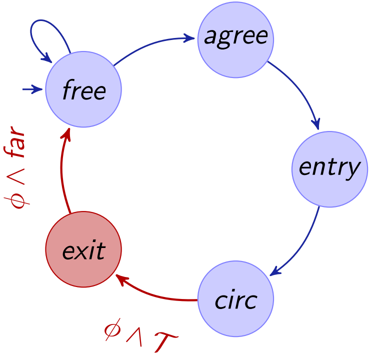
$$x = z \land \|d\|^2 \leq b^2 \land b \geq 0$$
$$\rightarrow [\tau := 0;\ \exists \omega\, \mathcal{F}(\omega) \land \tau' = 1]\, (\|x - z\|_\infty \leq \tau b)$$

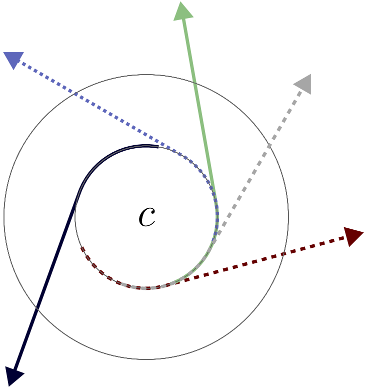




Example (d$\mathcal{L}$ formula of verification subgoal)

$$\mathcal{T} \land \|x - y\|^2 \geq p^2 \rightarrow [x' = d \land y' = e]\,(\|x - y\|^2 \geq p^2)$$

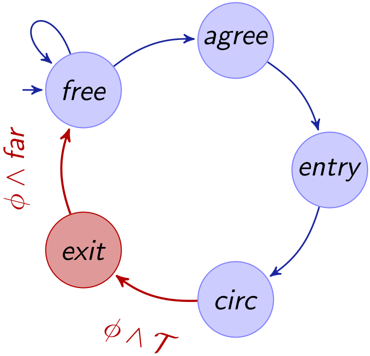


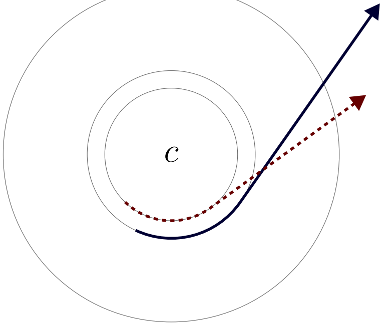


Example (d$\mathcal{L}$ formula of verification subgoal)

$$\mathcal{T} \wedge \|x - y\|^2 \geq p^2 \rightarrow [x' = d;\ y' = e]\,(\|x - y\|^2 \geq p^2)$$

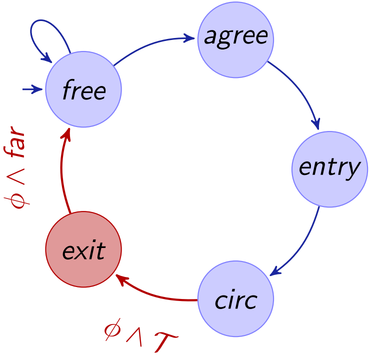
Flyable Roundabout Maneuver: Exit

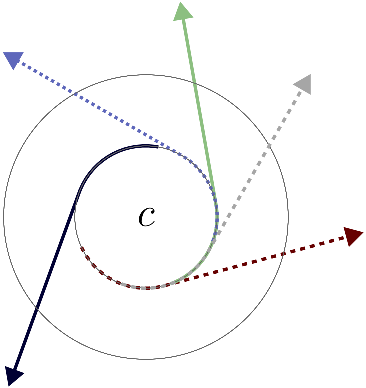




Example (d$\mathcal{L}$ formula of verification subgoal)

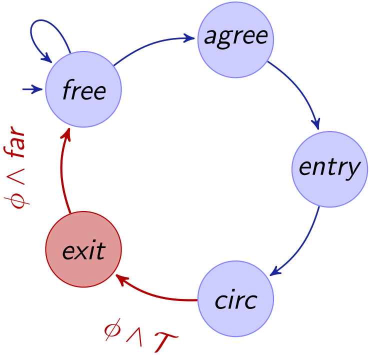
$$\mathcal{T} \land \|x - y\|^2 \geq p^2 \rightarrow [x' = d;\ y' = e]\,(\|x - y\|^2 \geq p^2)$$

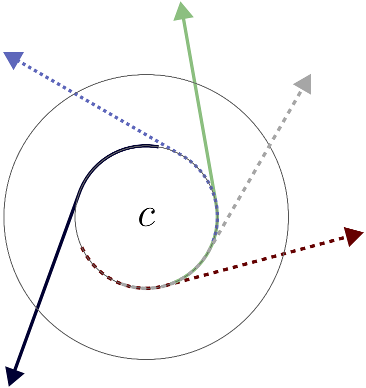




Example (d$\mathcal{L}$ formula of verification subgoal)

$$\mathcal{T} \wedge \|x - y\|^2 \geq p^2 \rightarrow [x' = d;\ y' = e]\,(\|x - y\|^2 \geq p^2)$$





Example (d$\mathcal{L}$ formula of verification subgoal)

$$\mathcal{T} \wedge d \neq e \rightarrow \forall a \, \langle x' = d \wedge y' = e \rangle \, (\|x - y\|^2 > a^2)$$

provable automatically!

$$\psi \equiv \phi \to [trm^*]\phi$$

$$\phi \equiv \|x-y\|^2 \geq p^2 \equiv (x_1-y_1)^2+(x_2-y_2)^2 \geq p^2$$

$$trm \equiv free; \quad entry; \quad \mathcal{F}(\omega) \land \mathcal{G}(\omega)$$

$$free \equiv \exists\omega\,\mathcal{F}(\omega) \land \exists\varpi\,\mathcal{G}(\varpi) \land \phi$$

$$entry \equiv \exists u\,\omega := u;\ \exists c\,(d := \omega(x-c)^{\perp} \land e := \omega(y-c)^{\perp})$$

$$\mathcal{F}(\omega) \equiv \begin{pmatrix} x_1' = v\cos\vartheta & = d_1 \\ \land\, x_2' = v\sin\vartheta & = d_2 \\ \land\, d_1' = v(-\sin\vartheta)\vartheta' & = -\omega d_2 \\ \land\, d_2' = v(\cos\vartheta)\vartheta' & = \quad \omega d_1 \end{pmatrix} \qquad \mathcal{G}(\varpi) \equiv \begin{pmatrix} y_1' = e_1 \\ \land\, y_2' = e_2 \\ \land\, e_1' = -\varpi e_2 \\ \land\, e_2' = \quad \varpi e_1 \end{pmatrix}$$

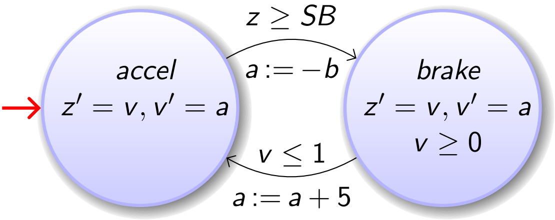
provable automatically!

$$
\begin{aligned}
\psi \quad & \equiv \phi \rightarrow [trm^*]\phi \\
\phi \quad & \equiv (x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2 \land (y_1 - z_1)^2 + (y_2 - z_2)^2 \geq p^2 \\
& \land (x_1 - z_1)^2 + (x_2 - z_2)^2 \geq p^2 \land (x_1 - u_1)^2 + (x_2 - u_2)^2 \geq p^2 \\
& \land (y_1 - u_1)^2 + (y_2 - u_2)^2 \geq p^2 \land (z_1 - u_1)^2 + (z_2 - u_2)^2 \geq p^2 \\
trm \quad & \equiv free; \quad entry; \\
& x_1' = d_1 \land x_2' = d_2 \land d_1' = -\omega_x d_2 \land d_2' = \omega_x d_1 \\
& \land y_1' = e_1 \land y_2' = e_2 \land e_1' = -\omega_y e_2 \land e_2' = \omega_y e_1 \\
& \land z_1' = f_1 \land z_2' = f_2 \land f_1' = -\omega_z f_2 \land f_2' = \omega_z f_1 \\
& \land u_1' = g_1 \land u_2' = g_2 \land g_1' = -\omega_u g_2 \land g_2' = \omega_u g_1 \\
free \quad & \equiv (\omega_x := *; \quad \omega_y := *; \quad \omega_z := *; \quad \omega_u := *; \\
& x_1' = d_1 \land x_2' = d_2 \land d_1' = -\omega_x d_2 \land d_2' = \omega_x d_1 \\
& \land y_1' = e_1 \land y_2' = e_2 \land e_1' = -\omega_y e_2 \land e_2' = \omega_y e_1 \\
& \land z_1' = f_1 \land z_2' = f_2 \land f_1' = -\omega_z f_2 \land f_2' = \omega_z f_1 \\
& \land u_1' = g_1 \land u_2' = g_2 \land g_1' = -\omega_u g_2 \land g_2' = \omega_u g_1 \land \phi)^* \\
entry \quad & \equiv \omega := *; \; c := *; \\
& d_1 := -\omega(x_2 - c_2); \; d_2 := \omega(x_1 - c_1); \\
& e_1 := -\omega(y_1 - c_1); \; e_2 := \omega(y_2 - c_2); \\
& f_1 := -\omega(z_1 - c_1); \; f_2 := \omega(z_2 - c_2); \\
& g_1 := -\omega(u_1 - c_1); \; g_2 := \omega(u_2 - c_2)
\end{aligned}
$$

Experimental Results (Air Traffic Control)

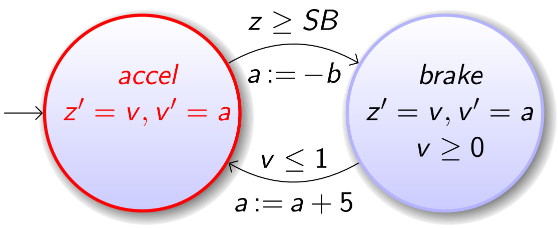
Case Study	Time(s)	Mem(Mb)	Steps	Dim
tangential roundabout (2a/c)	10.4	6.8	197	13
tangential roundabout (3a/c)	253.6	7.2	342	18
tangential roundabout (4a/c)	382.9	10.2	520	23
tangential roundabout (5a/c)	1882.9	39.1	735	28
bounded maneuver speed	0.5	6.3	14	4
flyable roundabout entry*	10.1	9.6	132	8
flyable entry feasible*	104.5	87.9	16	10
flyable entry circular	3.2	7.6	81	5
limited entry progress	1.9	6.5	60	8
entry separation	140.1	20.1	512	16
mutual negotiation successful	0.8	6.4	60	12
mutual negotiation feasible*	7.5	23.8	21	11
mutual far negotiation	2.4	8.1	67	14
simultaneous exit separation*	4.3	12.9	44	9
different exit directions	3.1	11.1	42	11

Outline Background



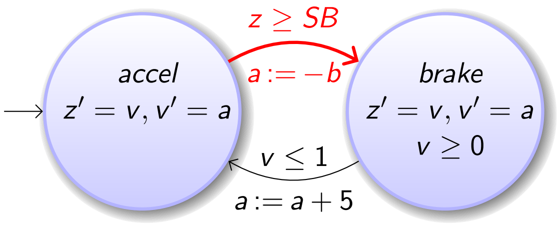
$$\rightsquigarrow$$

$$
\begin{aligned}
& q := accel; \\
& (\quad (?q = accel;\quad z' = v, v' = a) \\
& \cup\ (?q = accel \land z \geq SB;\quad a := -b;\quad q := brake;\quad ?v \geq 0) \\
& \cup\ (?q = brake;\quad z' = v, v' = a \,\&\, v \geq 0) \\
& \cup\ (?q = brake \land v \leq 1;\quad a := a + 5;\quad q := accel))^*
\end{aligned}
$$



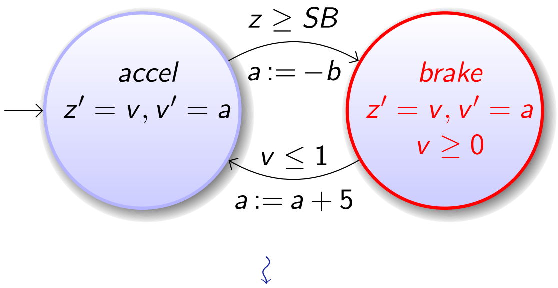
$$\rightsquigarrow$$

$$
\begin{aligned}
& q := accel;\\
& \big(\quad (?q = accel;\quad z' = v, v' = a)\\
& \cup\ (?q = accel \land z \geq SB;\quad a := -b;\quad q := brake;\quad ?v \geq 0)\\
& \cup\ (?q = brake;\quad z' = v, v' = a \,\&\, v \geq 0)\\
& \cup\ (?q = brake \land v \leq 1;\quad a := a + 5;\quad q := accel)\big)^*
\end{aligned}
$$



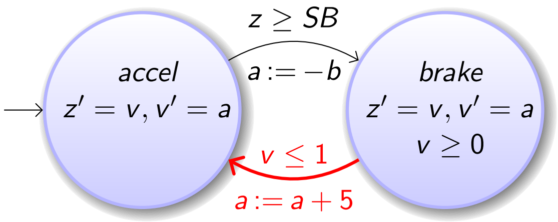
$\rightsquigarrow$

$$
\begin{aligned}
&q := accel;\\
&(\quad (?q = accel;\quad z' = v, v' = a)\\
&\cup\ (?q = accel \land z \geq SB;\quad a := -b;\quad q := brake;\quad ?v \geq 0)\\
&\cup\ (?q = brake;\quad z' = v, v' = a \,\&\, v \geq 0)\\
&\cup\ (?q = brake \land v \leq 1;\quad a := a + 5;\quad q := accel)\big)^*
\end{aligned}
$$



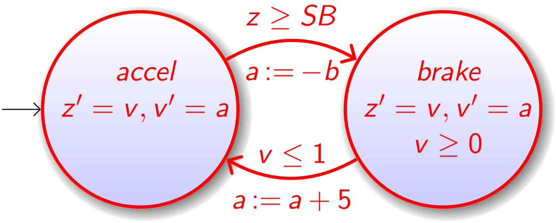
$$
\begin{aligned}
& q := accel; \\
& (\quad (?q = accel; \quad z' = v, v' = a) \\
& \cup \ (?q = accel \land z \geq SB; \quad a := -b; \quad q := brake; \quad ?v \geq 0) \\
& \cup \ (?q = brake; \quad z' = v, v' = a \,\&\, v \geq 0) \\
& \cup \ (?q = brake \land v \leq 1; \quad a := a + 5; \quad q := accel))^*
\end{aligned}
$$

Embedding Hybrid Automata as Hybrid Programs



$$\rightsquigarrow$$

$$
\begin{aligned}
& q := accel; \\
& \big(\quad (?q = accel; \quad z' = v, v' = a) \\
& \cup \ (?q = accel \land z \geq SB; \quad a := -b; \quad q := brake; \quad ?v \geq 0) \\
& \cup \ (?q = brake; \quad z' = v, v' = a \,\&\, v \geq 0) \\
& \cup \ (?q = brake \land v \leq 1; \quad a := a + 5; \quad q := accel) \big)^*
\end{aligned}
$$



$$\rightsquigarrow$$

$$
\begin{aligned}
& q := accel; \\
& \big(\ \ (?q = accel;\ \ z' = v, v' = a) \\
& \cup\ (?q = accel \land z \geq SB;\ \ a := -b;\ \ q := brake;\ \ ?v \geq 0) \\
& \cup\ (?q = brake;\ \ z' = v, v' = a \,\&\, v \geq 0) \\
& \cup\ (?q = brake \land v \leq 1;\ \ a := a + 5;\ \ q := accel)\big)^*
\end{aligned}
$$

Outline Background

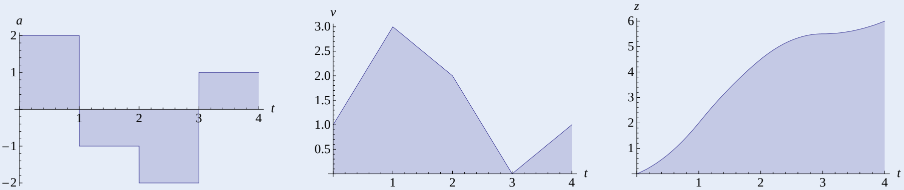
Q: I want to verify my car

Challenge

Q: I want to verify my car A: Hybrid systems

Challenge (Hybrid Systems)

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

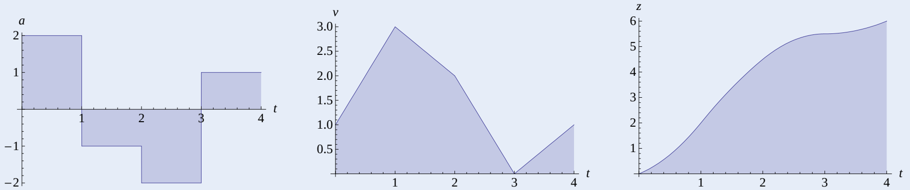


Cyber-Physical Systems: Hybrid Systems

Q: I want to verify my car A: Hybrid systems Q: But there's a lot of cars!

Challenge (Hybrid Systems)

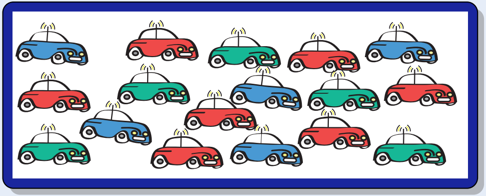
- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)



Cyber-Physical Systems:

Q: I want to verify a lot of cars

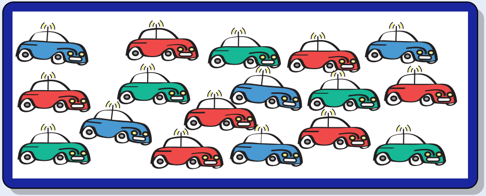
Challenge

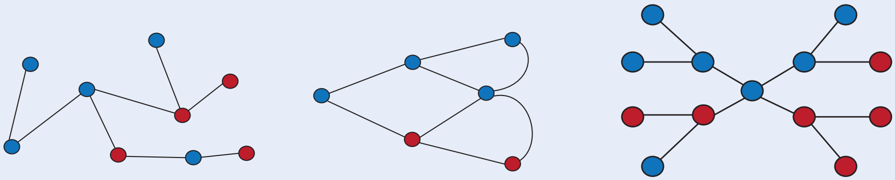


Q: I want to verify a lot of cars A: Distributed systems

Challenge (Distributed Systems)

- Local computation (finite state automaton)
- Remote communication (network graph)

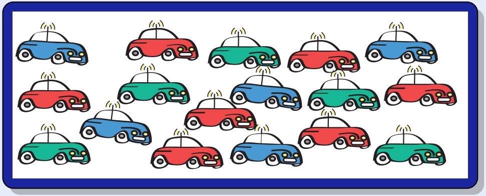


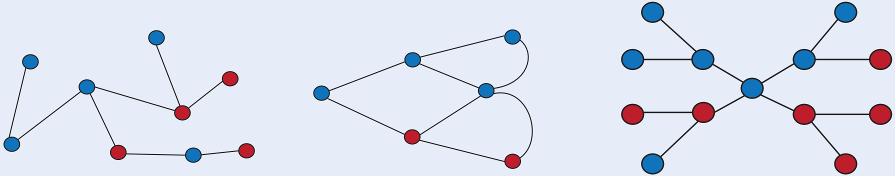


Q: I want to verify a lot of cars A: Distributed systems Q: But they move!

Challenge (Distributed Systems)

- Local computation (finite state automaton)
- Remote communication (network graph)

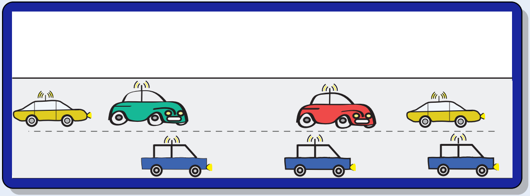




Cyber-Physical Systems:

Q: I want to verify lots of moving cars

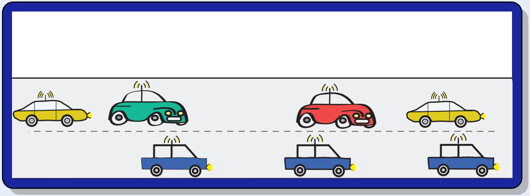
Challenge



Q: I want to verify lots of moving cars A: Distributed hybrid systems

Challenge (Distributed Hybrid Systems)

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)
- Structural dynamics (communication/coupling)

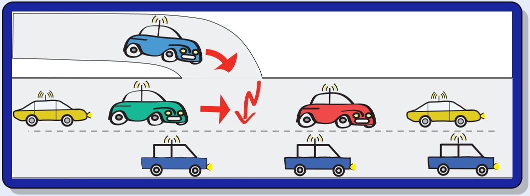


Cyber-Physical Systems: Distributed Hybrid Systems

Q: I want to verify lots of moving cars A: Distributed hybrid systems

Challenge (Distributed Hybrid Systems)

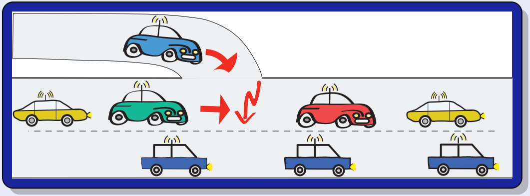
- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)
- Structural dynamics (communication/coupling)
- Dimensional dynamics (appearance)



Q: I want to verify lots of moving cars A: Distributed hybrid systems Q: How?

Challenge (Distributed Hybrid Systems)

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)
- Structural dynamics (communication/coupling)
- Dimensional dynamics (appearance)

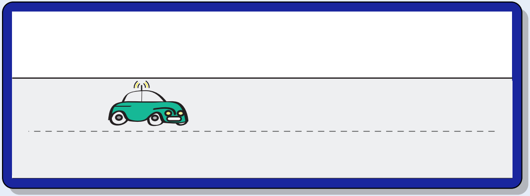


Model for Distributed Hybrid Systems

Q: How to model distributed hybrid systems

Model (Distributed Hybrid Systems)

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)
- Structural dynamics (communication/coupling)

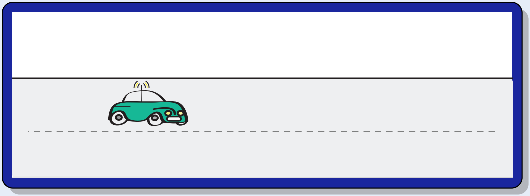


Model for Distributed Hybrid Systems

Q: How to model distributed hybrid systems

Model (Distributed Hybrid Systems)

- Continuous dynamics (differential equations)
  $x'' = a$
- Discrete dynamics (control decisions)
- Structural dynamics (communication/coupling)

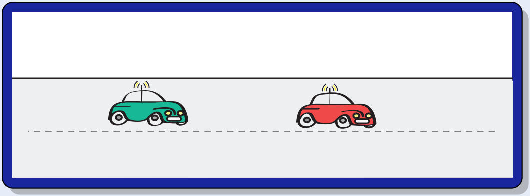


Model for Distributed Hybrid Systems

Q: How to model distributed hybrid systems

Model (Distributed Hybrid Systems)

- Continuous dynamics (differential equations)
  $x'' = a$
- Discrete dynamics (control decisions)
  $a := \texttt{if} .. \texttt{then}\, a\, \texttt{else}\, -b\, \texttt{fi}$
- Structural dynamics (communication/coupling)



Model for Distributed Hybrid Systems

Q: How to model distributed hybrid systems

Model (Distributed Hybrid Systems)

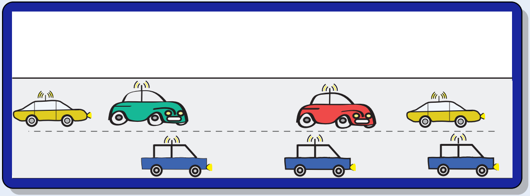
- Continuous dynamics (differential equations)

$$x'' = a$$

- Discrete dynamics (control decisions)

$$a := \texttt{if} \ldots \texttt{then}\, a\, \texttt{else} - b\, \texttt{fi}$$

- Structural dynamics (communication/coupling)

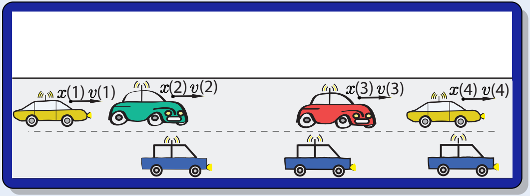


Model for Distributed Hybrid Systems

Q: How to model distributed hybrid systems

Model (Distributed Hybrid Systems)

- Continuous dynamics (differential equations)
  $$x'' = a$$
- Discrete dynamics (control decisions)
  $a := \texttt{if} .. \texttt{then}\ a\ \texttt{else}\ -b\ \texttt{fi}$
- Structural dynamics (communication/coupling)

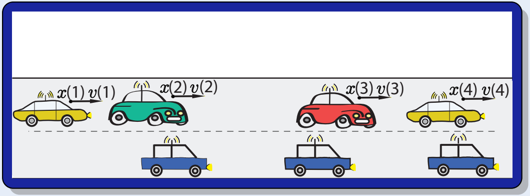


Model for Distributed Hybrid Systems

Q: How to model distributed hybrid systems

Model (Distributed Hybrid Systems)

- Continuous dynamics (differential equations)
  $$x(i)'' = a(i)$$
- Discrete dynamics (control decisions)
  $$a(i) := \texttt{if} .. \texttt{then}\, a \,\texttt{else}\, -b \,\texttt{fi}$$
- Structural dynamics (communication/coupling)



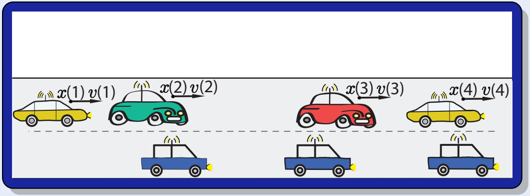
Q: How to model distributed hybrid systems

Model (Distributed Hybrid Systems)

- Continuous dynamics (differential equations)
  $\forall i\, x(i)'' = a(i)$
- Discrete dynamics (control decisions)

$\forall i\, a(i) := \texttt{if} .. \texttt{then}\, a\, \texttt{else}\, -b\, \texttt{fi}$

- Structural dynamics (communication/coupling)

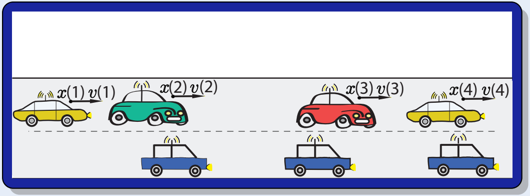


Model for Distributed Hybrid Systems

Q: How to model distributed hybrid systems

Model (Distributed Hybrid Systems)

- Continuous dynamics (differential equations)
  $\forall i\, x(i)'' = a(i)$
- Discrete dynamics (control decisions)
  $\forall i\, a(i) := \texttt{if} \,..\, \texttt{then}\, a\, \texttt{else}\, -b\, \texttt{fi}$
- Structural dynamics (communication/coupling)
  $\ell(i) := carInFrontOf(i)$

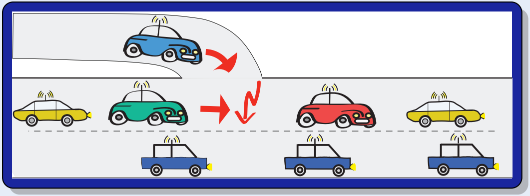


Model for Distributed Hybrid Systems

Q: How to model distributed hybrid systems A: Quantified Hybrid Programs

Model (Distributed Hybrid Systems)

- Continuous dynamics (differential equations)
  $\forall i\, x(i)'' = a(i)$
- Discrete dynamics (control decisions)
  $\forall i\, a(i) := \texttt{if} .. \texttt{then}\, a\, \texttt{else}\, -b\, \texttt{fi}$
- Structural dynamics (communication/coupling)
  $\ell(i) := carInFrontOf(i)$
- Dimensional dynamics (appearance)

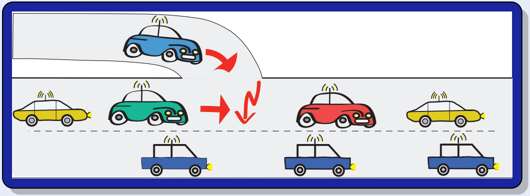


Model for Distributed Hybrid Systems

Q: How to model distributed hybrid systems A: Quantified Hybrid Programs

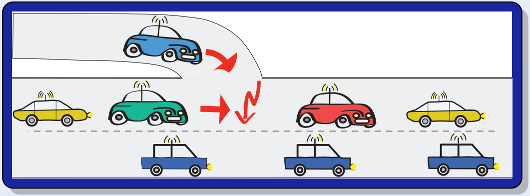
Model (Distributed Hybrid Systems)

- Continuous dynamics (differential equations)
  $\forall i\, x(i)'' = a(i)$
- Discrete dynamics (control decisions)
  $\forall i\, a(i) := \texttt{if}\, ..\, \texttt{then}\, a\, \texttt{else}\, -b\, \texttt{fi}$
- Structural dynamics (communication/coupling)
  $\ell(i) := \mathit{carInFrontOf}(i)$
- Dimensional dynamics (appearance)
  $n := \texttt{new}\ \mathit{Car}$



Q: How to model distributed hybrid systems A: Quantified Hybrid Programs

Model (Distributed Hybrid Systems)

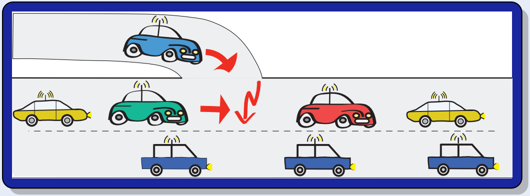


- Continuous dynamics (differential equations)
  $\forall i\, x(i)'' = a(i)$
- Discrete dynamics (control decisions)
  $\forall i\, a(i) := \texttt{if} .. \texttt{then}\, a\, \texttt{else} -b\, \texttt{fi}$
- Structural dynamics (communication/coupling)
  $\ell(i) := carInFrontOf(i)$
- Dimensional dynamics (appearance)
  $n := \texttt{new}\ Car$

$\Rightarrow$ Communication
$d(i, \ell(i)) := d(i, \ell(i)) + 10$

Q: How to model distributed hybrid systems A: Quantified Hybrid Programs

Model (Distributed Hybrid Systems)

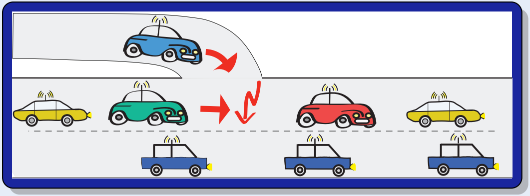


- Continuous dynamics (differential equations)
  $\forall i\, x(i)'' = a(i)$
- Discrete dynamics (control decisions)
  $\forall i\, a(i) := \texttt{if} .. \texttt{then}\, a\, \texttt{else} -b\, \texttt{fi}$
- Structural dynamics (communication/coupling)
  $\ell(i) := \mathit{carInFrontOf(i)}$
- Dimensional dynamics (appearance)
  $n := \texttt{new}\ \mathit{Car}$

$\Rightarrow$ Communication
$\forall i\, d(i, \ell(i)) := d(i, \ell(i)) + 10$

Q: How to model distributed hybrid systems A: Quantified Hybrid Programs

Model (Distributed Hybrid Systems)



- Continuous dynamics (differential equations)
  $$\forall i\ x(i)'' = a(i)$$
- Discrete dynamics (control decisions)
  $$\forall i\ a(i) := \mathtt{if}\ ..\ \mathtt{then}\ a\ \mathtt{else}\ -b\ \mathtt{fi}$$
- Structural dynamics (communication/coupling)
  $$\ell(i) := carInFrontOf(i)$$
- Dimensional dynamics (appearance)
  $$n := \mathtt{new}\ Car$$

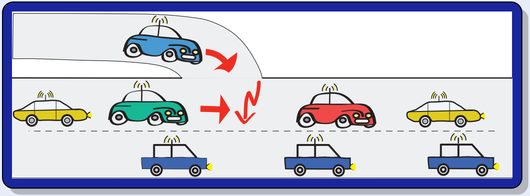
$\Rightarrow$ Communication
$$\forall i\ d(i, \ell(i)) := d(i, \ell(i)) + 10$$

$\Rightarrow$ Discrete structural dynamics
$$\ell(i) := \ell(\ell(i))$$

Q: How to model distributed hybrid systems A: Quantified Hybrid Programs

Model (Distributed Hybrid Systems)

- Continuous dynamics (differential equations)
  $\forall i\, x(i)'' = a(i)$
- Discrete dynamics (control decisions)
  $\forall i\, a(i) := \texttt{if} .. \texttt{then}\, a\, \texttt{else} -b\, \texttt{fi}$
- Structural dynamics (communication/coupling)
  $\ell(i) := carInFrontOf(i)$
- Dimensional dynamics (appearance)
  $n := \texttt{new}\ Car$



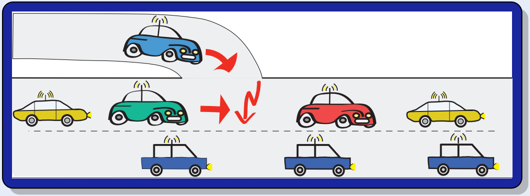
⇒ Communication
$\forall i\, d(i, \ell(i)) := d(i, \ell(i)) + 10$

⇒ Discrete structural dynamics
$\ell(i) := \ell(\ell(i))$

⇒ Continuous structural dynamics
$x(i)'' = a(i) + c(i, \ell(i))a(\ell(i))$

Q: How to model distributed hybrid systems A: Quantified Hybrid Programs

Model (Distributed Hybrid Systems)



- Continuous dynamics (differential equations) $\forall i\, x(i)'' = a(i)$
- Discrete dynamics (control decisions)

$\forall i\, a(i) := \texttt{if} .. \texttt{then}\, a\, \texttt{else}\, -b\, \texttt{fi}$

- Structural dynamics (communication/coupling) $\ell(i) := carInFrontOf(i)$
- Dimensional dynamics (appearance) $n := \texttt{new}\, Car$

$\Rightarrow$ Communication

$$\forall i\, d(i, \ell(i)) := d(i, \ell(i)) + 10$$

$\Rightarrow$ Discrete structural dynamics

$$\ell(i) := \ell(\ell(i))$$

$\Rightarrow$ Continuous structural dynamics

$$\forall i\, x(i)'' = a(i) + c(i, \ell(i))a(\ell(i))$$

Related Work

Shift [13] The Hybrid System Simulation Programming Language

R-Charon [14] Modeling Language for Reconfigurable Hybrid Systems

Hybrid CSP [15] Semantics in Extended Duration Calculus

Φ-calculus [18] Semantics in rich set theory

HyPA [16] Translate fragment into normal form.

ACP^{srt}_{hs} [19] Modeling language proposal

χ process algebra [17] Simulation, translation of fragments to PHAVER, UPPAAL

OBSHS [20] Partial random simulation of objects

Related Work

Shift [13] The Hybrid System Simulation Programming Language

Hybrid CSP [15] Semantics in Extended Duration Calculus

HyPA [16] Translate fragment into normal form.

χ process algebra [17] Simulation, translation of fragments to PHAVER, UPPAAL

R-Charon [14] Modeling Language for Reconfigurable Hybrid Systems

Φ-calculus [18] Semantics in rich set theory

ACP^{srt}_{hs} [19] Modeling language proposal

OBSHS [20] Partial random simulation of objects

Quantified Differential Dynamic Logic Qd$\mathcal{L}$: Syntax

Definition (Quantified hybrid program α)

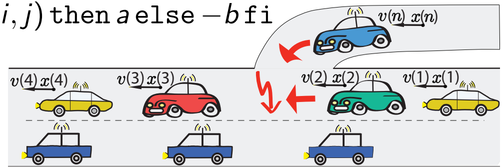
$\forall i : C\ x(i)' = \theta$	(quantified ODE)	
$\forall i : C\ x(i) := \theta$	(quantified assignment)	jump & test
$?\chi$	(conditional execution)	jump & test
$\alpha; \beta$	(seq. composition)	Kleene algebra
$\alpha \cup \beta$	(nondet. choice)	Kleene algebra
α^*	(nondet. repetition)	Kleene algebra

Definition (Quantified hybrid program α)

$\forall i : C\ x(i)' = \theta$	(quantified ODE)	
$\forall i : C\ x(i) := \theta$	(quantified assignment)	jump & test
$?\chi$	(conditional execution)	jump & test
$\alpha; \beta$	(seq. composition)	Kleene algebra
$\alpha \cup \beta$	(nondet. choice)	Kleene algebra
α^*	(nondet. repetition)	Kleene algebra

$$DCCS \equiv (ctrl; drive)^*$$

$$ctrl \equiv \forall i : C\ a(i) := \mathtt{if}\ \forall j : C\ far(i,j)\ \mathtt{then}\ a\ \mathtt{else}\ -b\ \mathtt{fi}$$
$$drive \equiv \forall i : C\ x(i)'' = a(i)$$



Quantified Differential Dynamic Logic Qd$\mathcal{L}$: Syntax

Definition (Quantified hybrid program α)

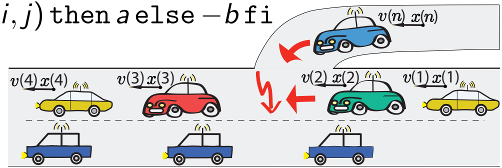
$\forall i : C\ x(i)' = \theta$	(quantified ODE)	
$\forall i : C\ x(i) := \theta$	(quantified assignment)	jump & test
$?\chi$	(conditional execution)	
$\alpha; \beta$	(seq. composition)	Kleene algebra
$\alpha \cup \beta$	(nondet. choice)	
α^*	(nondet. repetition)	

$$DCCS \equiv (appear; ctrl; drive)^*$$

$$appear \equiv n := \mathtt{new}\ C;\quad ?(\forall j : C\ far(j, n))$$

$$ctrl \equiv \forall i : C\ a(i) := \mathtt{if}\ \forall j : C\ far(i, j)\ \mathtt{then}\ a\ \mathtt{else}\ -b\ \mathtt{fi}$$

$$drive \equiv \forall i : C\ x(i)'' = a(i)$$



Definition (Quantified hybrid program α)

$\forall i : C \; x(i)' = \theta$	(quantified ODE)	
$\forall i : C \; x(i) := \theta$	(quantified assignment)	jump & test
$?\chi$	(conditional execution)	
$\alpha ; \beta$	(seq. composition)	Kleene algebra
$\alpha \cup \beta$	(nondet. choice)	
α^*	(nondet. repetition)	

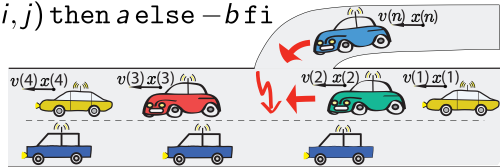
$$DCCS \equiv (appear\,;\, ctrl\,;\, drive)^*$$

$$appear \equiv n := \mathtt{new}\ C;\quad ?(\forall j : C\ far(j, n))$$

$$ctrl \equiv \forall i : C\ a(i) := \mathtt{if}\ \forall j : C\ far(i, j)\ \mathtt{then}\ a\ \mathtt{else}\ -b\ \mathtt{fi}$$

$$drive \equiv \forall i : C\ x(i)'' = a(i)$$

new C is definable!



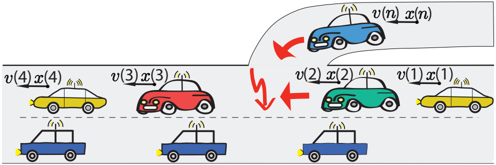
Definition (Qd$\mathcal{L}$ Formula ϕ)

$\neg, \wedge, \vee, \rightarrow, \ \forall x, \exists x, \ =, \leq, \ +, \cdot$ (ℝ-first-order part)

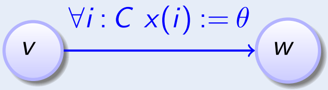
$[\alpha]\phi, \ \langle\alpha\rangle\phi$ (dynamic part)

$$\forall i, j : C \ far(i,j) \rightarrow [(appear; ctrl; drive)^*] \ \forall i{\neq}j : C \ x(i) \neq x(j)$$

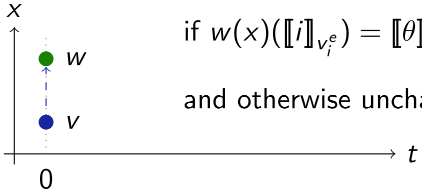
$$far(i,j) \equiv i \neq j \rightarrow x(i) < x(j) \wedge v(i) \leq v(j) \wedge a(i) \leq a(j) \vee x(i) > x(j) \wedge v(i) \geq v(j) \wedge a(i) \geq a(j) \dots$$



Definition (Quantified hybrid program α: transition semantics)



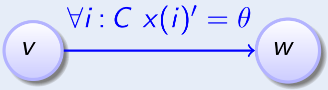
Example



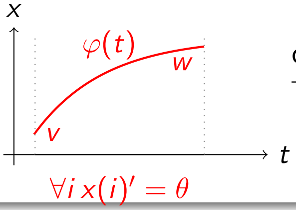
if $w(x)([\![i]\!]_{v_i^e}) = [\![\theta]\!]_{v_i^e}$ (for all e)

and otherwise unchanged

Definition (Quantified hybrid program α: transition semantics)



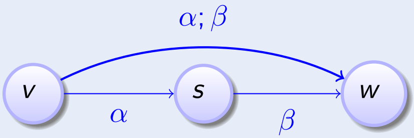
Example



$$\frac{\mathrm{d}\, [\![x(i)]\!]_{\varphi(t)_i^e}}{\mathrm{d}t}(\zeta) = [\![\theta]\!]_{\varphi(\zeta)_i^e}$$

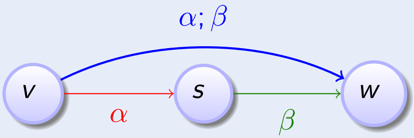
(for all e)

Definition (Quantified hybrid program α: transition semantics)

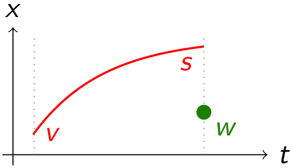


Example

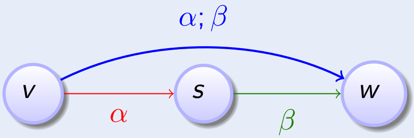
Definition (Quantified hybrid program α: transition semantics)



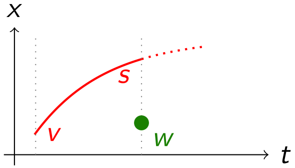
Example



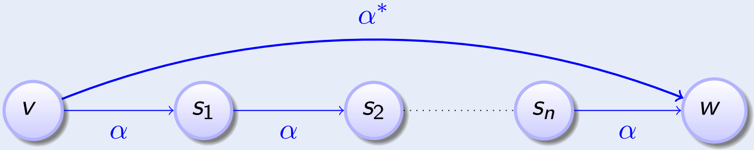
Definition (Quantified hybrid program α: transition semantics)



Example



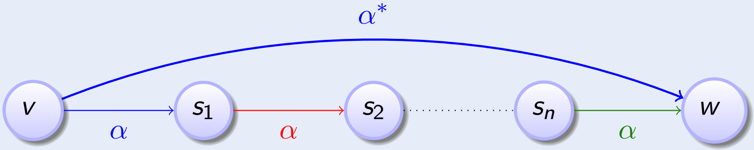
Definition (Quantified hybrid program α: transition semantics)



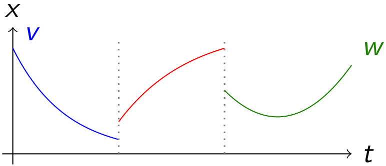
Example

Quantified Differential Dynamic Logic Qd$\mathcal{L}$: Semantics

Definition (Quantified hybrid program α: transition semantics)

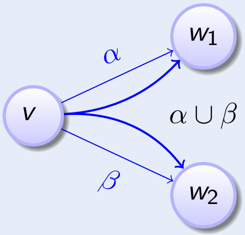


Example



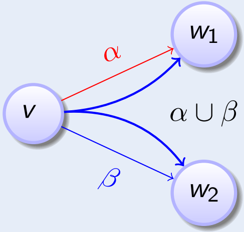
Quantified Differential Dynamic Logic Qd$\mathcal{L}$: Semantics

Definition (Quantified hybrid program α: transition semantics)

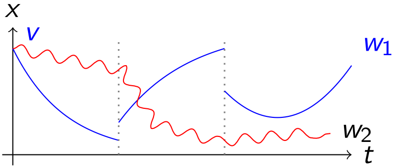


Example

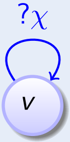
Definition (Quantified hybrid program α: transition semantics)



Example

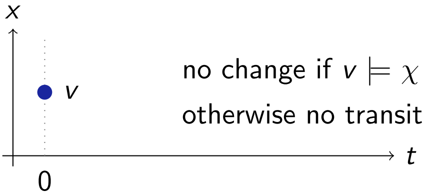


Definition (Quantified hybrid program α: transition semantics)



if $v \models \chi$

Example



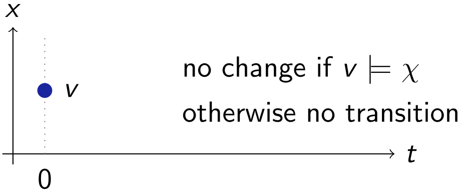
no change if $v \models \chi$

otherwise no transition

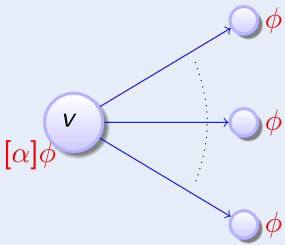
Definition (Quantified hybrid program α: transition semantics)

if $v \not\models \chi$

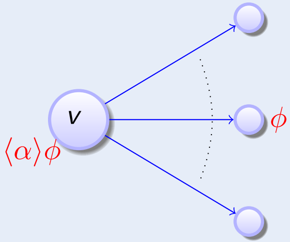
Example



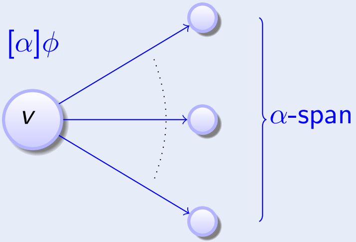
Definition (QdL Formula ϕ)



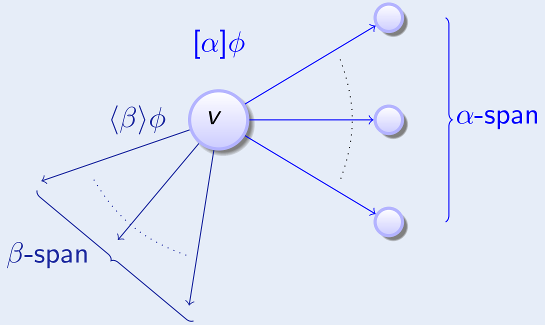
Definition (QdL Formula ϕ)



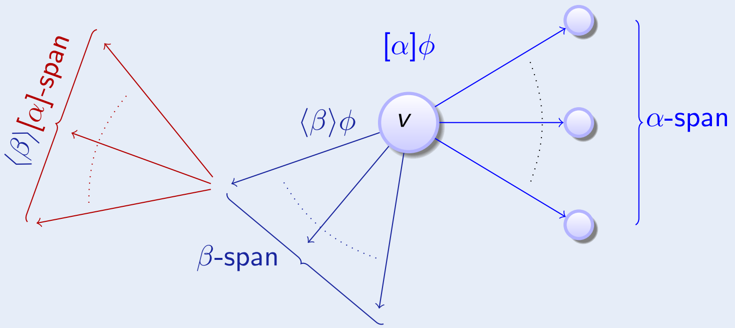
Definition (QdL Formula ϕ)



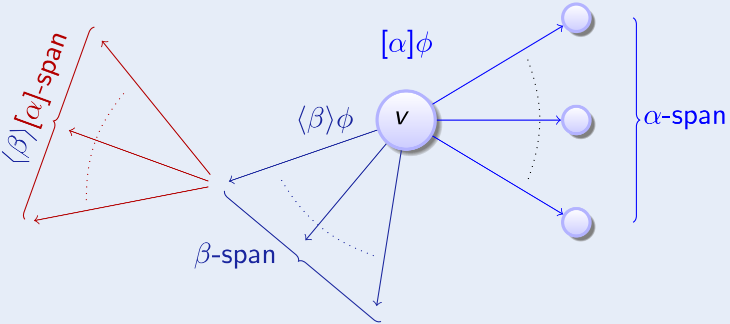
Definition (Qd$\mathcal{L}$ Formula ϕ)



Definition (QdL Formula ϕ)

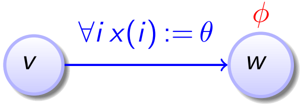


Definition (Qd$\mathcal{L}$ Formula ϕ)



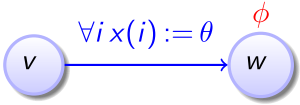
compositional semantics $\Rightarrow$ compositional calculus!

$$\frac{\forall i\,(i = \vec{u} \to \phi(\theta))}{\phi([\forall i\, x(i) := \theta]x(\vec{u}))}$$

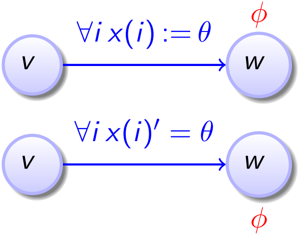


Proof Calculus: Quantified Differential Dynamic Logic

$$\frac{\forall i\,(i = [\forall i\, x(i) := \theta]\vec{u} \rightarrow \phi(\theta))}{\phi([\forall i\, x(i) := \theta]x(\vec{u}))}$$



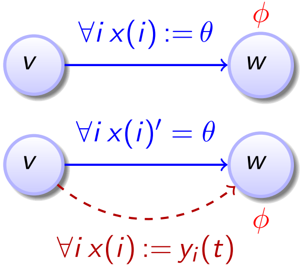
$$\frac{\forall i\,(i = [\forall i\, x(i) := \theta]\vec{u} \to \phi(\theta))}{\phi([\forall i\, x(i) := \theta]x(\vec{u}))}$$



$$\frac{\exists t{\geq}0\, \langle \forall i\, x(i) := y_i(t)\rangle \phi}{\langle \forall i\, x(i)' = \theta\rangle \phi}$$

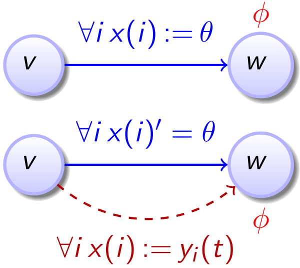
$$\frac{\forall i\,(i = [\forall i\, x(i) := \theta]\vec{u} \to \phi(\theta))}{\phi([\forall i\, x(i) := \theta]x(\vec{u}))}$$

$$\frac{\exists t{\geq}0\, \langle \forall i\, x(i) := y_i(t)\rangle\phi}{\langle \forall i\, x(i)' = \theta\rangle\phi}$$



$$\frac{\forall i\,(i = [\forall i\, x(i) := \theta]\vec{u} \rightarrow \phi(\theta))}{\phi([\forall i\, x(i) := \theta]x(\vec{u}))}$$

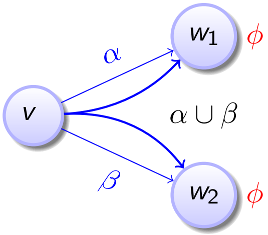
$$\frac{\exists t{\geq}0\, \langle \forall i\, x(i) := y_i(t)\rangle\phi}{\langle \forall i\, x(i)' = \theta\rangle\phi}$$



solve infinite-dimensional diff. eqn.?

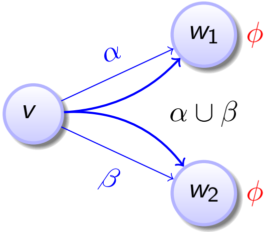
compositional semantics $\Rightarrow$ compositional rules!

$$\frac{[\alpha]\phi \land [\beta]\phi}{[\alpha \cup \beta]\phi}$$

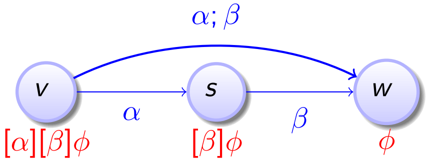


Proof Calculus: Quantified Differential Dynamic Logic

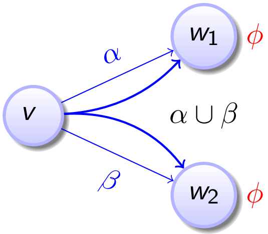
$$\frac{[\alpha]\phi \land [\beta]\phi}{[\alpha \cup \beta]\phi}$$



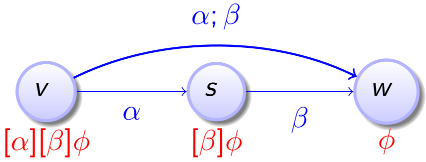
$$\frac{[\alpha][\beta]\phi}{[\alpha;\beta]\phi}$$



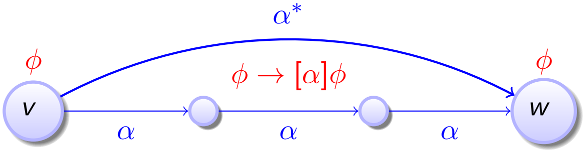
$$\frac{[\alpha]\phi \land [\beta]\phi}{[\alpha \cup \beta]\phi}$$



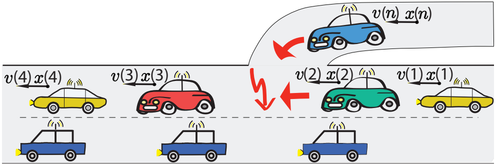
$$\frac{[\alpha][\beta]\phi}{[\alpha;\beta]\phi}$$



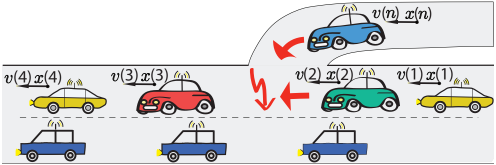
$$\frac{\phi \quad (\phi \to [\alpha]\phi)}{[\alpha^*]\phi}$$



$$\frac{}{\forall i{\neq}j\, x(i){\neq}x(j) \to [\forall i\, x(i)' = v(i), v(i)' = -b]\, \forall j{\neq}k\, x(j){\neq}x(k)}$$

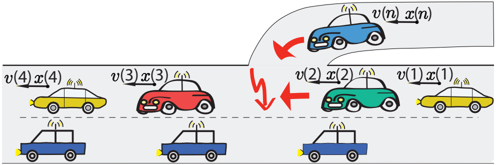


$$\frac{\forall i{\neq}j\, x(i){\neq}x(j) \rightarrow \forall t{\geq}0\, [\forall i\, x(i) := -\frac{b}{2}t^2 + v(i)t + x(i)]\, \forall j{\neq}k\, x(j){\neq}x(k)}{\forall i{\neq}j\, x(i){\neq}x(j) \rightarrow [\forall i\, x(i)' = v(i), v(i)' = -b]\, \forall j{\neq}k\, x(j){\neq}x(k)}$$



Deduction Modulo

$$\dfrac{\dfrac{\forall i{\neq}j\, x(i){\neq}x(j) \rightarrow [\forall i\, x(i)' = v(i), v(i)' = -b]\, \forall j{\neq}k\, x(j){\neq}x(k)}{\forall i{\neq}j\, x(i){\neq}x(j) \rightarrow \forall t{\geq}0\, [\forall i\, x(i) := -\frac{b}{2}t^2 + v(i)t + x(i)]\, \forall j{\neq}k\, x(j){\neq}x(k)}}{\forall i{\neq}j\, x(i){\neq}x(j) \rightarrow \forall t{\geq}0\, \forall j{\neq}k\, [\forall i\, x(i) := -\frac{b}{2}t^2 + v(i)t + x(i)]\, x(j){\neq}x(k)}$$



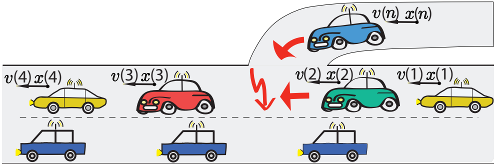
Deduction Modulo

$$\forall i{\neq}j\, x(i){\neq}x(j) \to \forall t{\geq}0\, \forall j{\neq}k\, \left(-\tfrac{b}{2}t^2 + v(j)t + x(j) \neq -\tfrac{b}{2}t^2 + v(k)t + x(k)\right)$$

$$\forall i{\neq}j\, x(i){\neq}x(j) \to \forall t{\geq}0\, \forall j{\neq}k\, [\forall i\, x(i) := -\tfrac{b}{2}t^2 + v(i)t + x(i)]\, x(j){\neq}x(k)$$

$$\forall i{\neq}j\, x(i){\neq}x(j) \to \forall t{\geq}0\, [\forall i\, x(i) := -\tfrac{b}{2}t^2 + v(i)t + x(i)]\, \forall j{\neq}k\, x(j){\neq}x(k)$$

$$\forall i{\neq}j\, x(i){\neq}x(j) \to [\forall i\, x(i)' = v(i), v(i)' = -b]\, \forall j{\neq}k\, x(j){\neq}x(k)$$



Deduction Modulo

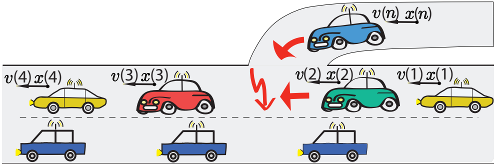
$$\forall i{\neq}j\, x(i){\neq}x(j) \rightarrow \forall j{\neq}k\, \forall t{\geq}0\, (-\tfrac{b}{2}t^2 + v(j)t + x(j) \neq -\tfrac{b}{2}t^2 + v(k)t + x(k))$$

$$\forall i{\neq}j\, x(i){\neq}x(j) \rightarrow \forall t{\geq}0\, \forall j{\neq}k\, (-\tfrac{b}{2}t^2 + v(j)t + x(j) \neq -\tfrac{b}{2}t^2 + v(k)t + x(k))$$

$$\forall i{\neq}j\, x(i){\neq}x(j) \rightarrow \forall t{\geq}0\, \forall j{\neq}k\, [\forall i\, x(i) := -\tfrac{b}{2}t^2 + v(i)t + x(i)]\, x(j){\neq}x(k)$$

$$\forall i{\neq}j\, x(i){\neq}x(j) \rightarrow \forall t{\geq}0\, [\forall i\, x(i) := -\tfrac{b}{2}t^2 + v(i)t + x(i)]\, \forall j{\neq}k\, x(j){\neq}x(k)$$

$$\forall i{\neq}j\, x(i){\neq}x(j) \rightarrow [\forall i\, x(i)' = v(i), v(i)' = -b]\, \forall j{\neq}k\, x(j){\neq}x(k)$$



Deduction Modulo

$$\forall i{\neq}j\, x(i){\neq}x(j) \rightarrow \forall j{\neq}k\, (x(j) \le x(k) \land v(j) \le v(k) \lor x(j) \ge x(k) \land v(j) \ge v$$

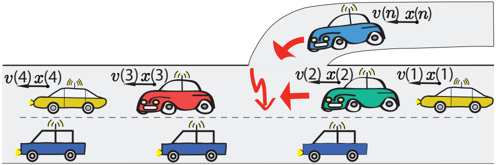
$$\forall i{\neq}j\, x(i){\neq}x(j) \rightarrow \forall j{\neq}k\, \forall t{\ge}0\, (-\tfrac{b}{2}t^2 + v(j)t + x(j) \neq -\tfrac{b}{2}t^2 + v(k)t + x(k))$$

$$\forall i{\neq}j\, x(i){\neq}x(j) \rightarrow \forall t{\ge}0\, \forall j{\neq}k\, (-\tfrac{b}{2}t^2 + v(j)t + x(j) \neq -\tfrac{b}{2}t^2 + v(k)t + x(k))$$

$$\forall i{\neq}j\, x(i){\neq}x(j) \rightarrow \forall t{\ge}0\, \forall j{\neq}k\, [\forall i\, x(i) := -\tfrac{b}{2}t^2 + v(i)t + x(i)]\, x(j){\neq}x(k)$$

$$\forall i{\neq}j\, x(i){\neq}x(j) \rightarrow \forall t{\ge}0\, [\forall i\, x(i) := -\tfrac{b}{2}t^2 + v(i)t + x(i)]\, \forall j{\neq}k\, x(j){\neq}x(k)$$

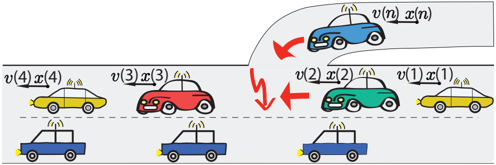
$$\forall i{\neq}j\, x(i){\neq}x(j) \rightarrow [\forall i\, x(i)' = v(i), v(i)' = -b]\, \forall j{\neq}k\, x(j){\neq}x(k)$$



Actual Existence and Creation

Actual Existence Function $\mathsf{E}(\cdot)$

$$\mathsf{E}(i) = \begin{cases} 0 & \text{if } i \text{ denotes a possible object} \\ 1 & \text{if } i \text{ denotes an actively existing objects} \end{cases}$$

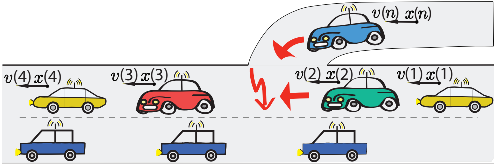


Actual Existence and Creation

Actual Existence Function $\mathsf{E}(\cdot)$

$$\mathsf{E}(i) = \begin{cases} 0 & \text{if } i \text{ denotes a possible object} \\ 1 & \text{if } i \text{ denotes an actively existing objects} \end{cases}$$

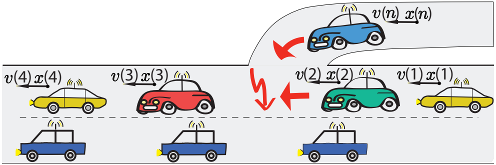
$$\frac{}{[n := \mathtt{new}\ C]\phi}$$



Actual Existence Function E(·)

$$\mathrm{E}(i) = \begin{cases} 0 & \text{if } i \text{ denotes a possible object} \\ 1 & \text{if } i \text{ denotes an actively existing objects} \end{cases}$$

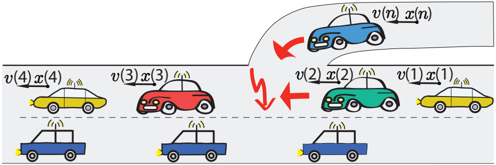
$$\frac{[(\forall j : C \ \ n := j); \qquad\qquad\qquad]\phi}{[n := \mathtt{new}\ C]\phi}$$



Actual Existence Function $\mathrm{E}(\cdot)$

$$\mathrm{E}(i) = \begin{cases} 0 & \text{if } i \text{ denotes a possible object} \\ 1 & \text{if } i \text{ denotes an actively existing objects} \end{cases}$$

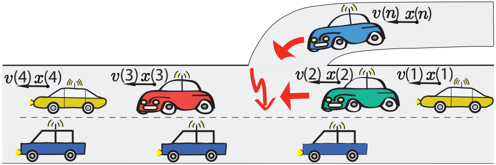
$$\frac{[(\forall j : C \;\; n := j);\;\; ?(\mathrm{E}(n) = 0);\qquad\qquad]\phi}{[n := \mathtt{new}\ C]\phi}$$



Actual Existence Function $\mathrm{E}(\cdot)$

$$\mathrm{E}(i) = \begin{cases} 0 & \text{if } i \text{ denotes a possible object} \\ 1 & \text{if } i \text{ denotes an actively existing objects} \end{cases}$$

$$\frac{[(\forall j : C\ \ n := j);\ \ ?(\mathrm{E}(n) = 0);\ \ \mathrm{E}(n) := 1]\phi}{[n := \mathtt{new}\ C]\phi}$$

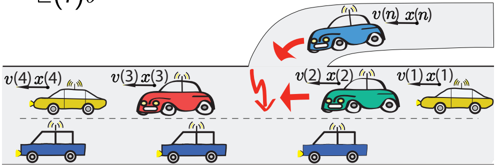


Actual Existence Function $\mathsf{E}(\cdot)$

$$\mathsf{E}(i) = \begin{cases} 0 & \text{if } i \text{ denotes a possible object} \\ 1 & \text{if } i \text{ denotes an actively existing objects} \end{cases}$$

$$\frac{[(\forall j : C\ n := j);\ ?(\mathsf{E}(n) = 0);\ \mathsf{E}(n) := 1]\phi}{[n := \mathtt{new}\ C]\phi}$$

$$\forall i : C!\ \phi \equiv \forall i : C\ (\mathsf{E}(i) = 1 \rightarrow \phi)$$
$$\forall i : C!\ f(i) := \theta \equiv \forall i : C\ f(i) := (\mathtt{if}\ \mathsf{E}(i) = 1\ \mathtt{then}\ \theta\ \mathtt{else}\ f(i)\ \mathtt{fi})$$
$$\forall i : C!\ f(i)' = \theta \equiv \forall i : C\ f(i)' = \mathsf{E}(i)\theta$$



Soundness and Completeness

Theorem (Relative Completeness)

QdL *calculus is a sound & complete axiomatisation of distributed hybrid systems relative to quantified differential equations.* Proof 16p.

André Platzer.
Quantified differential dynamic logic for distributed hybrid systems.
In Anuj Dawar and Helmut Veith, editors,
CSL, vol. 6247 of *LNCS*, 469–483. Springer, 2010.

Soundness and Completeness

Theorem (Relative Completeness)

Qd$\mathcal{L}$ *calculus is a sound & complete axiomatisation of distributed hybrid systems relative to quantified differential equations.* Proof 16p.

Corollary (Proof-theoretical Alignment)

proving distributed hybrid systems = proving dynamical systems!

André Platzer.
Quantified differential dynamic logic for distributed hybrid systems.
In Anuj Dawar and Helmut Veith, editors,
CSL, vol. 6247 of *LNCS*, 469–483. Springer, 2010.

Soundness and Completeness

Theorem (Relative Completeness)

Qd$\mathcal{L}$ *calculus is a sound & complete axiomatisation of distributed hybrid systems relative to quantified differential equations.* Proof 16p.

Corollary (Proof-theoretical Alignment)

proving distributed hybrid systems = proving dynamical systems!

Corollary (Decomposition!)

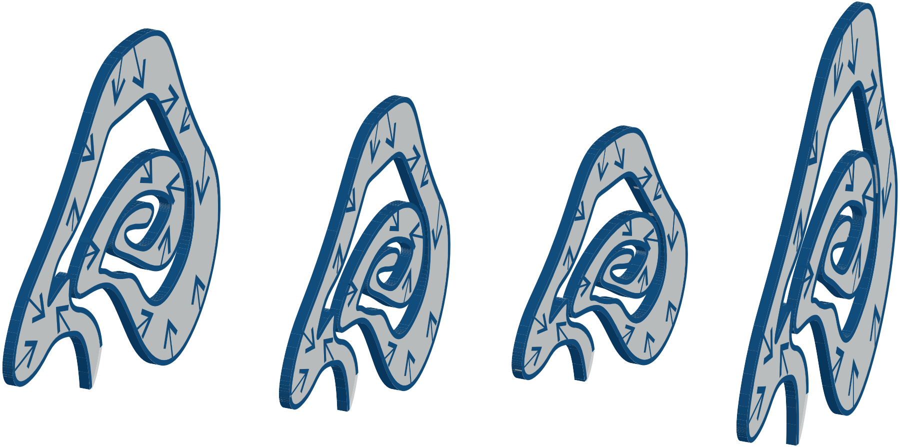
distributed hybrid systems can be verified by recursive decomposition

André Platzer.
Quantified differential dynamic logic for distributed hybrid systems.
In Anuj Dawar and Helmut Veith, editors,
CSL, vol. 6247 of *LNCS*, 469–483. Springer, 2010.

Quantified Differential Invariants

Definition (Quantified Differential Invariant)

Quantified formula F closed under total differentiation with respect to quantified differential constraints



Definition (Syntactic total derivation D)

$$
\begin{aligned}
D(r) &= 0 && \text{if } r \text{ a number symbol}\\
D(x(i)) &= x(i)' && \text{if } x : C \to \mathbb{R},\ C \neq \mathbb{R}\\
D(a+b) &= D(a) + D(b)\\
D(a \cdot b) &= D(a) \cdot b + a \cdot D(b)\\
D(a/b) &= (D(a) \cdot b - a \cdot D(b))/b^2
\end{aligned}
$$

Derivations and Differentiation

Definition (Syntactic total derivation D)

$$
\begin{aligned}
D(r) &= 0 && \text{if } r \text{ a number symbol}\\
D(x(i)) &= x(i)' && \text{if } x : C \to \mathbb{R},\ C \neq \mathbb{R}\\
D(a+b) &= D(a) + D(b)\\
D(a \cdot b) &= D(a) \cdot b + a \cdot D(b)\\
D(a/b) &= (D(a) \cdot b - a \cdot D(b))/b^2\\
D(a \geq b) &\equiv D(a) \geq D(b) && \text{accordingly for } >, =\\
D(F \wedge G) &\equiv D(F) \wedge D(G)\\
D(\forall i\, F) &\equiv \forall i\, D(F)
\end{aligned}
$$

Definition (Syntactic total derivation D)

$$
\begin{aligned}
D(r) &= 0 && \text{if } r \text{ a number symbol}\\
D(x(i)) &= x(i)' && \text{if } x : C \to \mathbb{R},\ C \neq \mathbb{R}\\
D(a+b) &= D(a) + D(b)\\
D(a \cdot b) &= D(a) \cdot b + a \cdot D(b)\\
D(a/b) &= (D(a) \cdot b - a \cdot D(b))/b^2\\
D(a \geq b) &\equiv D(a) \geq D(b) && \text{accordingly for } >, =\\
D(F \land G) &\equiv D(F) \land D(G)\\
D(\forall i\, F) &\equiv \forall i\, D(F)
\end{aligned}
$$

$$
\begin{aligned}
\mathcal{P} &\equiv \forall i,j : A\ \left(i = j \lor (x_1(i) - x_1(j))^2 + (x_2(i) - x_2(j))^2 \geq p^2\right)\\
\Rightarrow D(\mathcal{P}) &\equiv \forall i,j : A\ \left(i' = j' \land 2(x_1(i) - x_1(j))(x_1(i)' - x_1(j)')\right.\\
&\qquad \left. + 2(x_2(i) - x_2(j))(x_2(i)' - x_2(j)') \geq 0\right)
\end{aligned}
$$

Definition (Syntactic total derivation D)

$$
\begin{aligned}
D(r) &= 0 && \text{if } r \text{ a number symbol}\\
D(x(i)) &= x(i)' && \text{if } x : C \to \mathbb{R},\ \ C \neq \mathbb{R}\\
D(a+b) &= D(a) + D(b)\\
D(a \cdot b) &= D(a)\cdot b + a \cdot D(b)\\
D(a/b) &= (D(a)\cdot b - a\cdot D(b))/b^2\\
D(a \geq b) &\equiv D(a) \geq D(b) && \text{accordingly for } >, =\\
D(F \wedge G) &\equiv D(F) \wedge D(G)\\
D(\forall i\, F) &\equiv \forall i\, D(F)
\end{aligned}
$$

$$
\begin{aligned}
\mathcal{P} &\equiv \forall i,j\!:\!A\ \big(i = j \vee (x_1(i) - x_1(j))^2 + (x_2(i) - x_2(j))^2 \geq p^2\big)\\
\Rightarrow D(\mathcal{P}) &\equiv \forall i,j\!:\!A\ \big(i' = j' \wedge 2(x_1(i) - x_1(j))(x_1(i)' - x_1(j)')\\
&\qquad + 2(x_2(i) - x_2(j))(x_2(i)' - x_2(j)') \geq 0\big)
\end{aligned}
$$

Syntactic derivation $D(\cdot)$ coincides with analytic differentiation:

Lemma (Derivation lemma)

Valuation is a differential homomorphism: for all flows φ *all* $\zeta \in [0, r]$

$$\frac{\mathrm{d}\,[\![\theta]\!]_{\varphi(t)}}{\mathrm{d}t}(\zeta) = [\![D(\theta)]\!]_{\bar{\varphi}(\zeta)}$$

Derivations and Differentiation

Syntactic derivation $D(\cdot)$ coincides with analytic differentiation:

Lemma (Derivation lemma)

Valuation is a differential homomorphism: for all flows φ *all* $\zeta \in [0, r]$

$$\frac{\mathrm{d}\,[\![\theta]\!]_{\varphi(t)}}{\mathrm{d}t}(\zeta) = [\![D(\theta)]\!]_{\bar{\varphi}(\zeta)}$$

Locally understand QDE as quantified assignments:

Lemma (Quantified differential substitution principle)

If $\varphi \models \forall i : C\ f(i)' = \theta \,\&\, H$*, then* $\varphi \models \upsilon = [\forall i : C\ f(i)' := \theta]\upsilon$ *for all* υ*.*

Syntactic derivation $D(\cdot)$ coincides with analytic differentiation:

Lemma (Derivation lemma)

Valuation is a differential homomorphism: for all flows φ all $\zeta \in [0, r]$

$$\frac{\mathrm{d}\, [\![\theta]\!]_{\varphi(t)}}{\mathrm{d}t}(\zeta) = [\![D(\theta)]\!]_{\bar{\varphi}(\zeta)}$$

Locally understand QDE as quantified assignments:

Lemma (Quantified differential substitution principle)

If $\varphi \models \forall i : C\ f(i)' = \theta \,\&\, H$, then $\varphi \models \upsilon = [\forall i : C\ f(i)' := \theta]\upsilon$ for all υ.

Theorem (Quantified Differential Invariant)

$$(QDI)\quad \frac{H \rightarrow [\forall i : C\ f(\vec{i})' := \theta] D(F)}{F \rightarrow [\forall i : C\ f(\vec{i})' = \theta \,\&\, H] F} \quad \textit{is sound}$$

$$\overline{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}$$
$$\forall i : C\ 2x(i)^3 \geq 1 \rightarrow [\forall i : C\ x(i)' = x(i)^2 + x(i)^4 + 2]\forall i : C\ 2x(i)^3 \geq 1$$

A Simple Proof with Quantified Differential Invariants

$$\dfrac{[\forall i : C\ x(i)' := x(i)^2 + x(i)^4 + 2]\forall i : C\ 2(x(i)^3)' \geq 0}{\forall i : C\ 2x(i)^3 \geq 1 \rightarrow [\forall i : C\ x(i)' = x(i)^2 + x(i)^4 + 2]\forall i : C\ 2x(i)^3 \geq 1}$$

$$\dfrac{\dfrac{[\forall i : C\ x(i)' := x(i)^2 + x(i)^4 + 2]\forall i : C\ 6x(i)^2 x(i)' \geq 0}{[\forall i : C\ x(i)' := x(i)^2 + x(i)^4 + 2]\forall i : C\ 2(x(i)^3)' \geq 0}}{\forall i : C\ 2x(i)^3 \geq 1 \rightarrow [\forall i : C\ x(i)' = x(i)^2 + x(i)^4 + 2]\forall i : C\ 2x(i)^3 \geq 1}$$

A Simple Proof with Quantified Differential Invariants

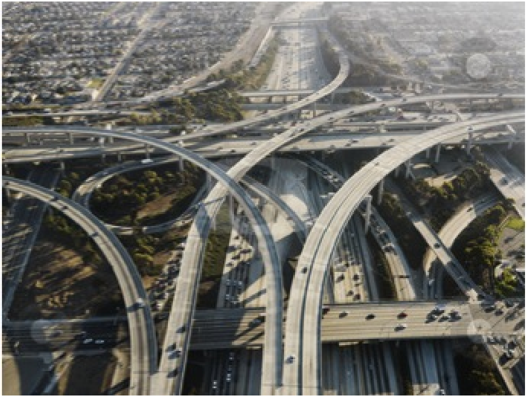
$$\dfrac{\dfrac{\dfrac{\dfrac{}{\forall i : C\ 6x(i)^2(x(i)^2 + x(i)^4 + 2) \geq 0}}{[\forall i : C\ x(i)' := x(i)^2 + x(i)^4 + 2]\forall i : C\ 6x(i)^2 x(i)' \geq 0}}{[\forall i : C\ x(i)' := x(i)^2 + x(i)^4 + 2]\forall i : C\ 2(x(i)^3)' \geq 0}}{\forall i : C\ 2x(i)^3 \geq 1 \rightarrow [\forall i : C\ x(i)' = x(i)^2 + x(i)^4 + 2]\forall i : C\ 2x(i)^3 \geq 1}$$

A Simple Proof with Quantified Differential Invariants

$$\dfrac{\dfrac{\dfrac{\dfrac{\mathit{true}}{\forall i : C\ 6x(i)^2(x(i)^2+x(i)^4+2)\geq 0}}{[\forall i : C\ x(i)' := x(i)^2+x(i)^4+2]\forall i : C\ 6x(i)^2 x(i)' \geq 0}}{[\forall i : C\ x(i)' := x(i)^2+x(i)^4+2]\forall i : C\ 2(x(i)^3)' \geq 0}}{\forall i : C\ 2x(i)^3 \geq 1 \rightarrow [\forall i : C\ x(i)' = x(i)^2+x(i)^4+2]\forall i : C\ 2x(i)^3 \geq 1}$$

Outline Background

Driver's License Test for Robotic Cars?



Driver's License Test for Robotic Cars? Proof!

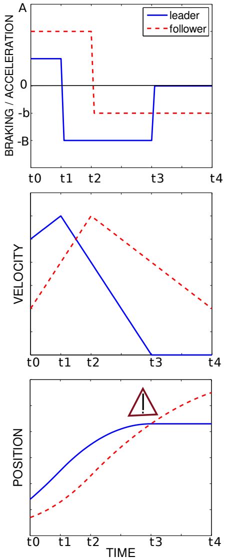
Car Control: Local Lane Control Challenge

Challenge: Local lane dynamics

- A car controller for a differential equation respects separation of local lane.

Challenge: Local lane dynamics

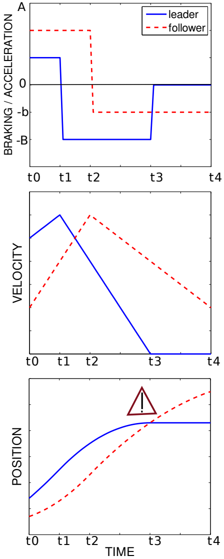
- A car controller for a differential equation respects separation of local lane.
- Follower car maintains safe distance to leader:



Challenge: Local lane dynamics

- A car controller for a differential equation respects separation of local lane.
- Follower car maintains safe distance to leader:

$$f \ll \ell \rightarrow [(a_i := ctrl;\ x_i'' = a_i)^*]\, f \ll \ell$$



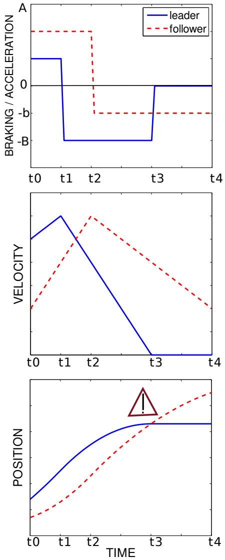
Car Control: Local Lane Control Challenge

Challenge: Local lane dynamics

- A car controller for a differential equation respects separation of local lane.
- Follower car maintains safe distance to leader:

$$f \ll \ell \rightarrow [(a_i := ctrl;\ x_i'' = a_i)^*]\, f \ll \ell$$

$$f \ll \ell \equiv\ (x_f \leq x_\ell) \land (f \neq \ell) \rightarrow \\ (x_\ell > x_f + \frac{v_f^2}{2b} - \frac{v_\ell^2}{2B} \\ \land x_\ell > x_f \land v_f \geq 0 \land v_\ell \geq 0)$$



$$f \ll \ell \rightarrow [\texttt{llc}]\, f \ll \ell$$

Hybrid Program (Local lane control)

$$\begin{aligned}
\texttt{llc} &\equiv (ctrl; dyn)^* \\
ctrl &\equiv \ell_{ctrl} \mid\mid f_{ctrl}; \\
\ell_{ctrl} &\equiv (a_\ell := *; \quad ?(-B \leq a_\ell \leq A)) \\
f_{ctrl} &\equiv \big(a_f := *; \quad ?(-B \leq a_f \leq -b)\big) \\
&\qquad \cup \quad \big(?\mathbf{Safe}_\varepsilon; \quad a_f := *; \quad ?(-B \leq a_f \leq A)\big) \\
&\qquad \cup \quad \big(?(v_f = 0); \; a_f := 0\big) \\
\mathbf{Safe}_\varepsilon &\equiv x_f + \frac{v_f^2}{2b} + \left(\frac{A}{b} + 1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon v_f\right) < x_\ell + \frac{v_\ell^2}{2B} \\
dyn &\equiv (t := 0; \; x_f' = v_f, \; v_f' = a_f, \; x_\ell' = v_\ell, \; v_\ell' = a_\ell, t' = 1 \\
&\qquad \& \; v_f \geq 0 \; \land \; v_\ell \geq 0 \; \land \; t \leq \varepsilon)
\end{aligned}$$

Challenge: Global lane dynamics

- All controllers for arbitrarily many differential equations respect separation globally on lane.

Car Control: Global Lane Control Challenge

Challenge: Global lane dynamics

- All controllers for arbitrarily many differential equations respect separation globally on lane.
- Each car safe behind all others

Car Control: Global Lane Control Challenge

Challenge: Global lane dynamics

- All controllers for arbitrarily many differential equations respect separation globally on lane.
- Each car safe behind all others

$$[(\forall i\; a(i) := ctrl;\; \forall i\; x(i)'' = a(i))^*]\,\forall i, j\; i \ll j$$

Car Control: Global Lane Control Challenge

$$\forall i : C\ i \ll \ell(i) \to [\mathtt{glc}](\forall i : C\ i \ll \ell^*(i))$$

Quantified Hybrid Program (Global lane control)

$$\mathtt{glc} \equiv (ctrl^n; dyn^n)^*$$

$$ctrl^n \equiv \forall i : C\ (ctrl(i))$$

$$ctrl(i) \equiv \big(a(i) := *; ?(-B \le a(i) \le -b)\big)$$
$$\cup\ \big(?\mathbf{Safe}_\varepsilon(i);\ a(i) := *;\ ?(-B \le a(i) \le A)\big)$$
$$\cup\ \big(?(v(i) = 0);\ a(i) := 0\big)$$

$$\mathbf{Safe}_\varepsilon(i) \equiv x(i) + \frac{v(i)^2}{2b} + \left(\frac{A}{b} + 1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon v(i)\right) < x(\ell(i)) + \frac{v(\ell(i))^2}{2B}$$

$$dyn^n \equiv t := 0;\ \forall i : C\ (dyn(i), t' = 1\ \&\ v(i) \ge 0 \land t \le \varepsilon)$$

$$dyn(i) \equiv x(i)' = v(i), v(i)' = a(i)$$

$$i \ll \ell^*(i) \equiv [k := i;\ (k := \ell(k))^*] i \ll k$$

$$\forall i : C\ i \ll \ell(i) \rightarrow [\mathtt{glc}](\forall i : C\ i \ll \ell^*(i))$$

Quantified Hybrid Program (Global lane control)

$$\mathtt{glc} \equiv (ctrl^n; dyn^n)^*$$

$$ctrl^n \equiv \forall i : C\ (ctrl(i))$$

$$ctrl(i) \equiv (a(i) := *; ?(-B \le a(i) \le -b))$$
$$\cup\ (?\mathbf{Safe}_\varepsilon(i);\ a(i) := *;\ ?(-B \le a(i) \le A))$$
$$\cup\ (?(v(i) = 0);\ a(i) := 0)$$

$$\mathbf{Safe}_\varepsilon(i) \equiv x(i) + \frac{v(i)^2}{2b} + \left(\frac{A}{b} + 1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon v(i)\right) < x(\ell(i)) + \frac{v(\ell(i))^2}{2B}$$

$$dyn^n \equiv t := 0;\ \forall i : C\ (dyn(i), t' = 1\ \&\ v(i) \ge 0 \land t \le \varepsilon)$$

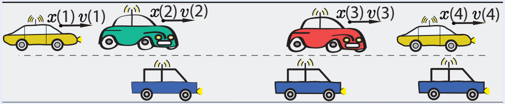
$$dyn(i) \equiv x(i)' = v(i), v(i)' = a(i)$$

$$i \ll \ell^*(i) \equiv [k := i;\ (k := \ell(k))^*] i \ll k$$

Car Control: Global Lane Control Challenge

$$\forall i : C\ i \ll \ell(i) \rightarrow [\mathtt{glc}](\forall i : C\ i \ll \ell^*(i))$$

Quantified Hybrid Program (Global lane control)



$$i \ll \ell^*(i) \equiv [k := i;\ (k := \ell(k))^*] i \ll k$$

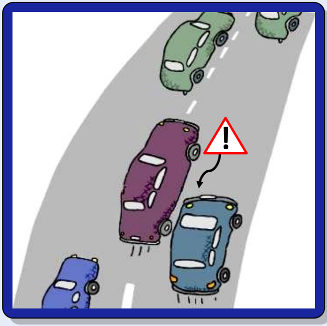
Car Control: Local Highway Control Challenge

Challenge: Local highway dynamics

- All controllers for arbitrarily many differential equations respect separation locally on highway.

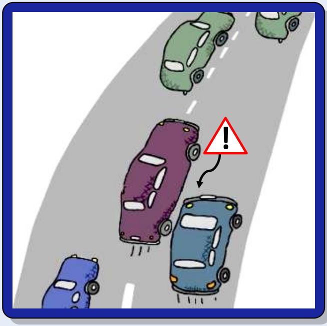
Challenge: Local highway dynamics

- All controllers for arbitrarily many differential equations respect separation locally on highway.
- For each lane: all controllers for the differential equations respect separation even if cars appear or disappear.



Challenge: Local highway dynamics

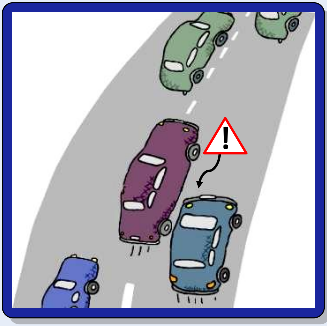
- All controllers for arbitrarily many differential equations respect separation locally on highway.
- For each lane: all controllers for the differential equations respect separation even if cars appear or disappear.
- Each car safe behind all others, even if new cars appear or disappear.



Car Control: Local Highway Control Challenge

Challenge: Local highway dynamics

- All controllers for arbitrarily many differential equations respect separation locally on highway.
- For each lane: all controllers for the differential equations respect separation even if cars appear or disappear.
- Each car safe behind all others, even if new cars appear or disappear.



$$[(n := \mathtt{new}\ C;\ \forall i\, a(i) := ctrl;\ \forall i\, x(i)'' = a(i))^*]\,\forall i,j\; i \ll j$$

Car Control: Local Highway Control Challenge

$$\forall i : C\ i \ll \ell(i) \rightarrow [\mathtt{glc}](\forall i : C\ i \ll \ell^*(i))$$

Quantified Hybrid Program (Local highway control)

$$\begin{aligned}
\mathtt{lhc} &\equiv (delete^*; create^*; ctrl^n; dyn^n)^* \\
create &\equiv n := new;\ ?(F(n) \ll n \land n \ll \ell(n)) \\
(n := new) &\equiv n := *;\ ?(\mathrm{E}(n) = 0);\ \mathrm{E}(n) := 1 \\
F(n) \ll n &\equiv \forall j : C\ (\ell(j) = n \rightarrow j \ll n) \\
delete &\equiv n := *;\ ?(\mathrm{E}(n) = 1);\ \mathrm{E}(n) := 0
\end{aligned}$$

Car Control: Local Highway Control Challenge

$$\forall i : C\ i \ll \ell(i) \rightarrow [\mathtt{glc}](\forall i : C\ i \ll \ell^*(i))$$

Quantified Hybrid Program (Local highway control)

$$\begin{aligned}
\mathtt{lhc} &\equiv (\textcolor{red}{delete^*; create^*}; ctrl^n; dyn^n)^* \\
create &\equiv n := new;\ ?(F(n) \ll n \wedge n \ll \ell(n)) \\
(n := new) &\equiv n := *;\ ?(\mathrm{E}(n) = 0);\ \mathrm{E}(n) := 1 \\
F(n) \ll n &\equiv \forall j : C\ (\ell(j) = n \rightarrow j \ll n) \\
delete &\equiv n := *;\ ?(\mathrm{E}(n) = 1);\ \mathrm{E}(n) := 0
\end{aligned}$$

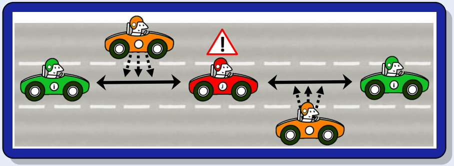
Challenge: Global highway dynamics

- All controllers for arbitrarily many differential equations respect separation globally on highway.

Car Control: Global Highway Control Challenge

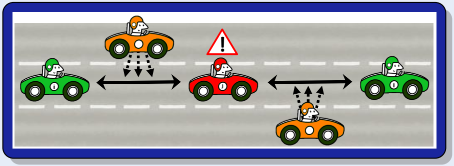
Challenge: Global highway dynamics

- All controllers for arbitrarily many differential equations respect separation globally on highway.
- All controllers for the differential equations respect separation even if cars switch lanes.

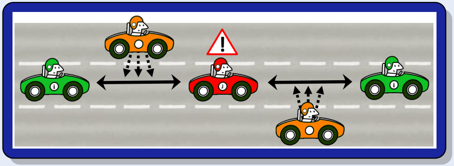


Challenge: Global highway dynamics

- All controllers for arbitrarily many differential equations respect separation globally on highway.
- All controllers for the differential equations respect separation even if cars switch lanes.
- On all lanes, all car safe behind all others on their lanes, even if cars switch lanes.



Challenge: Global highway dynamics



- All controllers for arbitrarily many differential equations respect separation globally on highway.
- All controllers for the differential equations respect separation even if cars switch lanes.
- On all lanes, all car safe behind all others on their lanes, even if cars switch lanes.

$$[\forall l\,(n := \mathtt{new}\ C;\ \forall i\, a(i) := ctrl;\ \forall i\, x(i)'' = a(i))^*]\,\forall l\,\forall i,j\; i \ll j$$

Car Control: Global Highway Control Challenge

$$\forall l : L \forall i : C_l\, i \ll \ell_l(i) \rightarrow$$
$$[(\forall l : L\, delete_l^*; \forall l : L\, new_l^*; \forall l : L\, ctrl_l^n; \forall l : L\, dyn_l^n)^*]\, \forall l : L \forall i : C_l\, i \ll \ell_l^*(i)$$

Quantified Hybrid Program (Global highway control)

$$\mathtt{ghc} \equiv (\forall l : L\, delete_l^*;\ \forall l : L\, new_l^*;\ \forall l : L\, ,ctrl_l^n;\ \forall l : L\, dyn_l^n)^*$$

$$\forall I : L \forall i : C_I\, i \ll \ell_I(i) \rightarrow$$
$$[(\forall I : L\, delete_I^*; \forall I : L\, new_I^*; \forall I : L\, ctrl_I^n; \forall I : L\, dyn_I^n)^*]\, \forall I : L \forall i : C_I\, i \ll \ell_I^*(i)$$

Quantified Hybrid Program (Global highway control)

$$\mathrm{ghc} \equiv (\forall I : L\, delete_I^*;\ \forall I : L\, new_I^*;\ \forall I : L\, , ctrl_I^n;\ \forall I : L\, dyn_I^n)^*$$

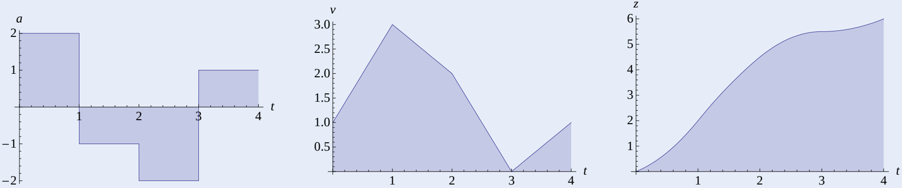
Q: I want to verify trains

Challenge

Q: I want to verify trains A: Hybrid systems

Challenge (Hybrid Systems)

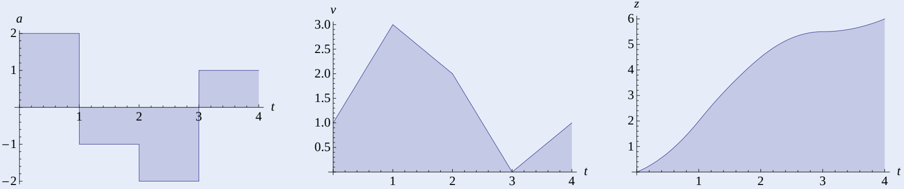
- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)



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

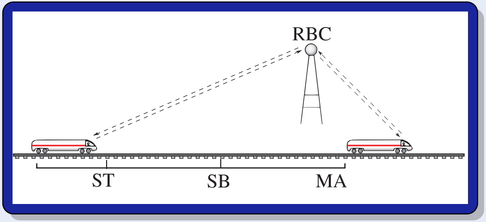
Challenge (Hybrid Systems)

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



Q: I want to verify uncertain trains

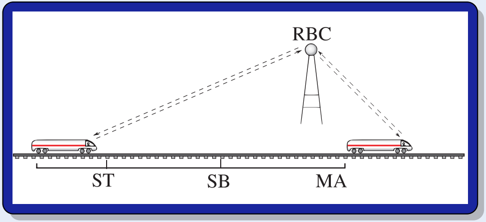
Challenge

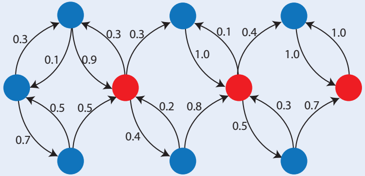


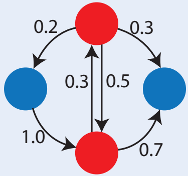
Q: I want to verify uncertain trains A: Markov chains

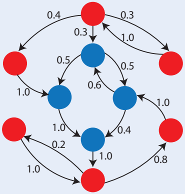
Challenge (Probabilistic Systems)

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





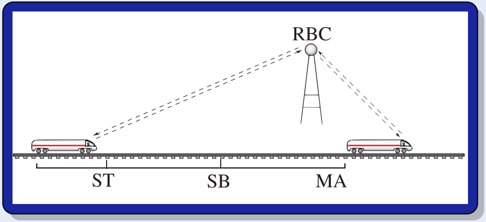


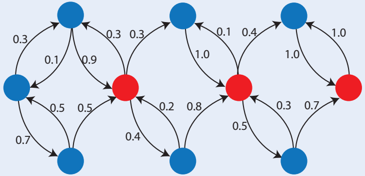


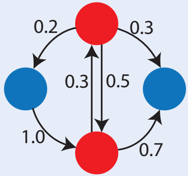
Q: I want to verify uncertain trains A: Markov chains Q: But trains move!

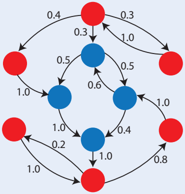
Challenge (Probabilistic Systems)

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



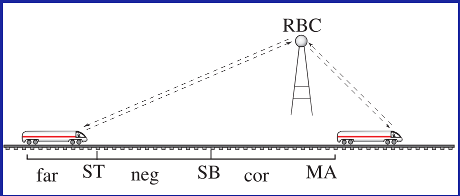






Q: I want to verify uncertain systems

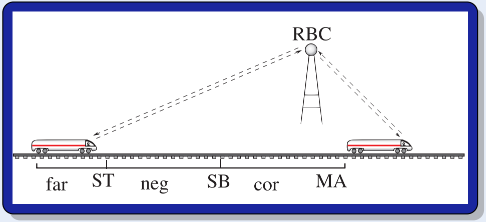
Challenge



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

Challenge (Stochastic Hybrid Systems)

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

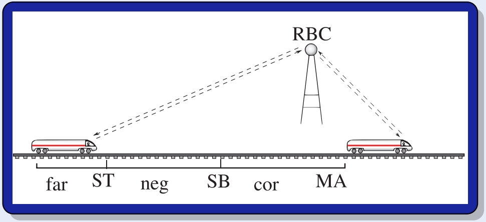


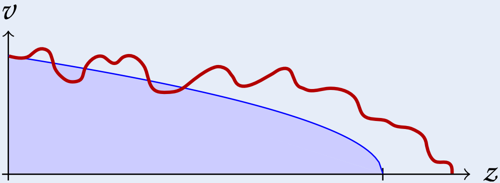
Q: I want to verify uncertain systems A: Stochastic hybrid systems

Challenge (Stochastic Hybrid Systems)

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

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



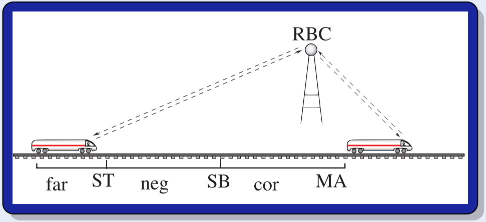


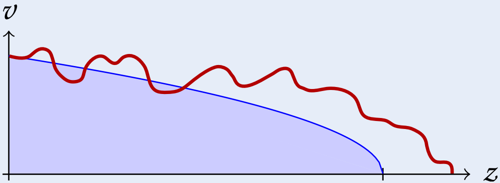
Q: I want to verify uncertain systems A: Stochastic hybrid systems Q: How?

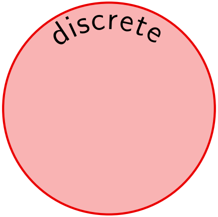
Challenge (Stochastic Hybrid Systems)

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

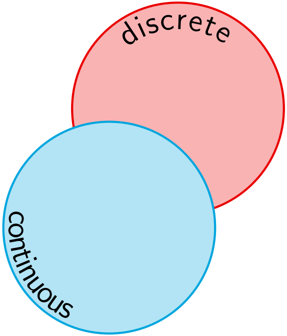
- Discrete stochastic (lossy communication)
- Continuous stochastic (wind, track)

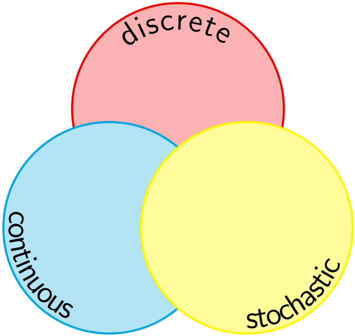




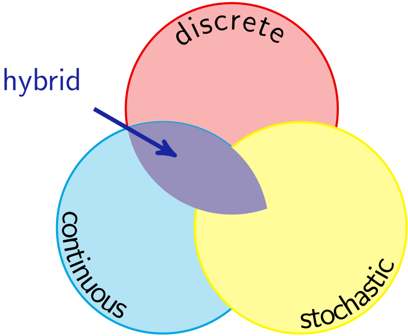

discrete

Cyber-Physical Systems

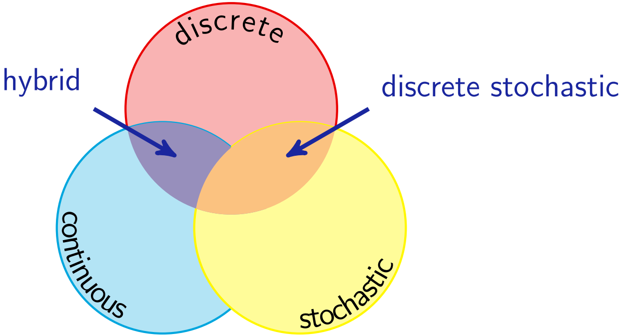


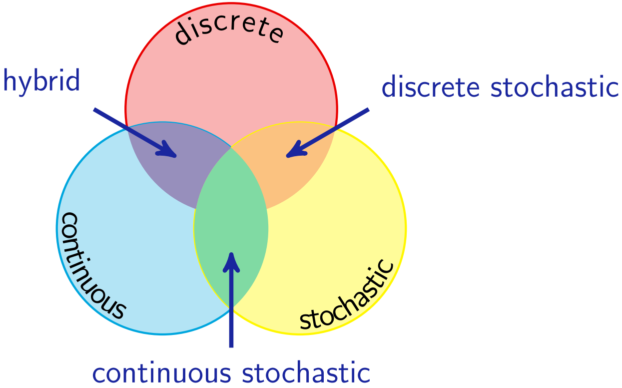

discrete
continuous
stochastic

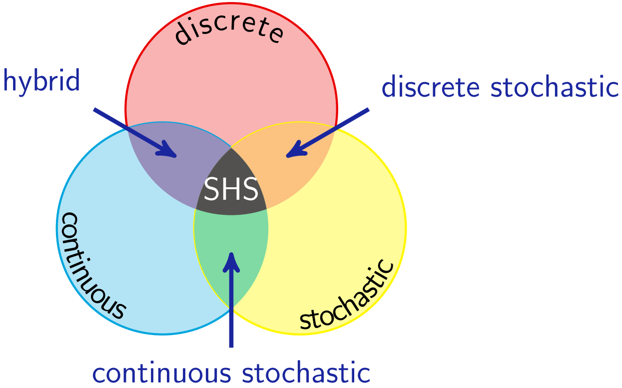
Cyber-Physical Systems



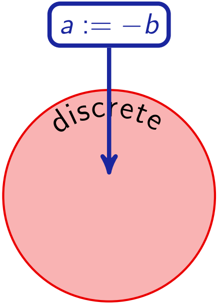
Cyber-Physical Systems



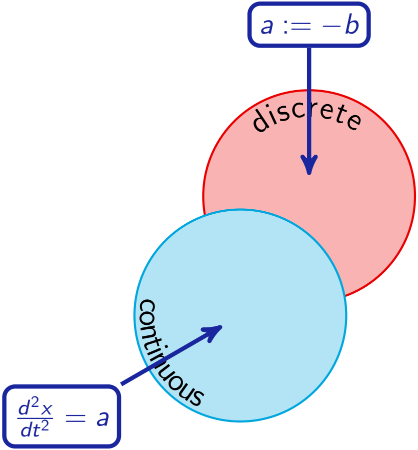

discrete
hybrid
discrete stochastic
continuous
stochastic
continuous stochastic


discrete
hybrid
discrete stochastic
SHS
continuous
stochastic
continuous stochastic

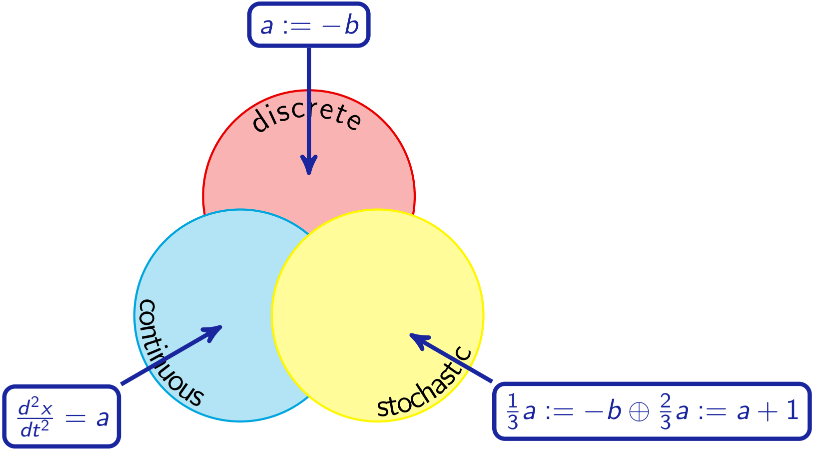
Model for Stochastic Hybrid Systems



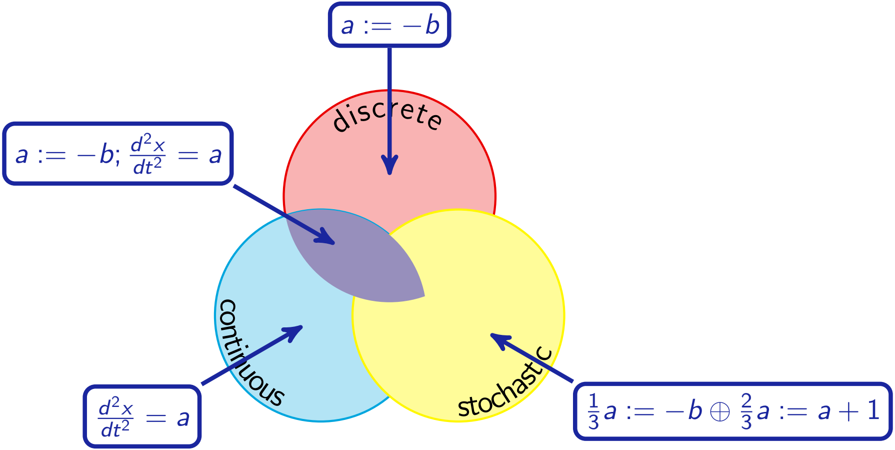
Model for Stochastic Hybrid Systems

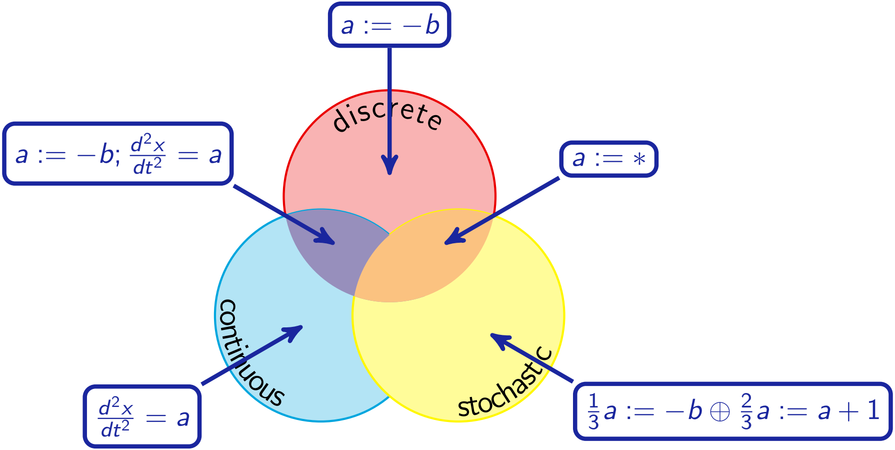


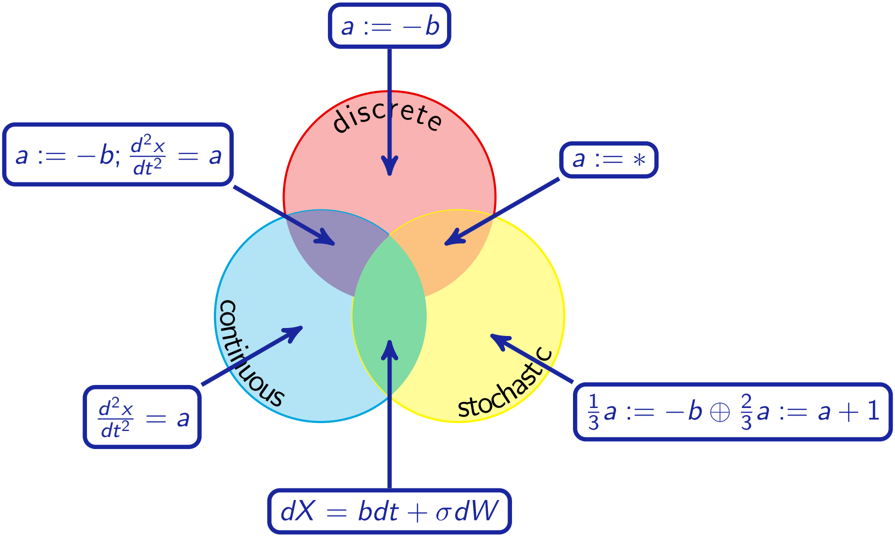
Model for Stochastic Hybrid Systems



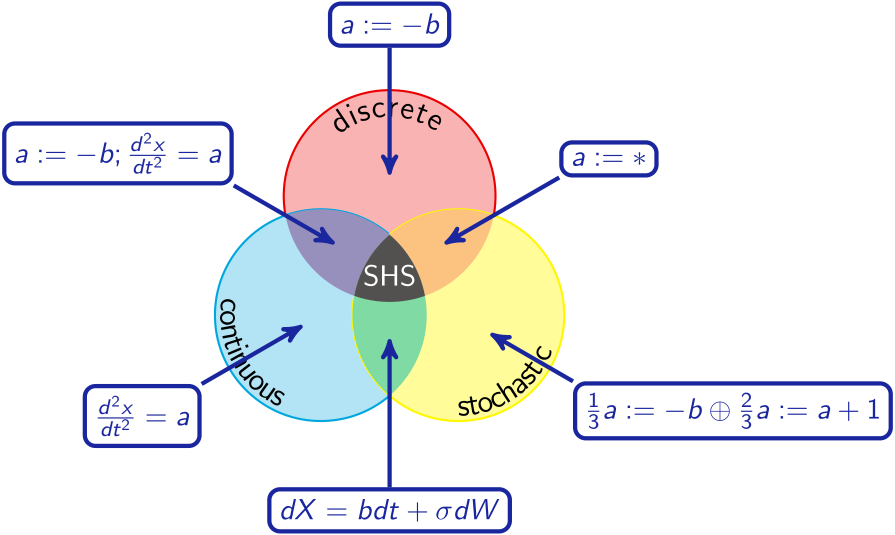
Model for Stochastic Hybrid Systems




$a := -b$
discrete
$a := -b;\ \frac{d^2x}{dt^2} = a$
$a := *$
continuous
stochastic
$\frac{d^2x}{dt^2} = a$
$\frac{1}{3} a := -b \oplus \frac{2}{3} a := a + 1$


$a := -b$
$a := -b; \frac{d^2x}{dt^2} = a$
discrete
$a := *$
continuous
stochastic
$\frac{d^2x}{dt^2} = a$
$\frac{1}{3}a := -b \oplus \frac{2}{3}a := a+1$
$dX = bdt + \sigma dW$

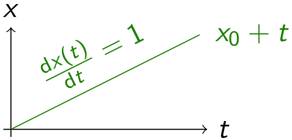
Model for Stochastic Hybrid Systems



Stochastic Differential Equations (SDE)

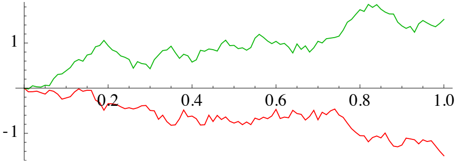
Definition (Ordinary differential equation (ODE))

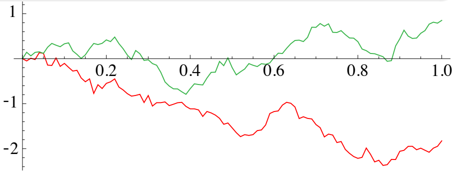
$$\frac{\mathrm{d}x(t)}{\mathrm{d}t} = b(x(t)) \quad x(0) = x_0$$



Definition (Itō stochastic differential equation (SDE))

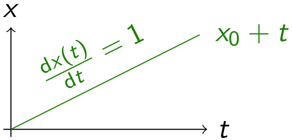
$$dX_t = b(X_t)dt + \sigma(X_t)dW_t \quad X_0 = Z$$





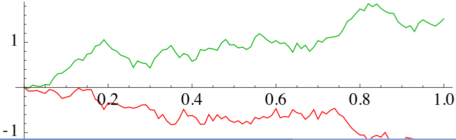
Definition (Ordinary differential equation (ODE))

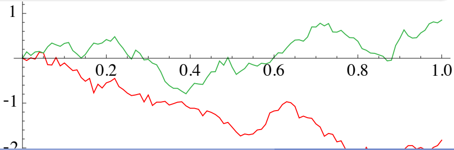
$$\frac{\mathrm{d}x(t)}{\mathrm{d}t} = b(x(t)) \quad x(0) = x_0$$



Definition (Itō stochastic differential equation (SDE))

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

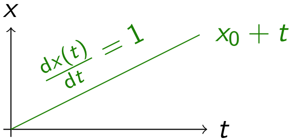




Stochastic Differential Equations (SDE)

Definition (Ordinary differential equation (ODE))

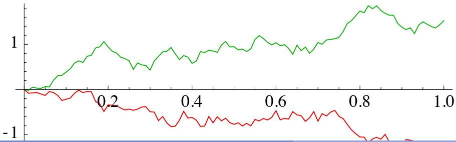
$$\frac{\mathrm{d}x(t)}{\mathrm{d}t} = b(x(t)) \quad x(0) = x_0$$

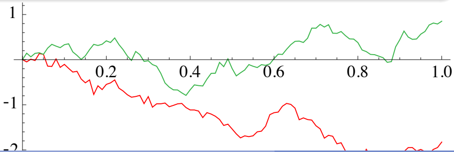


Calculus

Definition (Itō stochastic differential equation (SDE))

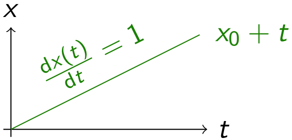
$$X_s = Z + \int_0^s dX_t = Z + \int_0^s b(X_t)dt + \int_0^s \sigma(X_t)dW_t$$

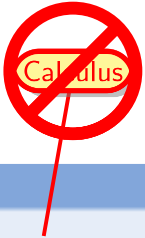




Definition (Ordinary differential equation (ODE))

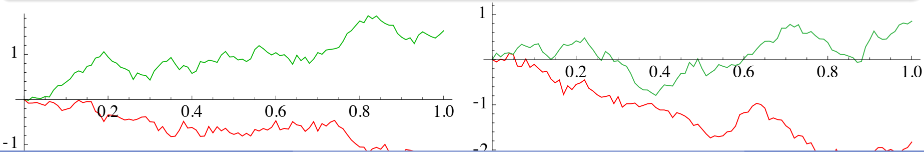
$$\frac{\mathrm{d}x(t)}{\mathrm{d}t} = b(x(t)) \quad x(0) = x_0$$





Definition (Itō stochastic differential equation (SDE))

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



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

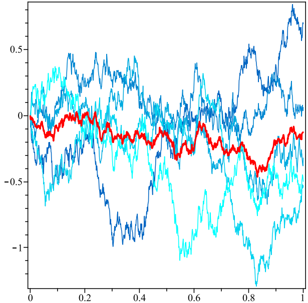
Brownian Motion is Extremely Complex

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

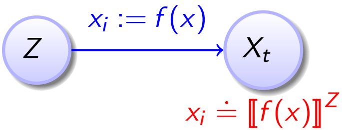
$\Rightarrow$ a.s. unbounded variation, $\notin$ FV, nonmonotonic on every interval



Stochastic Hybrid Programs: Syntax

Definition (Stochastic hybrid program α)

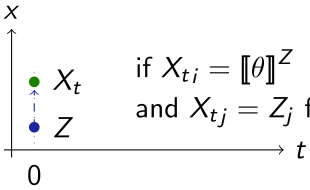
$x := \theta$	(assignment)	jump & test
$x := *$	(random assignment)	
$?H$	(conditional execution)	
$dx = bdt + \sigma dW \& H$	(SDE)	
$\alpha; \beta$	(seq. composition)	algebra
$\lambda\alpha \oplus \nu\beta$	(convex combination)	
α^*	(nondet. repetition)	



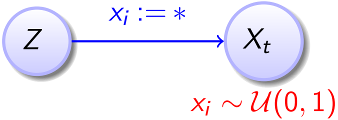
Definition (Stochastic hybrid program α: process semantics)

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

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



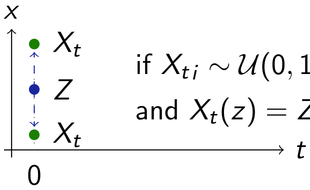
if $X_{t\,i} = [\![\theta]\!]^Z$
and $X_{t\,j} = Z_j$ for $j \neq i$



Definition (Stochastic hybrid program α: process semantics)

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

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

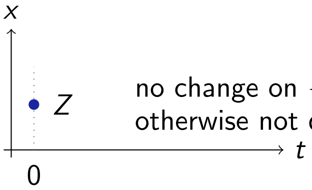


if $X_{t\,i} \sim \mathcal{U}(0,1)$
and $X_t(z) = Z(z)$ for $z \neq x$

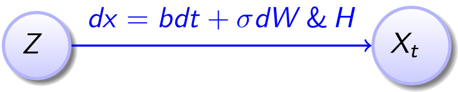
on $\{Z \models H\}$

Definition (Stochastic hybrid program α: process semantics)

$$?H = \hat{Z} \quad \text{on the event } \{Z \models H\}$$
$$(\!|?H|\!)^Z = 0$$



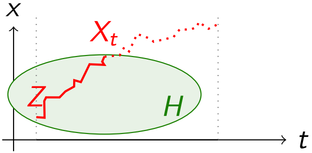
no change on $\{Z \models H\}$
otherwise not defined



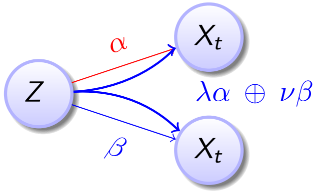
Definition (Stochastic hybrid program α: process semantics)

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

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



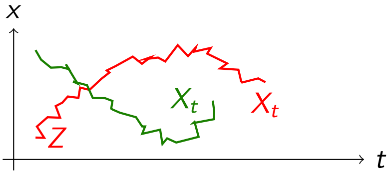
$dx = bdt + \sigma dW \,\&\, H$

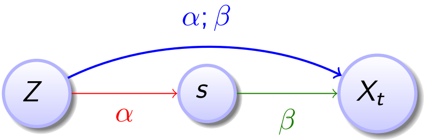


Definition (Stochastic hybrid program α: process semantics)

$$\lambda\alpha \oplus \nu\beta = \mathcal{I}_{U\leq\lambda}\alpha + \mathcal{I}_{U>\lambda}\beta = \begin{cases} \alpha & \text{on event } \{U \leq \lambda\} \\ \beta & \text{on event } \{U > \lambda\} \end{cases}$$

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

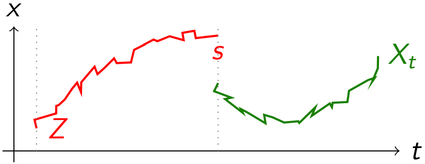


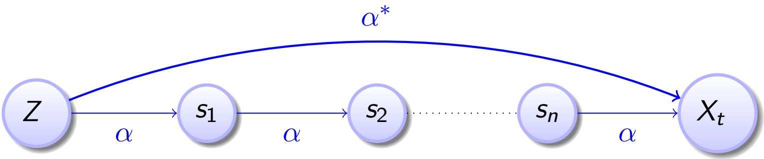


Definition (Stochastic hybrid program α: process semantics)

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

$$(\!|\alpha;\beta|\!)^Z = (\!|\alpha|\!)^Z + (\!|\beta|\!)^\alpha$$

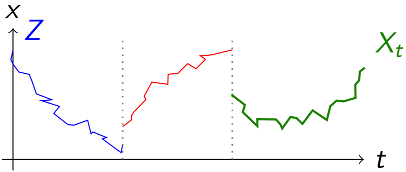


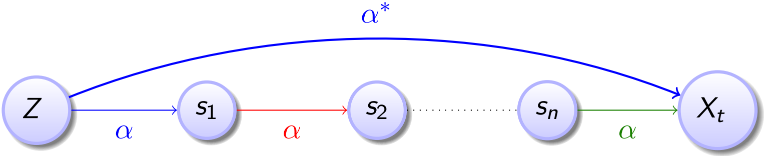


Definition (Stochastic hybrid program α: process semantics)

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

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

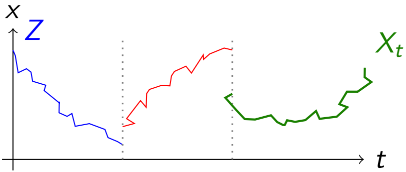




Definition (Stochastic hybrid program α: process semantics)

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

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



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

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

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

Definition (Measurable semantics)

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

Definition (Measurable semantics)

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

Definition (Measurable semantics)

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

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

Definition (Measurable semantics)

$$
\begin{aligned}
[\![F]\!]^Z &= F^\ell(Z) \text{ i.e., } [\![F]\!]^Z(\omega) = F^\ell(Z(\omega))\\
[\![\lambda f + \nu g]\!]^Z &= \lambda[\![f]\!]^Z + \nu[\![g]\!]^Z\\
[\![Bf]\!]^Z &= [\![B]\!]^Z * [\![f]\!]^Z \text{ i.e., } [\![Bf]\!]^Z(\omega) = [\![B]\!]^Z(\omega)[\![f]\!]^Z(\omega)
\end{aligned}
$$

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

Definition (Measurable semantics)

$$
\begin{aligned}
[\![F]\!]^Z &= F^\ell(Z) \text{ i.e., } [\![F]\!]^Z(\omega) = F^\ell(Z(\omega))\\
[\![\lambda f + \nu g]\!]^Z &= \lambda [\![f]\!]^Z + \nu [\![g]\!]^Z\\
[\![Bf]\!]^Z &= [\![B]\!]^Z * [\![f]\!]^Z \text{ i.e., } [\![Bf]\!]^Z(\omega) = [\![B]\!]^Z(\omega)[\![f]\!]^Z(\omega)\\
[\![\langle\alpha\rangle f]\!]^Z &= \sup\{[\![f]\!]^\alpha \;:\; 0 \le t \le (\!|\alpha|\!)^Z\}
\end{aligned}
$$

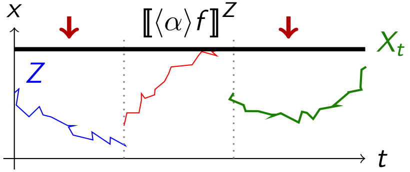
Definition (Measurable semantics)

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

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

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

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



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

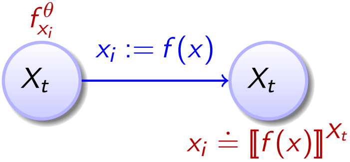
Theorem (Measurable)

$[\![f]\!]^Z$ 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)

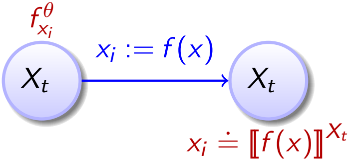
$$S \mapsto P(([\![f]\!]^Z)^{-1}(S)) = P(\{\omega \in \Omega \;:\; [\![f]\!]^Z(\omega) \in S\}) = P([\![f]\!]^Z \in S)$$

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

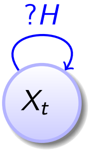


Proof Calculus: Stochastic Differential Dynamic Logic

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

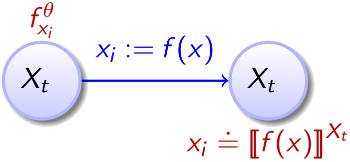


$$\langle ?H \rangle f \;=\; Hf$$

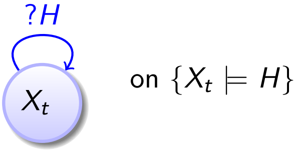


on $\{X_t \models H\}$

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



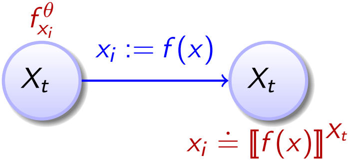
$$\langle ?H \rangle f = Hf$$



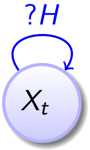
$$\langle \alpha \rangle (\lambda f) = \lambda \langle \alpha \rangle f$$

Proof Calculus: Stochastic Differential Dynamic Logic

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



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



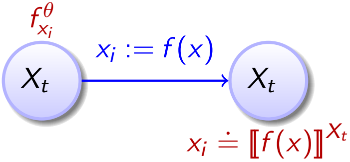
on $\{X_t \models H\}$

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

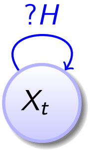
$$\langle \alpha \rangle (\lambda f + \nu g) \;\leq\; \lambda \langle \alpha \rangle f + \nu \langle \alpha \rangle g$$

Proof Calculus: Stochastic Differential Dynamic Logic

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



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



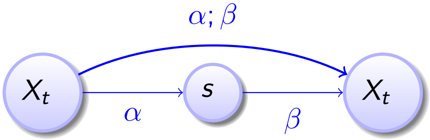
on $\{X_t \models H\}$

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

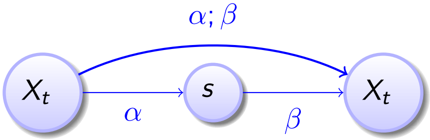
$\langle \alpha \rangle (\lambda f + \nu g) \;\leq\; \lambda \langle \alpha \rangle f + \nu \langle \alpha \rangle g$

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

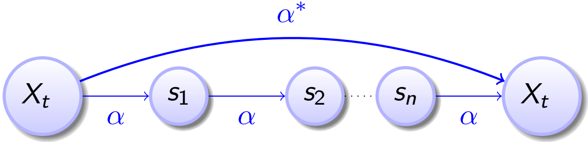
$$\langle\alpha;\beta\rangle f \;\leq\; \langle\alpha\rangle(f \sqcup \langle\beta\rangle f)$$



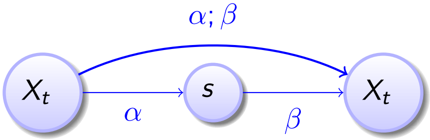
$\langle\alpha;\beta\rangle f \;\le\; \langle\alpha\rangle(f \sqcup \langle\beta\rangle f)$



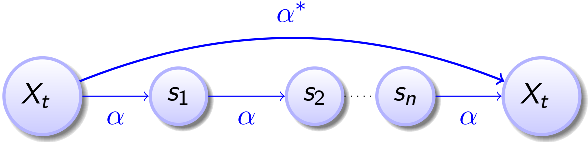
$\langle\alpha\rangle f \le f \vDash \langle\alpha^*\rangle f \le f$



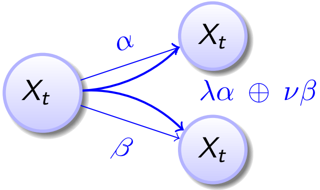
$$\langle \alpha; \beta \rangle f \;\leq\; \langle \alpha \rangle (f \sqcup \langle \beta \rangle f)$$



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



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



Soundness

Theorem (Soundness)

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)

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 (Stochastic Differential Invariants)

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

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

Soundness

Theorem (Stochastic Differential Invariants)

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

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

Theorem (Dynkin for càdlàg strong Markov X_t and $\phi \in C_C^2(\mathbb{R}^d, \mathbb{R})$)

$$Af(x) := \lim_{t \searrow 0} \frac{E^x f(X_t) - f(x)}{t} \overset{E^x\tau<\infty}{\Rightarrow} E^x f(X_\tau) = f(x) + E^x \int_0^\tau Af(X_s)ds$$

Soundness

Theorem (Stochastic Differential Invariants)

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

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

Theorem (Dynkin for càdlàg strong Markov X_t and $\phi \in C_C^2(\mathbb{R}^d, \mathbb{R})$)

$$Af(x) := \lim_{t \searrow 0} \frac{E^x f(X_t) - f(x)}{t} \overset{E^x\tau<\infty}{\Rightarrow} E^x f(X_\tau) = f(x) + E^x \int_0^\tau Af(X_s)ds$$

Theorem (Differential generator for SDE solution and $\phi \in C_C^2(\mathbb{R}^d, \mathbb{R})$)

$$A\phi = L\phi := b\nabla f + \frac{\sigma\sigma^T}{2}\nabla\nabla f$$

Soundness

Theorem (Stochastic Differential Invariants)

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

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

Theorem (Dynkin for càdlàg strong Markov X_t and $\phi \in C^2_C(\mathbb{R}^d, \mathbb{R})$)

$$Af(x) := \lim_{t \searrow 0} \frac{E^x f(X_t) - f(x)}{t} \overset{E^x\tau<\infty}{\Longrightarrow} E^x f(X_\tau) = f(x) + E^x \int_0^\tau Af(X_s)ds$$

Theorem (Differential generator for SDE solution and $\phi \in C^2_C(\mathbb{R}^d, \mathbb{R})$)

$$A\phi = L\phi := b\nabla f + \frac{\sigma\sigma^T}{2}\nabla\nabla f = \sum_i b_i \frac{\partial f}{\partial x_i} + \frac{1}{2}\sum_{i,j}(\sigma\sigma^T)_{i,j}\frac{\partial^2 f}{\partial x_i \partial x_j}$$

Soundness

Theorem (Stochastic Differential Invariants)

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

$$\frac{\langle\alpha\rangle(H \to \phi) \leq \lambda p \quad H \to \phi \geq 0 \quad H \to L f \leq 0}{P(\langle\alpha\rangle\langle dx = b dt + \sigma dW \,\&\, H\rangle \phi \geq \lambda) \leq p} \quad \textit{sound}$$

Theorem (Dynkin for càdlàg strong Markov X_t and $\phi \in C_C^2(\mathbb{R}^d, \mathbb{R})$)

$$Af(x) := \lim_{t \searrow 0} \frac{E^x f(X_t) - f(x)}{t} \overset{E^x \tau < \infty}{\Rightarrow} E^x f(X_\tau) = f(x) + E^x \int_0^\tau Af(X_s) ds$$

$$A\phi(X_s) = L\phi(X_s) \leq 0 \text{ on } H \quad \Rightarrow \quad E^x \phi(X_\tau) \leq \phi(x) \forall x, \tau$$

$$\Rightarrow \quad P^x\text{-a.s. } E^x(\phi(X_t) | \mathcal{F}_s) = E^{X_s} \phi(X_{t-s}) \leq \phi(X_s)$$

$$\Rightarrow \quad X_t \text{ supermartingale}$$

Soundness

Theorem (Stochastic Differential Invariants)

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

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

Theorem (Dynkin for càdlàg strong Markov X_t and $\phi \in C_C^2(\mathbb{R}^d, \mathbb{R})$)

$$Af(x) := \lim_{t \searrow 0} \frac{E^x f(X_t) - f(x)}{t} \overset{E^x \tau < \infty}{\Rightarrow} E^x f(X_\tau) = f(x) + E^x \int_0^\tau Af(X_s) ds$$

Theorem (Doob maximal martingale ineq., càdlàg supermartingale)

$$\forall\ f \geq 0, \lambda > 0 \quad P\left(\sup_{t \geq 0} f(X_t) \geq \lambda \,|\, \mathcal{F}_0\right) \leq \frac{Ef(X_0)}{\lambda}$$

Soundness

Theorem (Stochastic Differential Invariants)

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

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

Theorem (Dynkin for càdlàg strong Markov X_t and $\phi \in C_C^2(\mathbb{R}^d, \mathbb{R})$)

$$Af(x) := \lim_{t \searrow 0} \frac{E^x f(X_t) - f(x)}{t} \overset{E^x\tau<\infty}{\Rightarrow} E^x f(X_\tau) = f(x) + E^x \int_0^\tau Af(X_s)ds$$

Theorem (Doob maximal martingale ineq., càdlàg supermartingale)

$$\forall\ f \geq 0, \lambda > 0 \quad P\left(\sup_{t\geq 0} f(X_t) \geq \lambda \,|\, \mathcal{F}_0\right) \leq \frac{Ef(X_0)}{\lambda} \leq \frac{\lambda p}{\lambda} = p$$

Proof Example

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

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

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

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

$\le$ (by **??**)

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

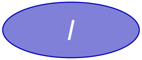
$$\le \frac{1}{3}$$

Outline Background

Image Computation

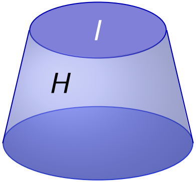
Problem (Image Computation – generic)

Do transitions of system H reach bad state in B from an initial state in I?



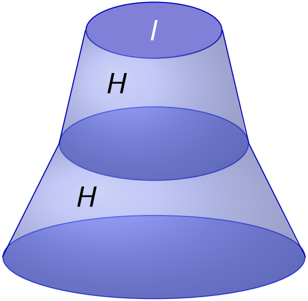
Problem (Image Computation – generic)

Do transitions of system H reach bad state in B from an initial state in I?



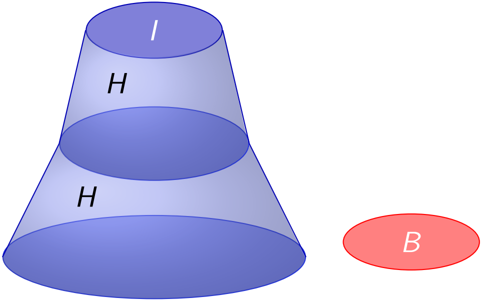
Problem (Image Computation – generic)

Do transitions of system H reach bad state in B from an initial state in I?



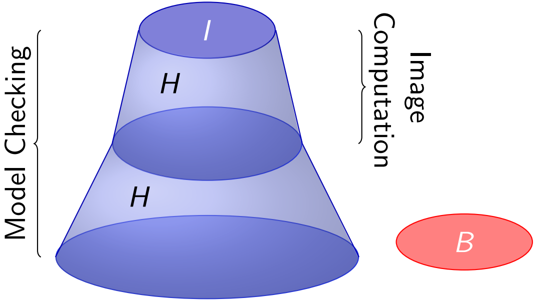
Problem (Image Computation – generic)

Do transitions of system H reach bad state in B from an initial state in I?



Problem (Image Computation – generic)

Do transitions of system H reach bad state in B from an initial state in I?



Problem (Image Computation – continuous transition)

Flow $\varphi : [0,\infty) \times \mathbb{R}^n \to \mathbb{R}^n$ reaches state B, i.e., $\exists t, x_0 : \varphi(t, x_0) \in B$?

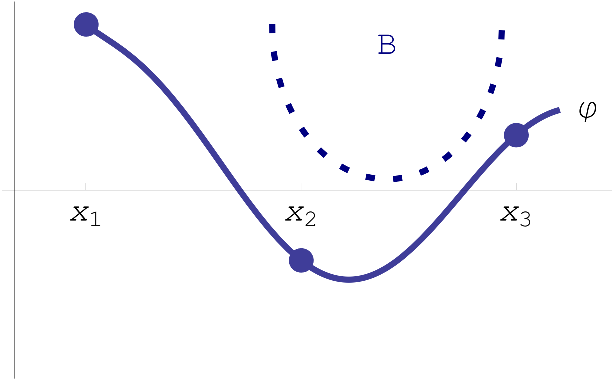
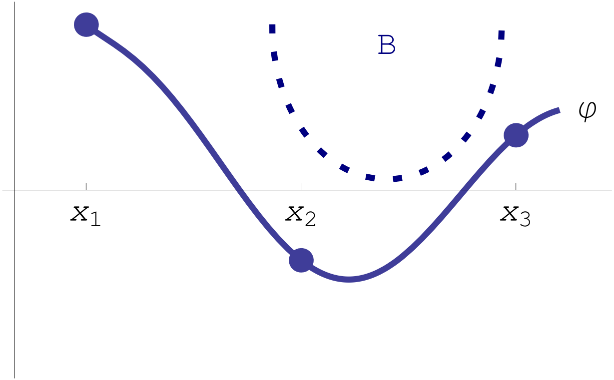


Image Computation: Continuous Systems

Problem (Image Computation – continuous transition)

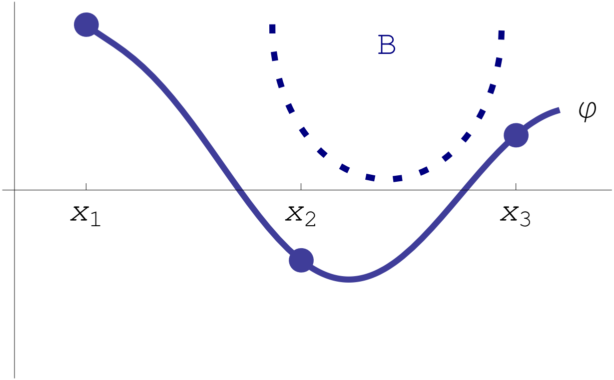
Flow $\varphi : [0,\infty) \times \mathbb{R}^n \to \mathbb{R}^n$ reaches state B, i.e., $\exists t, x_0 : \varphi(t, x_0) \in B$?



Idea: Sample points

Problem (Image Computation – continuous transition)

Flow $\varphi : [0,\infty) \times \mathbb{R}^n \to \mathbb{R}^n$ reaches state B, i.e., $\exists t, x_0 : \varphi(t, x_0) \in B$?

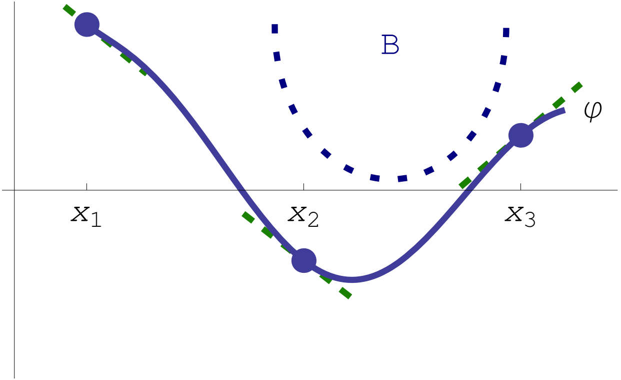


Idea: Sample points

too many!

Problem (Image Computation – continuous transition)

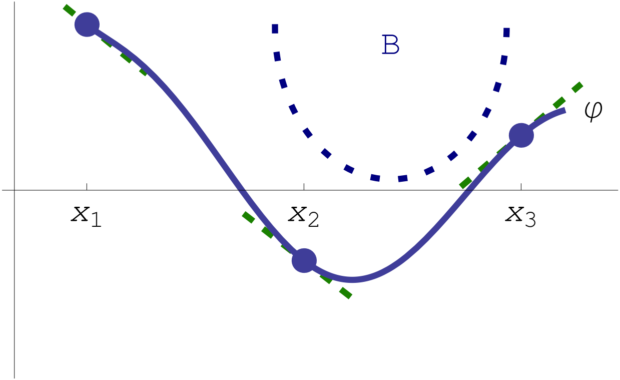
Flow $\varphi : [0, \infty) \times \mathbb{R}^n \to \mathbb{R}^n$ reaches state B, i.e., $\exists t, x_0 : \varphi(t, x_0) \in B$?



Idea: Sample points & derivatives

Problem (Image Computation – continuous transition)

Flow $\varphi : [0,\infty) \times \mathbb{R}^n \to \mathbb{R}^n$ reaches state B, i.e., $\exists t, x_0 : \ \varphi(t, x_0) \in B$?

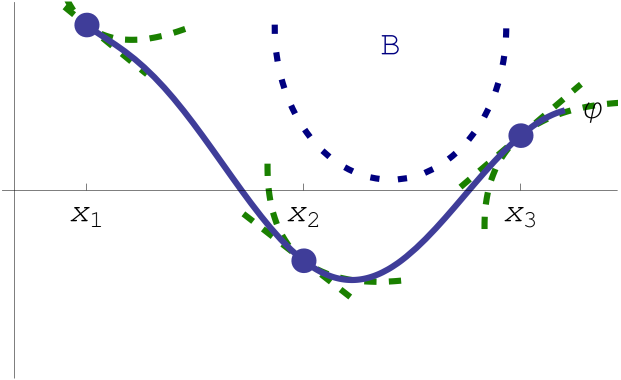


Idea: Sample points & derivatives

too many!

Problem (Image Computation – continuous transition)

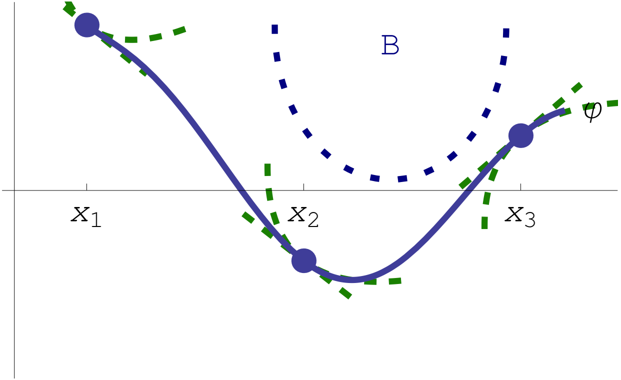
Flow $\varphi : [0,\infty) \times \mathbb{R}^n \to \mathbb{R}^n$ reaches state B, i.e., $\exists t, x_0 : \varphi(t, x_0) \in B$?



Idea: Sample points & derivatives 1&2

Problem (Image Computation – continuous transition)

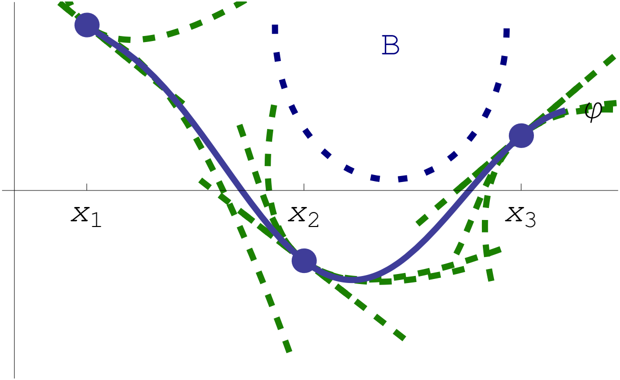
Flow $\varphi : [0,\infty) \times \mathbb{R}^n \to \mathbb{R}^n$ reaches state B, i.e., $\exists t, x_0 : \varphi(t, x_0) \in B$?



Idea: Sample points & derivatives 1&2 too many!

Problem (Image Computation – continuous transition)

Flow $\varphi : [0,\infty) \times \mathbb{R}^n \to \mathbb{R}^n$ reaches state B, i.e., $\exists t, x_0 : \varphi(t, x_0) \in B$?

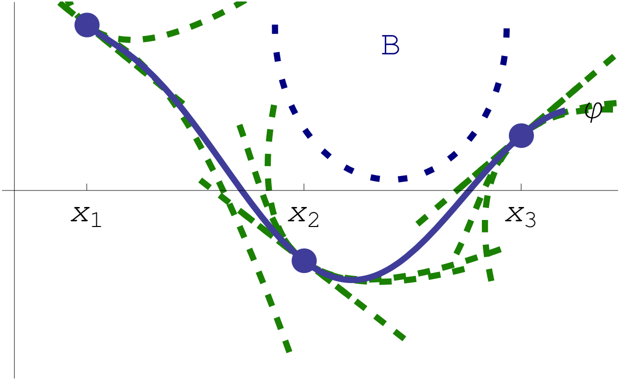


Idea: Sample points & derivatives 1&2&3

Image Computation: Continuous Systems

Problem (Image Computation – continuous transition)

Flow $\varphi : [0,\infty) \times \mathbb{R}^n \to \mathbb{R}^n$ reaches state B, i.e., $\exists t, x_0 : \varphi(t, x_0) \in B$?

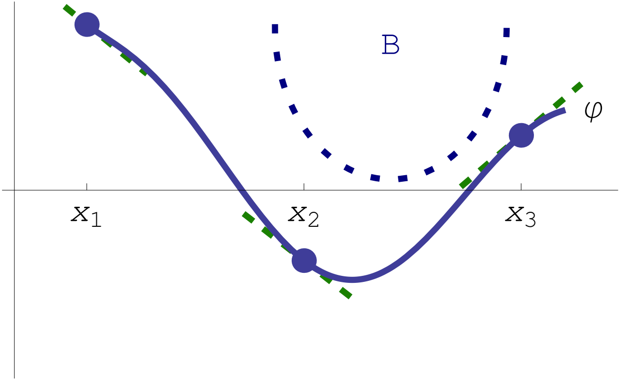


Idea: Sample points & derivatives 1&2&3 too many!

Image Computation: Continuous Systems

Problem (Image Computation – continuous transition)

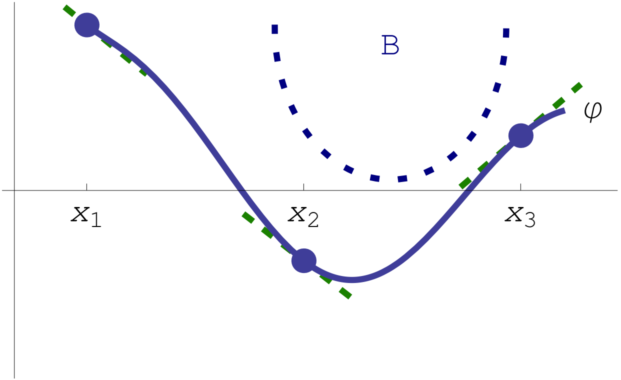
Flow $\varphi : [0, \infty) \times \mathbb{R}^n \to \mathbb{R}^n$ reaches state B, i.e., $\exists t, x_0 : \varphi(t, x_0) \in B$?



Idea: Sample points & X curve & blow up to regions & ...

Problem (Image Computation – continuous transition)

Flow $\varphi : [0,\infty) \times \mathbb{R}^n \to \mathbb{R}^n$ reaches state B, i.e., $\exists t, x_0 : \varphi(t, x_0) \in B$?



Idea: Sample points & X curve & blow up to regions & . . . too many!

Problem (Image Computation – ODE transition)

Flow $\varphi : [0, \infty) \times \mathbb{R}^n \to \mathbb{R}^n$ solving $x' = f(x)$ reaches state B?

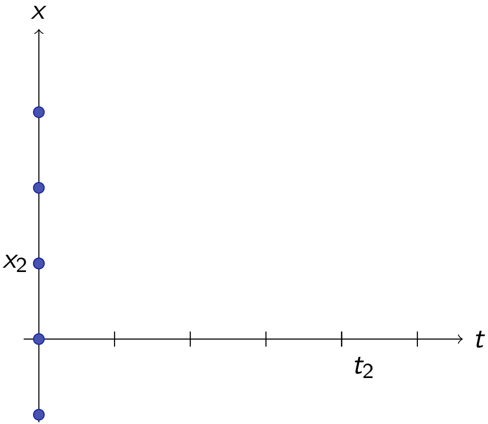
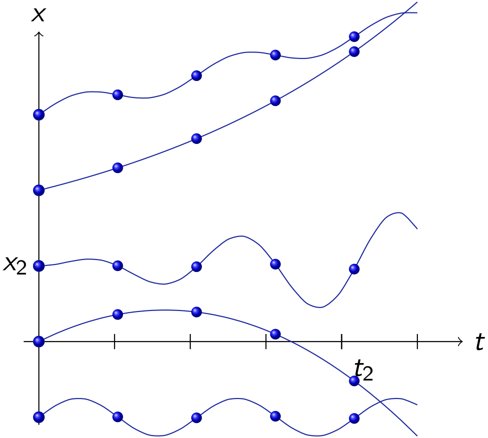


Image Computation: Continuous Systems

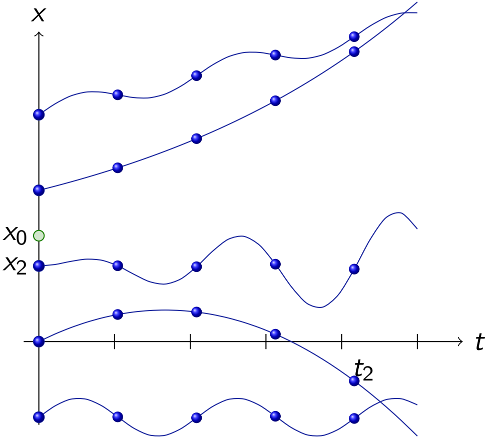
Problem (Image Computation – ODE transition)

Flow $\varphi : [0, \infty) \times \mathbb{R}^n \to \mathbb{R}^n$ solving $x' = f(x)$ reaches state B?



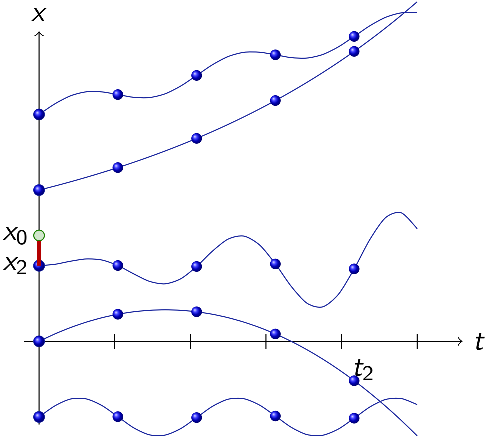
Problem (Image Computation – ODE transition)

Flow $\varphi : [0,\infty) \times \mathbb{R}^n \to \mathbb{R}^n$ solving $x' = f(x)$ reaches state B?



Problem (Image Computation – ODE transition)

Flow $\varphi : [0,\infty) \times \mathbb{R}^n \to \mathbb{R}^n$ solving $x' = f(x)$ reaches state B?



Problem (Image Computation – ODE transition)

Flow $\varphi : [0, \infty) \times \mathbb{R}^n \to \mathbb{R}^n$ solving $x' = f(x)$ reaches state B?

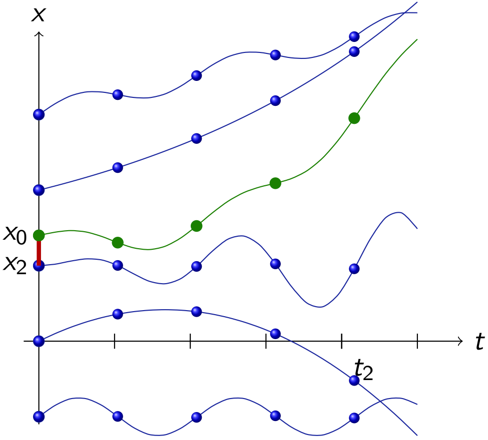
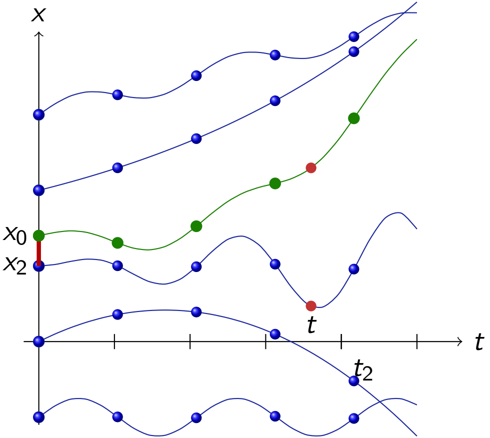


Image Computation: Continuous Systems

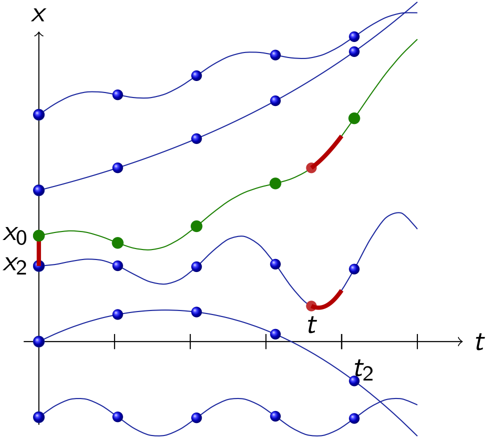
Problem (Image Computation – ODE transition)

Flow $\varphi : [0,\infty) \times \mathbb{R}^n \to \mathbb{R}^n$ solving $x' = f(x)$ reaches state B?



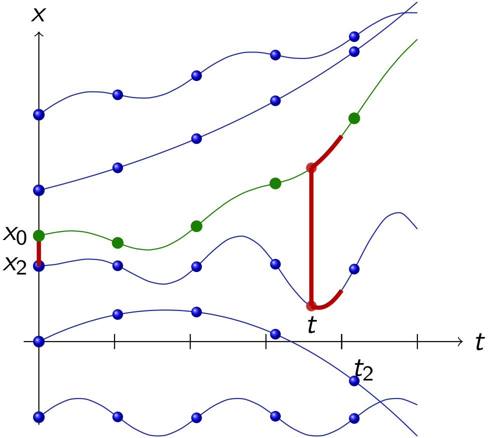
Problem (Image Computation – ODE transition)

Flow $\varphi : [0,\infty) \times \mathbb{R}^n \to \mathbb{R}^n$ solving $x' = f(x)$ reaches state B?



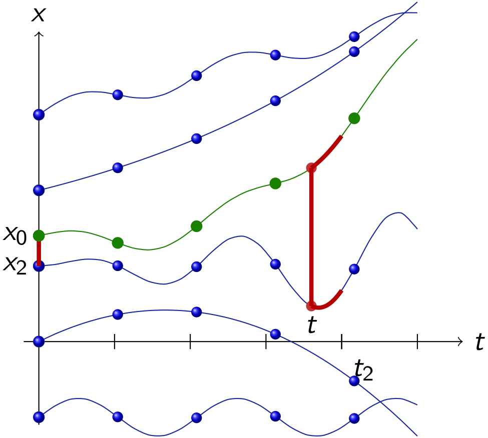
Problem (Image Computation – ODE transition)

Flow $\varphi : [0,\infty) \times \mathbb{R}^n \to \mathbb{R}^n$ solving $x' = f(x)$ reaches state B?



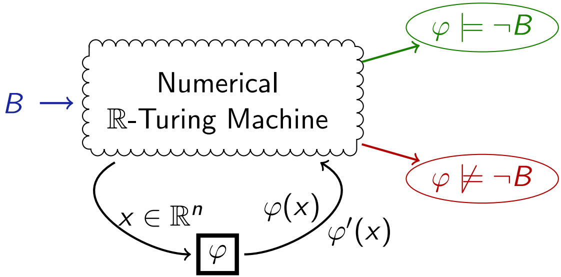
Problem (Image Computation – ODE transition)

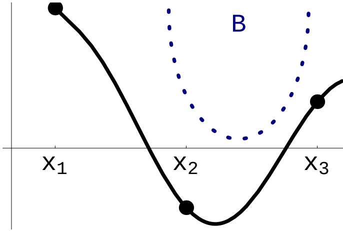
Flow $\varphi : [0, \infty) \times \mathbb{R}^n \to \mathbb{R}^n$ solving $x' = f(x)$ reaches state B?



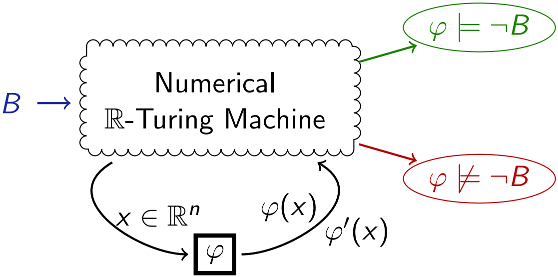
errors!

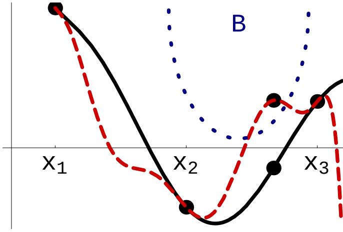
too many!



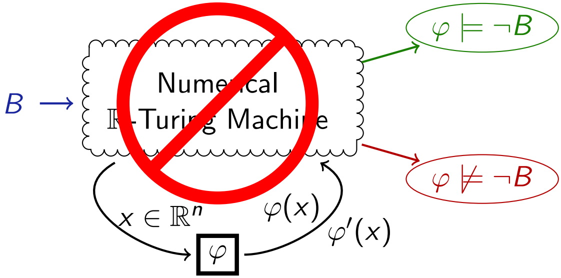


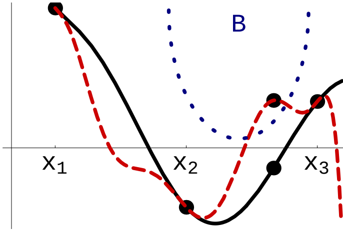
André Platzer and Edmund M. Clarke.
The image computation problem in hybrid systems model checking.
HSCC, vol. 4416 of *LNCS*, 473–486. Springer, 2007.





André Platzer and Edmund M. Clarke.
The image computation problem in hybrid systems model checking.
HSCC, vol. 4416 of *LNCS*, 473–486. Springer, 2007.





Proposition (Image computation undecidable numerically for. . .)

- *arbitrarily effective flow* $\varphi \in C^k(D \subseteq \mathbb{R}^n, \mathbb{R}^m)$*; D, B effective*
- *tolerate error* $\epsilon > 0$ *in decisions*

André Platzer and Edmund M. Clarke.
The image computation problem in hybrid systems model checking.
HSCC, vol. 4416 of *LNCS*, 473–486. Springer, 2007.