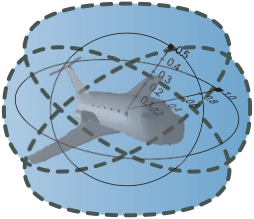
# Dynamic Logic for Dynamical Systems

André Platzer

Carnegie Mellon University

Summer School Marktoberdorf 2017



# Outline

1. CPS are Multi-Dynamical Systems
   - Hybrid Systems / Games / Stochastic / Distributed Hybrid Systems
2. Differential Dynamic Logic
   - Syntax
   - Semantics
   - Example: Car Control Design
3. Dynamic Axioms for Dynamical Systems
   - Axiomatics
   - Example: Safe Car Control
   - Soundness and Completeness
4. Differential Invariants for Differential Equations
   - Differential Axioms
   - Example: Differential Ghosts
5. Applications
6. Summary

# Outline (Introduction to CPS)

1. CPS are Multi-Dynamical Systems
    - Hybrid Systems / Games / Stochastic / Distributed Hybrid Systems
2. Differential Dynamic Logic
    - Syntax
    - Semantics
    - Example: Car Control Design
3. Dynamic Axioms for Dynamical Systems
    - Axiomatics
    - Example: Safe Car Control
    - Soundness and Completeness
4. Differential Invariants for Differential Equations
    - Differential Axioms
    - Example: Differential Ghosts
5. Applications
6. Summary

# Cyber-Physical Systems Analysis: Aircraft Example

Which control decisions are safe for aircraft collision avoidance?

**Cyber-Physical Systems**

CPSs combine cyber capabilities with physical capabilities
to solve problems that neither part could solve alone.

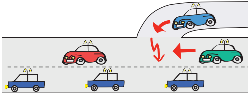
# CPSs Promise Transformative Impact!

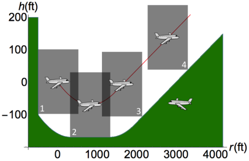
## Prospects: Safe & Efficient

Driver assistance
Autonomous cars

Pilot decision support
Autopilots / UAVs

Train protection
Robots near humans





## Prerequisite: CPSs need to be safe

How do we make sure CPSs make the world a better place?

# Can you trust a computer to control physics?

# Can you trust a computer to control physics?

1. Depends on how it has been programmed
2. And on what will happen if it malfunctions

## Rationale

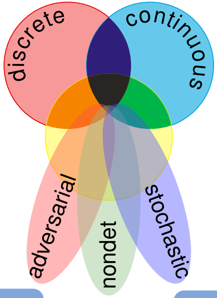
1. Safety guarantees require analytic foundations.
2. A common foundational core helps all application domains.
3. Foundations revolutionized digital computer science & our society.
4. Need even stronger foundations when software reaches out into our physical world.

**CPSs deserve proofs as safety evidence!**

# CPSs are Multi-Dynamical Systems

**CPS Dynamics**

CPS are characterized by multiple facets of dynamical systems.



**CPS Compositions**

CPS combines multiple simple dynamical effects.

Descriptive simplification

**Tame Parts**

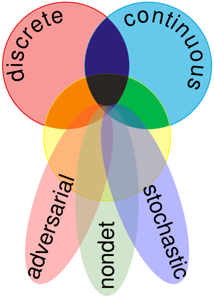
Exploiting compositionality tames CPS complexity.

Analytic simplification

# CPSs are Multi-Dynamical Systems

**hybrid systems**

HS = discrete + ODE

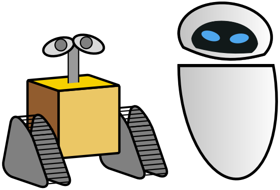


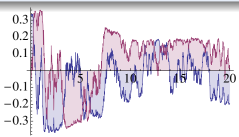
**hybrid games**

HG = HS + adversary

**stochastic hybrid sys.**

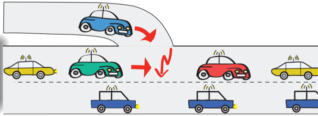
SHS = HS + stochastics





**distributed hybrid sys.**

DHS = HS + distributed



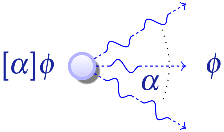
# Outline (Modeling CPS)

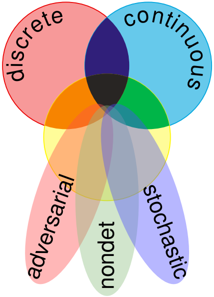
1. CPS are Multi-Dynamical Systems
   - Hybrid Systems / Games / Stochastic / Distributed Hybrid Systems
2. Differential Dynamic Logic
   - Syntax
   - Semantics
   - Example: Car Control Design
3. Dynamic Axioms for Dynamical Systems
   - Axiomatics
   - Example: Safe Car Control
   - Soundness and Completeness
4. Differential Invariants for Differential Equations
   - Differential Axioms
   - Example: Differential Ghosts
5. Applications
6. Summary

# Dynamic Logics for Dynamical Systems

**differential dynamic logic**

$\text{dL} = \text{DL} + \text{HP}$



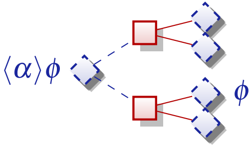


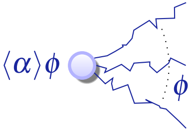
**differential game logic**

$\text{dGL} = \text{GL} + \text{HG}$

**stochastic differential DL**

$\text{SdL} = \text{DL} + \text{SHP}$





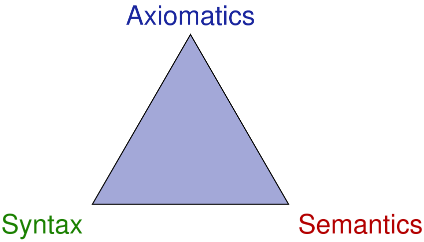
**quantified differential DL**

$\text{QdL} = \text{FOL} + \text{DL} + \text{QHP}$

JAR'08,CADE'11,LMCS'12,LICS'12,LICS'12

TOCL'15,CADE'15,JAR'17,TOCL'17

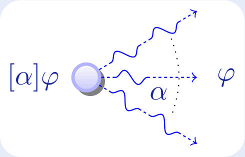
# Logical Trinity

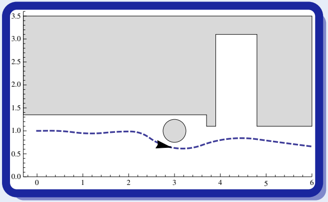


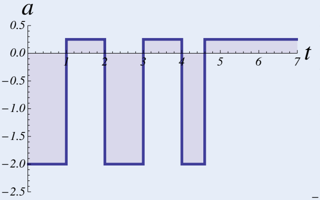
| | |
|---|---|
| Syntax | defines the notation<br>What problems are we allowed to write down? |
| Semantics | what carries meaning.<br>What real or mathematical objects does the syntax stand for? |
| Axiomatics | internalizes semantic relations into universal syntactic trafo.<br>How does the semantics of $A$ relate to semantics of $A \land B$, syntactically? If $A$ is true, is $A \land B$ true, too? Conversely? |

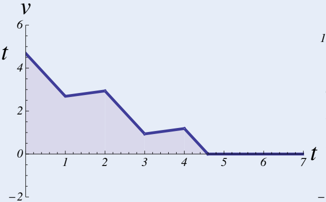
# CPS Analysis

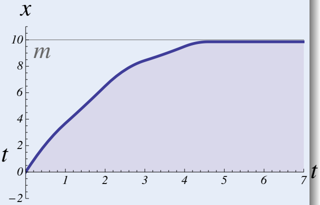
## Concept (Differential Dynamic Logic) (JAR'08,LICS'12)





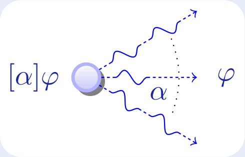


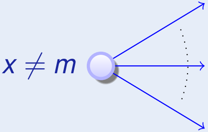


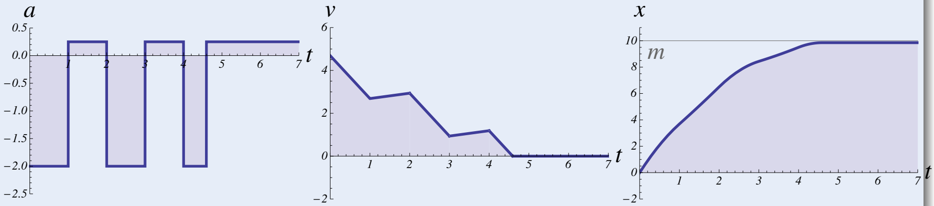


# CPS Analysis

## Concept (Differential Dynamic Logic) (JAR'08,LICS'12)

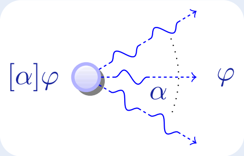


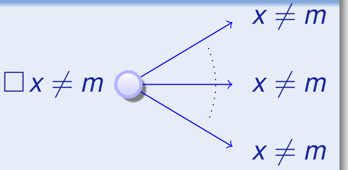


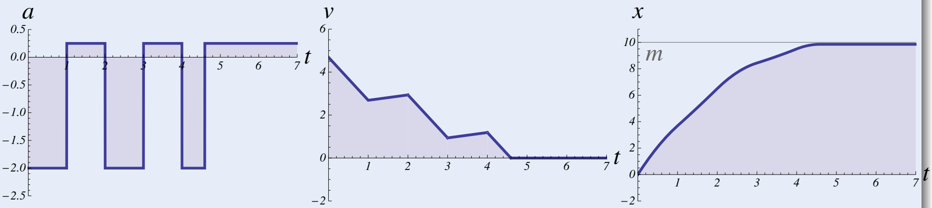


# CPS Analysis

## Concept (Differential Dynamic Logic) (JAR'08,LICS'12)

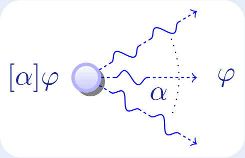


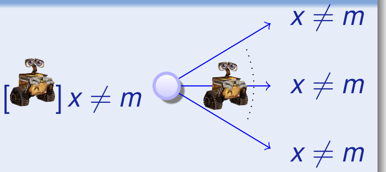


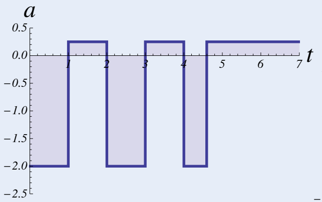


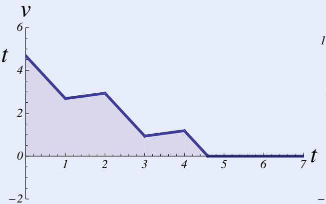
# CPS Analysis

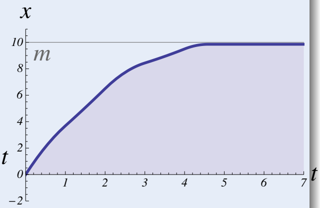
## Concept (Differential Dynamic Logic) (JAR'08,LICS'12)





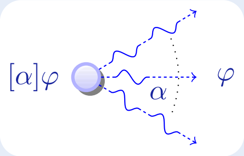


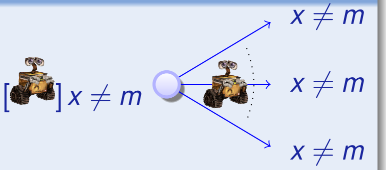




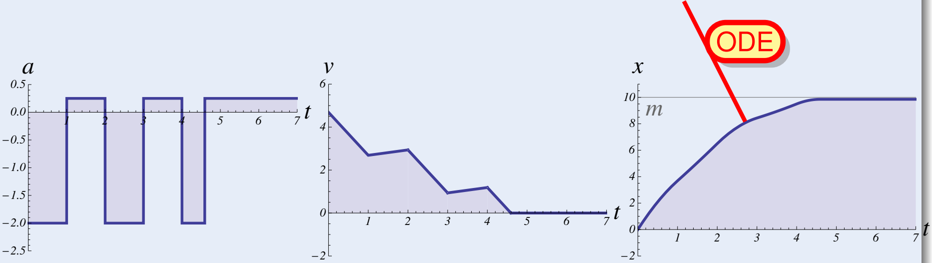
# CPS Analysis

## Concept (Differential Dynamic Logic) (JAR'08,LICS'12)



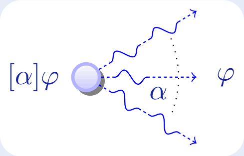


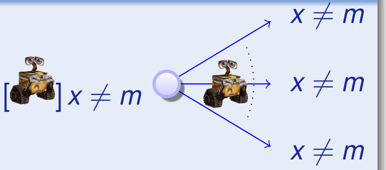
$x' = v, v' = a$



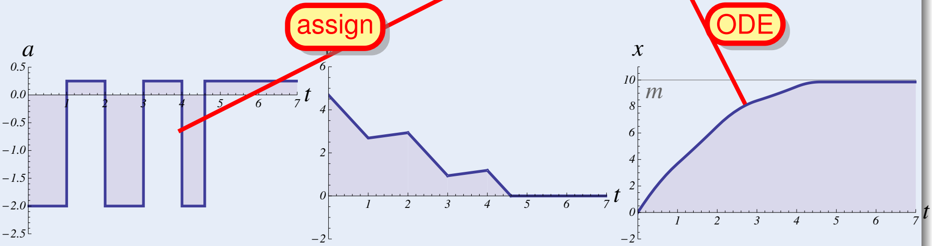
# CPS Analysis

## Concept (Differential Dynamic Logic) (JAR'08,LICS'12)



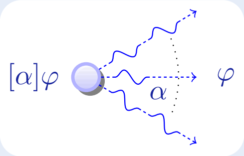


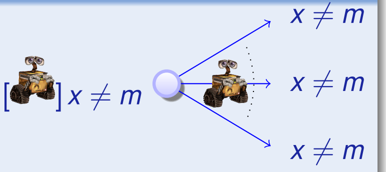
$a := -b$  $x' = v, v' = a$



# CPS Analysis

## Concept (Differential Dynamic Logic) (JAR'08,LICS'12)

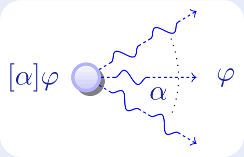




$(\text{if}(SB(x,m)) \quad a := -b) \quad x' = v, v' = a$

# CPS Analysis

## Concept (Differential Dynamic Logic) (JAR'08,LICS'12)



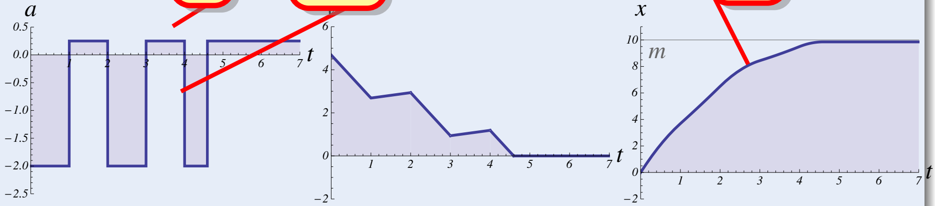
seq. compose

$$(\text{if}(SB(x,m))\quad a:=-b)\ ;\ x'=v, v'=a$$

test

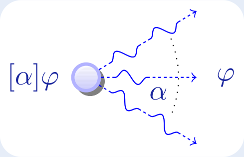
assign

ODE



# CPS Analysis

## Concept (Differential Dynamic Logic) (JAR'08,LICS'12)



seq. compose

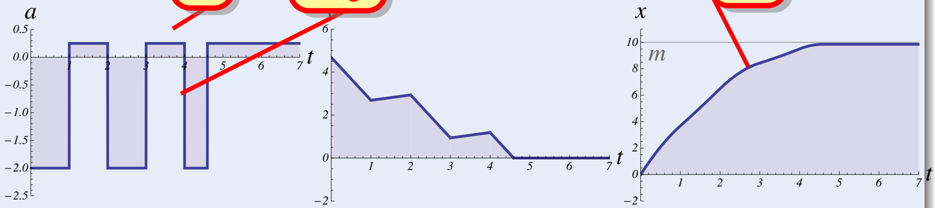
nondet. repeat

$$\big((\text{if}(\mathrm{SB}(x,m))\quad a := -b)\ ;\ x' = v, v' = a\big)^*$$

test

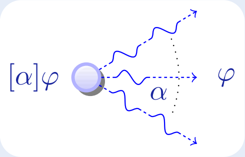
assign

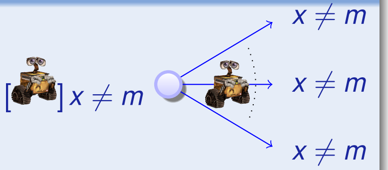
ODE



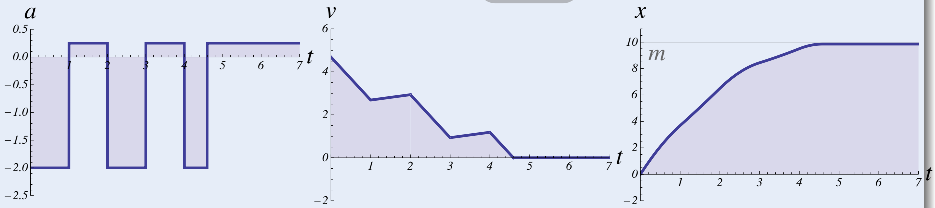
# CPS Analysis

## Concept (Differential Dynamic Logic) (JAR'08,LICS'12)



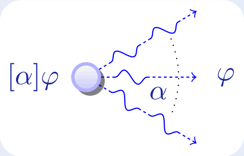


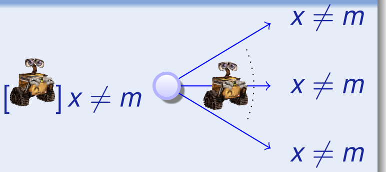
$$\underbrace{[((\text{if}(SB(x,m)) \quad a:=-b) ; x' = v, v' = a)^*]}_{\text{all runs}} \underbrace{x \neq m}_{\text{post}}$$



# CPS Analysis

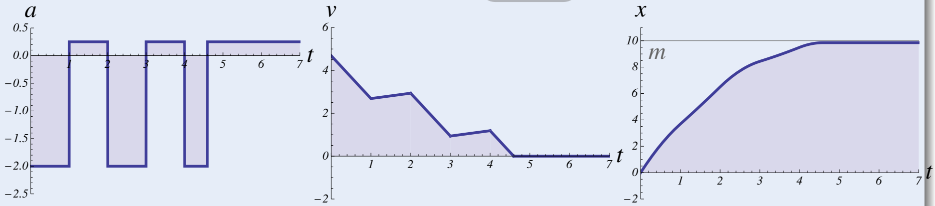
## Concept (Differential Dynamic Logic) (JAR'08,LICS'12)





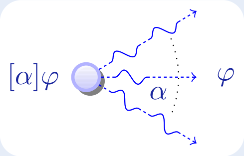
$$\underbrace{x \neq m \wedge b > 0}_{\text{init}} \rightarrow \Big[\Big(\big(\text{if}(SB(x,m))\quad a := -b\big)\;;\; x' = v, v' = a\Big)^*\Big]\underbrace{x \neq m}_{\text{post}}$$

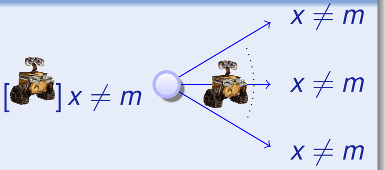
all runs



# CPS Analysis

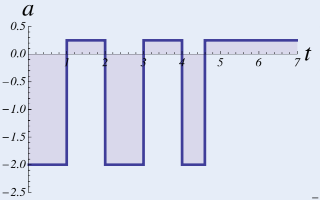
## Concept (Differential Dynamic Logic) (JAR'08,LICS'12)

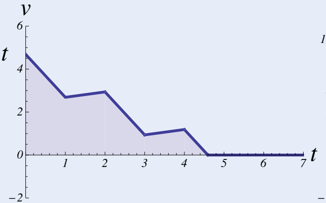


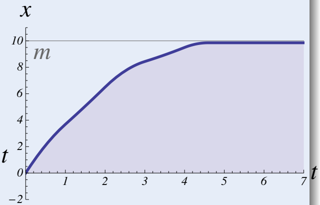


nondet. choice

$$\underbrace{x \neq m \land b > 0}_{\text{init}} \to \left[\left(\left(?\neg SB(x,m) \cup a := -b\right) ;\ x' = v, v' = a\right)^*\right] \underbrace{x \neq m}_{\text{post}}$$

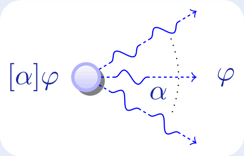


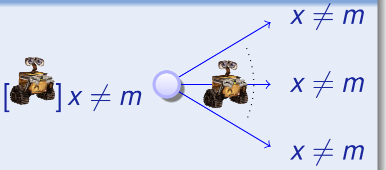




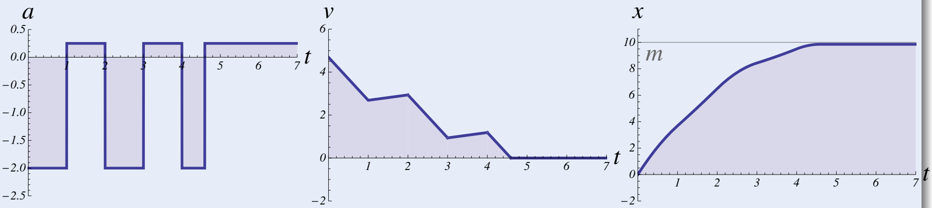
# CPS Analysis

## Concept (Differential Dynamic Logic) (JAR'08,LICS'12)



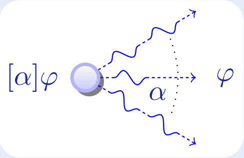


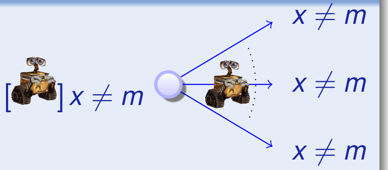
$$\underbrace{x \neq m \land b > 0}_{\text{init}} \to \left[\left(\left(\overset{\text{test}}{?}\neg SB(x,m) \overset{\text{nondet. choice}}{\cup} a := -b\right) ; \; x' = v, v' = a\right)^*\right] \underbrace{x \neq m}_{\text{post}}$$



# CPS Analysis

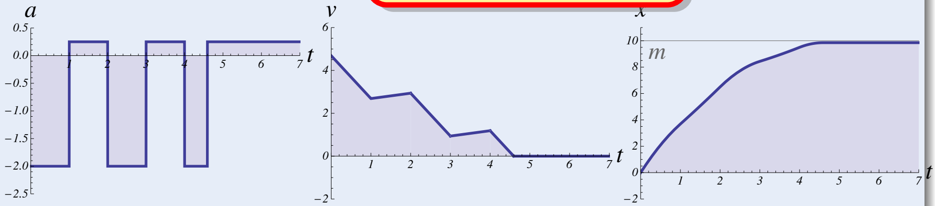
## Concept (Differential Dynamic Logic) (JAR'08,LICS'12)





$$\underbrace{x \neq m \land b > 0}_{\text{init}} \to \Big[\Big(\big(?\neg SB(x,m) \cup a := -b\big) \,;\, x' = v, v' = a\Big)^*\Big]\underbrace{x \neq m}_{\text{post}}$$

hybrid program dynamics



# Differential Dynamic Logic dL: Syntax

**Definition (Hybrid program $\alpha$)**

$$x := f(x) \mid ?Q \mid x' = f(x) \,\&\, Q \mid \alpha \cup \beta \mid \alpha;\beta \mid \alpha^*$$

**Definition (dL Formula $P$)**

$$e \geq \tilde{e} \mid \neg P \mid P \wedge Q \mid \forall x\, P \mid \exists x\, P \mid [\alpha]P \mid \langle\alpha\rangle P$$

JAR'08,LICS'12,JAR'17

# Differential Dynamic Logic dL: Syntax

Discrete Assign

Test Condition

Differential Equation

Nondet. Choice

Seq. Compose

Nondet. Repeat

**Definition (Hybrid program $\alpha$)**

$$x := f(x) \mid ?Q \mid x' = f(x) \,\&\, Q \mid \alpha \cup \beta \mid \alpha ; \beta \mid \alpha^*$$

**Definition (dL Formula $P$)**

$$e \geq \tilde{e} \mid \neg P \mid P \wedge Q \mid \forall x\, P \mid \exists x\, P \mid [\alpha]P \mid \langle \alpha \rangle P$$

All Reals

Some Reals

All Runs

Some Runs

JAR'08,LICS'12,JAR'17

# Differential Dynamic Logic dL: Semantics

**Definition (Hybrid program semantics)** $([\![\cdot]\!] : \mathrm{HP} \to \wp(\mathscr{S} \times \mathscr{S}))$

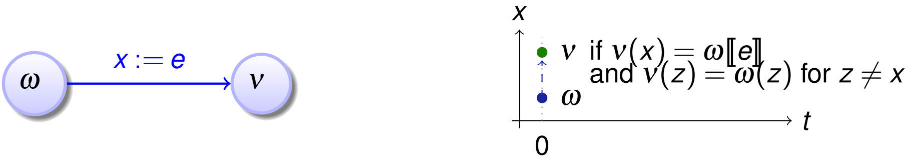
$$\begin{aligned}
[\![x := e]\!] &= \{(\omega,\nu) \;:\; \nu = \omega \text{ except } \nu[\![x]\!] = \omega[\![e]\!]\}\\
[\![?Q]\!] &= \{(\omega,\omega) \;:\; \omega \in [\![Q]\!]\}\\
[\![x' = f(x)]\!] &= \{(\varphi(0),\varphi(r)) \;:\; \varphi \models x' = f(x) \text{ for some duration } r\}\\
[\![\alpha \cup \beta]\!] &= [\![\alpha]\!] \cup [\![\beta]\!]\\
[\![\alpha;\beta]\!] &= [\![\alpha]\!] \circ [\![\beta]\!]\\
[\![\alpha^*]\!] &= [\![\alpha]\!]^* = \bigcup_{n\in\mathbb{N}} [\![\alpha^n]\!]
\end{aligned}$$

compositional semantics

**Definition (dL semantics)** $([\![\cdot]\!] : \mathrm{Fml} \to \wp(\mathscr{S}))$

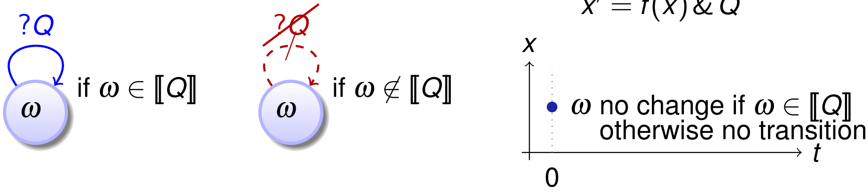
$$\begin{aligned}
[\![e \geq \tilde{e}]\!] &= \{\omega \;:\; \omega[\![e]\!] \geq \omega[\![\tilde{e}]\!]\}\\
[\![\neg P]\!] &= [\![P]\!]^{\complement}\\
[\![P \wedge Q]\!] &= [\![P]\!] \cap [\![Q]\!]\\
[\![\langle\alpha\rangle P]\!] &= [\![\alpha]\!] \circ [\![P]\!] = \{\omega \;:\; \nu \in [\![P]\!] \text{ for some } \nu :\; (\omega,\nu) \in [\![\alpha]\!]\}\\
[\![[\alpha]P]\!] &= [\![\neg\langle\alpha\rangle\neg P]\!] = \{\omega \;:\; \nu \in [\![P]\!] \text{ for all } \nu :\; (\omega,\nu) \in [\![\alpha]\!]\}\\
[\![\exists x\, P]\!] &= \{\omega \;:\; \omega_x^r \in [\![P]\!] \text{ for some } r \in \mathbb{R}\}
\end{aligned}$$

# Differential Dynamic Logic dL: Semantics



if $\nu(x) = \omega[\![e]\!]$ and $\nu(z) = \omega(z)$ for $z \neq x$

$x' = f(x) \,\&\, Q$

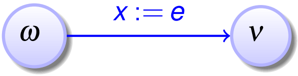


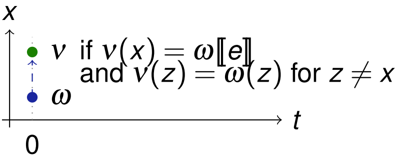
if $\omega \in [\![Q]\!]$

if $\omega \notin [\![Q]\!]$

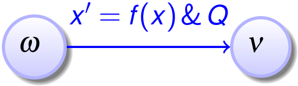
$\omega$ no change if $\omega \in [\![Q]\!]$ otherwise no transition

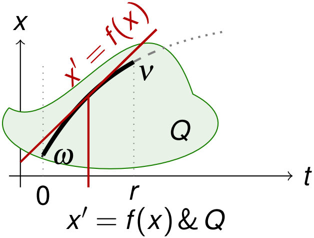
# Differential Dynamic Logic dL: Semantics



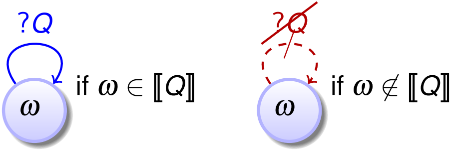


$\nu$ if $\nu(x) = \omega[\![e]\!]$
and $\nu(z) = \omega(z)$ for $z \neq x$



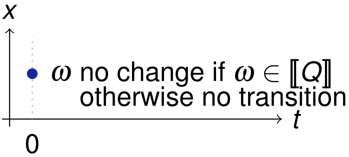


$x' = f(x) \,\&\, Q$



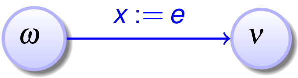
if $\omega \in [\![Q]\!]$

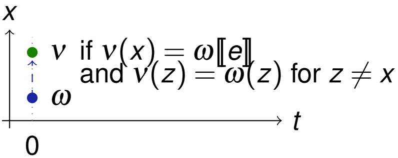
if $\omega \notin [\![Q]\!]$



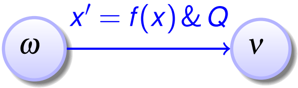
$\omega$ no change if $\omega \in [\![Q]\!]$
otherwise no transition

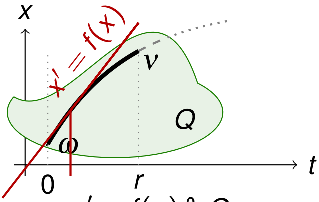
# Differential Dynamic Logic dL: Semantics



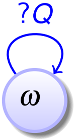


$\nu$ if $\nu(x) = \omega[\![e]\!]$ and $\nu(z) = \omega(z)$ for $z \neq x$

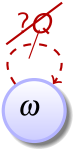




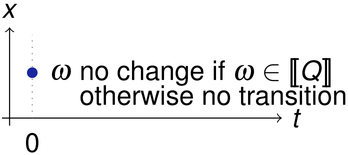
$x' = f(x) \,\&\, Q$



if $\omega \in [\![Q]\!]$

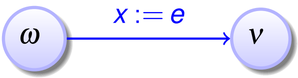


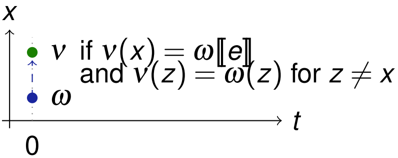
if $\omega \notin [\![Q]\!]$



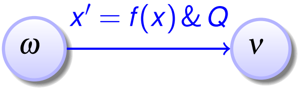
$\omega$ no change if $\omega \in [\![Q]\!]$ otherwise no transition

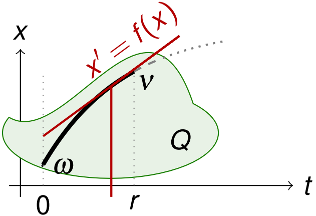
# Differential Dynamic Logic dL: Semantics



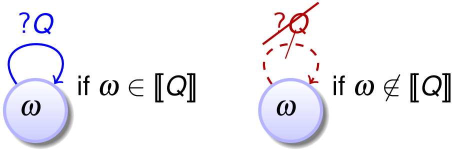


$\nu$ if $\nu(x) = \omega[\![e]\!]$
and $\nu(z) = \omega(z)$ for $z \neq x$



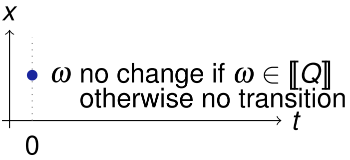


$x' = f(x) \,\&\, Q$



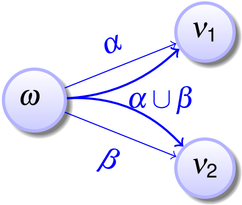
if $\omega \in [\![Q]\!]$

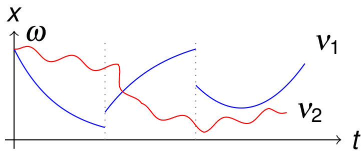
if $\omega \notin [\![Q]\!]$

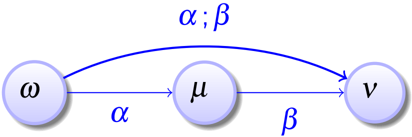


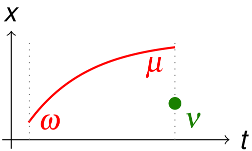
$\omega$ no change if $\omega \in [\![Q]\!]$
otherwise no transition

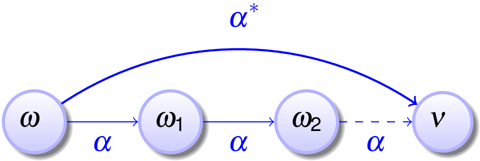
# Differential Dynamic Logic dL: Semantics

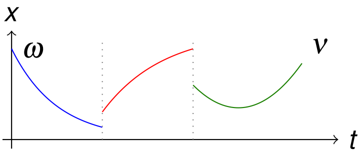




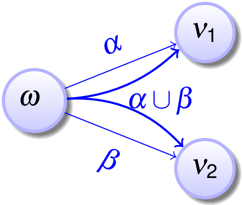


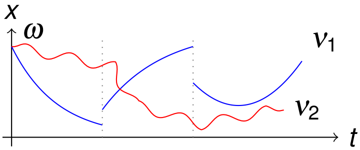


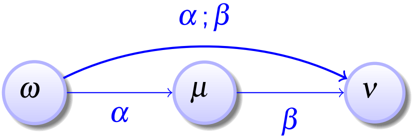


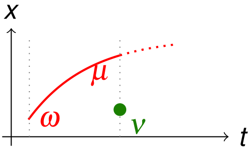


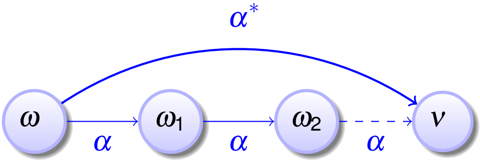
# Differential Dynamic Logic dL: Semantics

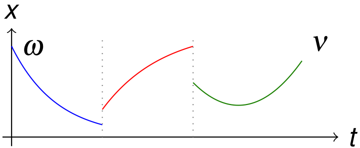




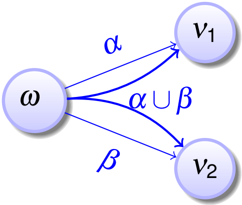


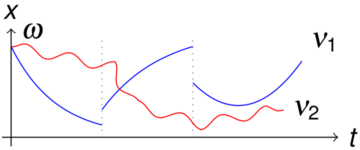


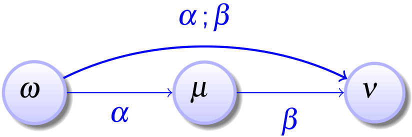


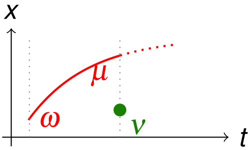


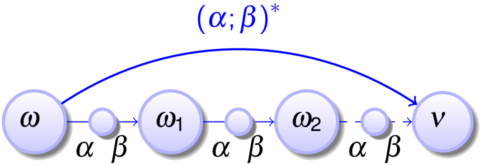
# Differential Dynamic Logic dL: Semantics

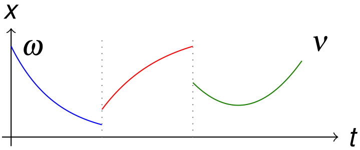






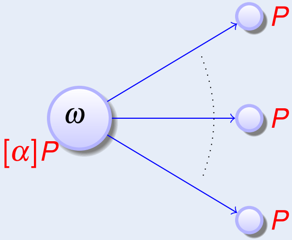






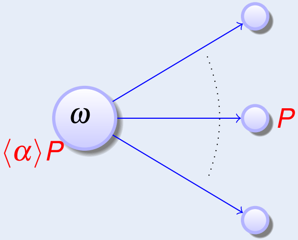
# Differential Dynamic Logic dL: Semantics

## Definition (dL Formulas)



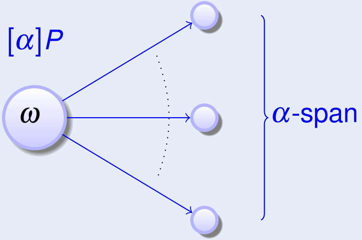
# Differential Dynamic Logic dL: Semantics

## Definition (dL Formulas)



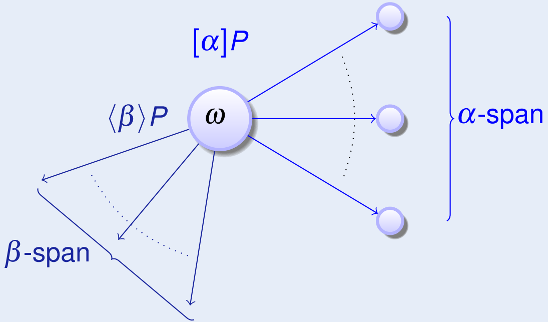
# Differential Dynamic Logic dL: Semantics

## Definition (dL Formulas)



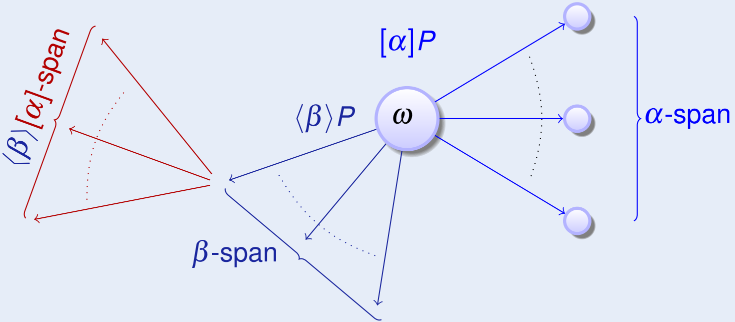
# Differential Dynamic Logic dL: Semantics

## Definition (dL Formulas)



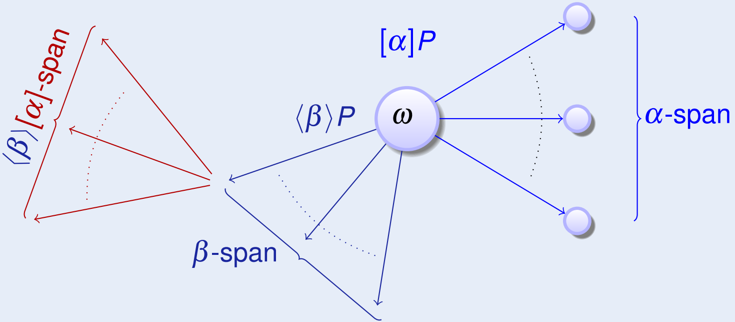
# Differential Dynamic Logic dL: Semantics

## Definition (dL Formulas)



# Differential Dynamic Logic dL: Semantics

## Definition (dL Formulas)



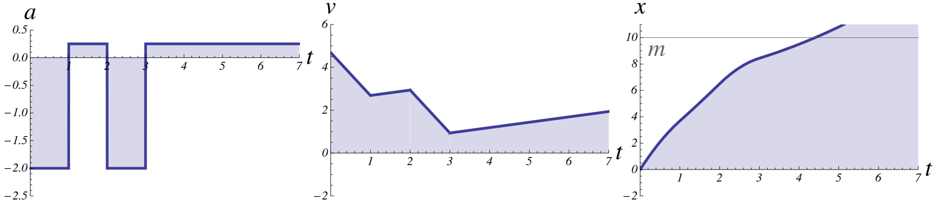
compositional semantics $\Rightarrow$ compositional proofs!

# Ex: Car Control Programs

Repeat control decisions

**Example (Single car $car_s$)**

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

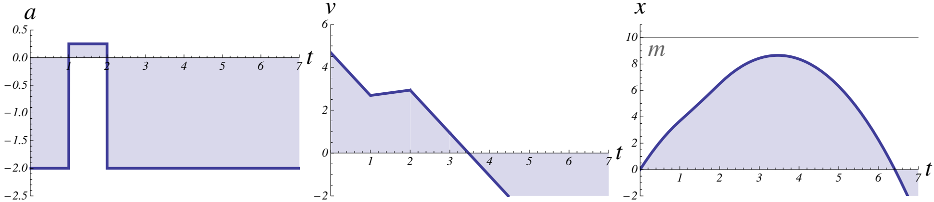


# Ex: Car Control Programs

How does this model brake?

**Example (  Single car $car_s$)**

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

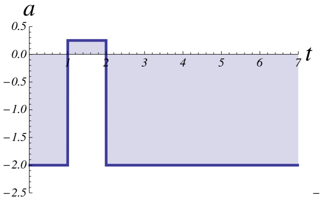


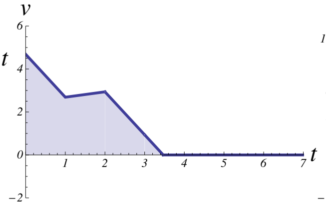
# Ex: Car Control Programs

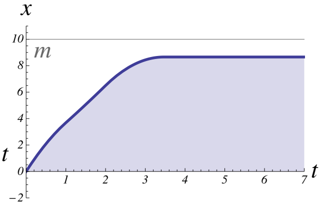
Velocity bound $v \geq 0$ in evolution domain

**Example (▶ Single car $car_s$)**

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





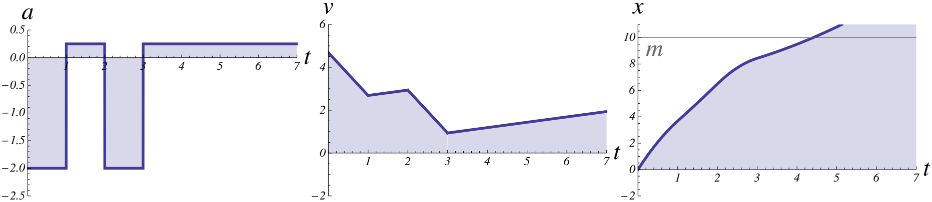


# Ex: Car Control Programs

Acceleration not always safe

**Example (▶ Single car $car_s$)**

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

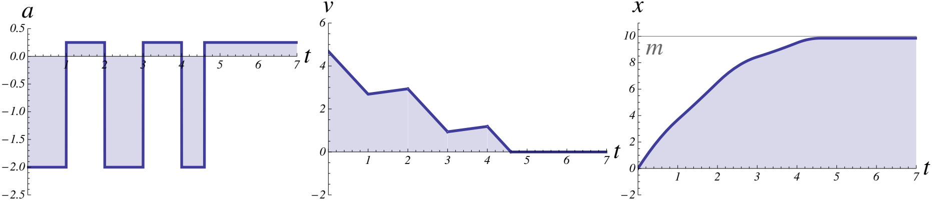


# Ex: Car Control Programs

Acceleration condition $?Q$

**Example ( Single car $car_s$)**

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



# Ex: Car Control Properties

time-triggered

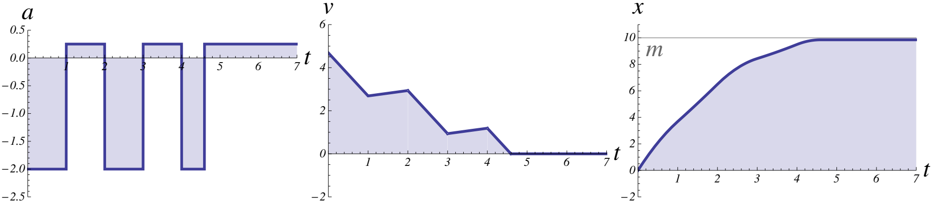
$Q \equiv$

**Example (Single car $car_\varepsilon$ time-triggered)**

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

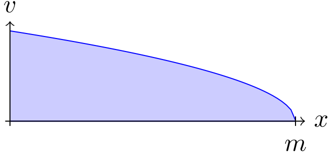
**Example (▶ Safely stays before traffic light $m$)**

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



# Ex: Car Control Properties

$Q \equiv$

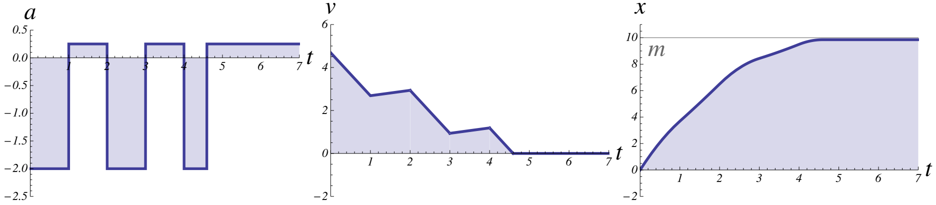


## Example (Single car $car_\varepsilon$ time-triggered)

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

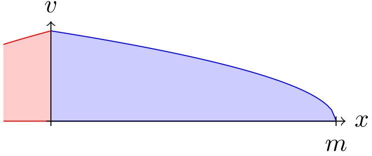
## Example (▶ Safely stays before traffic light $m$)

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



# Ex: Car Control Properties

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

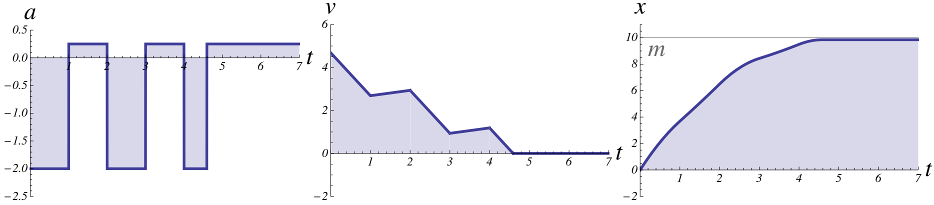


### Example (Single car $car_\varepsilon$ time-triggered)

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

### Example (▶ Safely stays before traffic light $m$)

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



# Ex: Car Control Properties

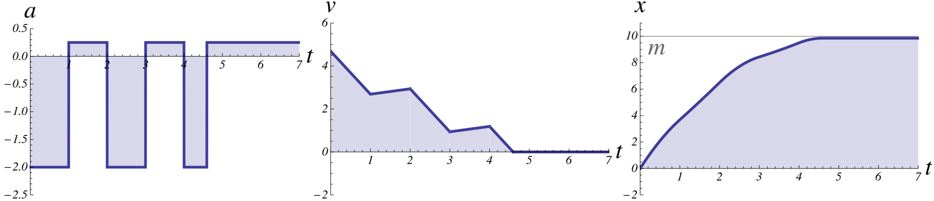
$$Q \equiv 2b(m-x) \geq v^2 + \left(A+b\right)\left(A\varepsilon^2 + 2\varepsilon v\right)$$

**Example (Single car $car_\varepsilon$ time-triggered)**

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

**Example (▶ Live, can move everywhere)**

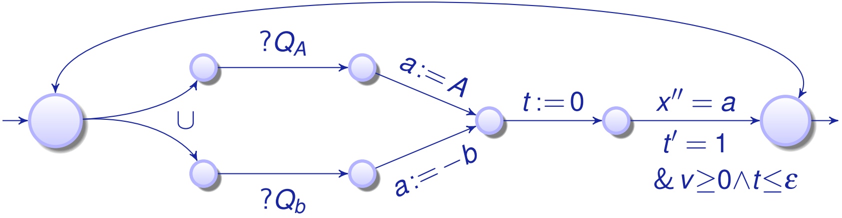
$$\varepsilon > 0 \land A > 0 \land b > 0 \rightarrow \forall p \exists m \langle car_\varepsilon \rangle x \geq p$$



# Branching Transition Structure in Hybrid Programs

$$\begin{aligned}
\text{car} &\equiv (\text{ctrl}\,;\text{drive})^* \\
\text{ctrl} &\equiv (?Q_A; a := A) \\
&\quad \cup (?Q_b; a := -b) \\
\text{drive} &\equiv t := 0; \{x' = v, v' = a, t' = 1 \,\&\, v \geq 0 \land t \leq \varepsilon\}
\end{aligned}$$

# Branching Transition Structure in Hybrid Programs



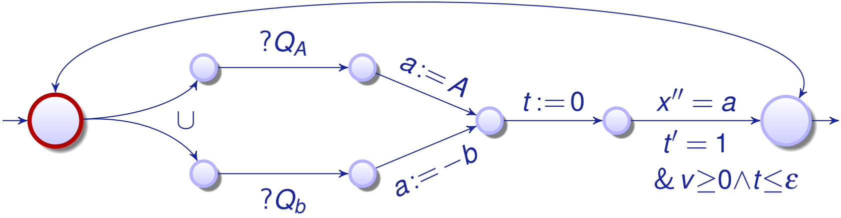
$$\text{car} \equiv (\text{ctrl}\,;\text{drive})^*$$

$$\text{ctrl} \equiv (?Q_A; a := A)$$

$$\cup\,(?Q_b; a := -b)$$

$$\text{drive} \equiv t := 0; \{x' = v, v' = a, t' = 1 \,\&\, v \geq 0 \land t \leq \varepsilon\}$$

# Branching Transition Structure in Hybrid Programs



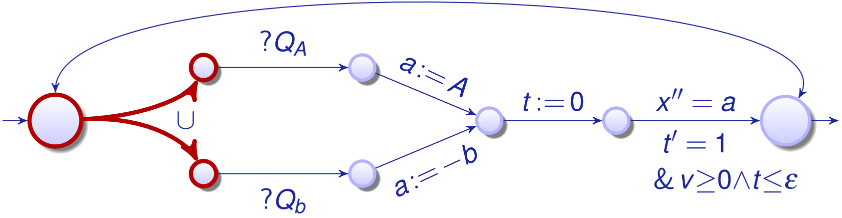
$$\text{car} \equiv (\text{ctrl}\,;\text{drive})^*$$

$$\text{ctrl} \equiv (?Q_A; a := A)$$

$$\cup (?Q_b; a := -b)$$

$$\text{drive} \equiv t := 0; \{x' = v, v' = a, t' = 1 \,\&\, v \geq 0 \land t \leq \varepsilon\}$$

# Branching Transition Structure in Hybrid Programs



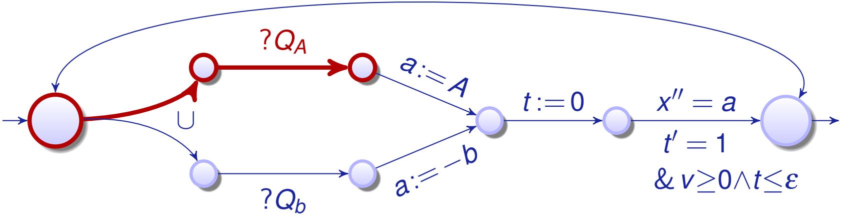
$$\text{car} \equiv (\text{ctrl} \,; \text{drive})^*$$

$$\text{ctrl} \equiv (?Q_A; a := A)$$

$$\cup (?Q_b; a := -b)$$

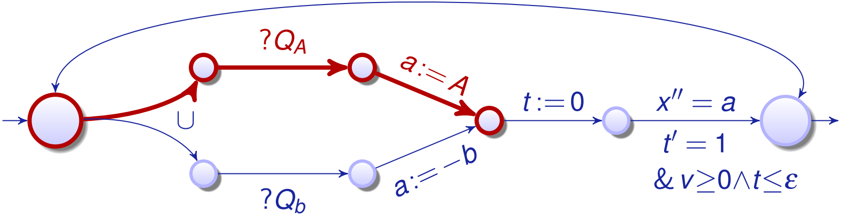
$$\text{drive} \equiv t := 0; \{x' = v, v' = a, t' = 1 \,\&\, v \geq 0 \land t \leq \varepsilon\}$$

# Branching Transition Structure in Hybrid Programs



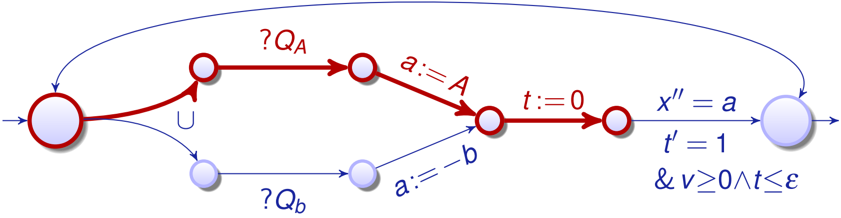
$$
\begin{aligned}
\text{car} &\equiv (\text{ctrl}\,;\text{drive})^* \\
\text{ctrl} &\equiv (?Q_A; a := A) \\
&\quad \cup (?Q_b; a := -b) \\
\text{drive} &\equiv t := 0; \{x' = v, v' = a, t' = 1 \,\&\, v \geq 0 \land t \leq \varepsilon\}
\end{aligned}
$$

# Branching Transition Structure in Hybrid Programs



$$\begin{aligned} \text{car} &\equiv (\text{ctrl} ; \text{drive})^* \\ \text{ctrl} &\equiv (?Q_A; a := A) \\ &\quad \cup (?Q_b; a := -b) \\ \text{drive} &\equiv t := 0; \{x' = v, v' = a, t' = 1 \,\&\, v \geq 0 \land t \leq \varepsilon\} \end{aligned}$$

# Branching Transition Structure in Hybrid Programs



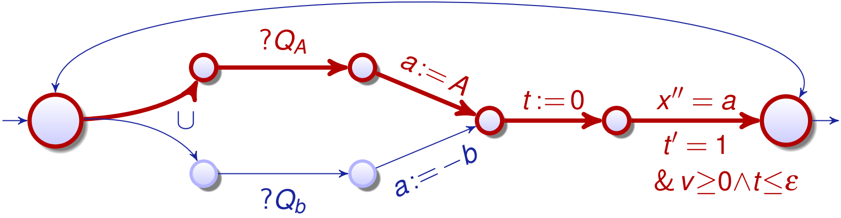
$$\mathrm{car} \equiv (\mathrm{ctrl}\,;\mathrm{drive})^*$$

$$\mathrm{ctrl} \equiv (?Q_A; a := A)$$

$$\cup (?Q_b; a := -b)$$

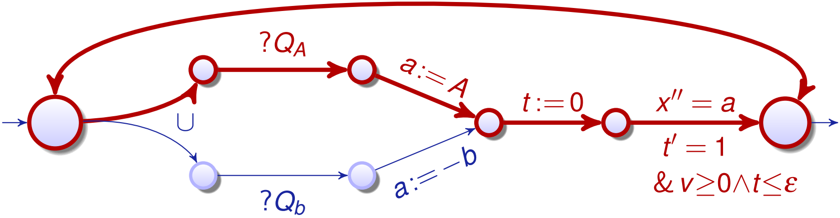
$$\mathrm{drive} \equiv t := 0; \{x' = v, v' = a, t' = 1 \,\&\, v \geq 0 \wedge t \leq \varepsilon\}$$

# Branching Transition Structure in Hybrid Programs



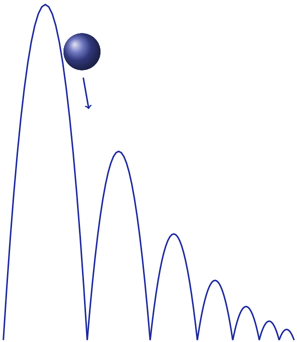
$$\begin{aligned}
\text{car} &\equiv (\text{ctrl}\,;\text{drive})^* \\
\text{ctrl} &\equiv (?Q_A; a := A) \\
&\quad \cup (?Q_b; a := -b) \\
\text{drive} &\equiv t := 0; \{x' = v, v' = a, t' = 1 \,\&\, v \geq 0 \land t \leq \varepsilon\}
\end{aligned}$$

# Branching Transition Structure in Hybrid Programs



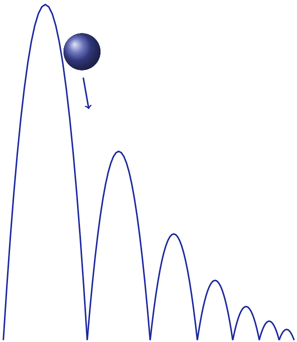
$$\begin{aligned} \text{car} &\equiv (\text{ctrl}\,;\text{drive})^* \\ \text{ctrl} &\equiv (?Q_A; a := A) \\ &\quad \cup (?Q_b; a := -b) \\ \text{drive} &\equiv t := 0; \{x' = v, v' = a, t' = 1 \,\&\, v \geq 0 \land t \leq \varepsilon\} \end{aligned}$$

# Ex: The Acrophobic Bouncing Ball



**Example (▶ Bouncing Ball)**

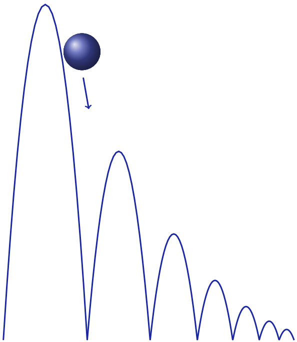
# Ex: The Acrophobic Bouncing Ball



**Example (▶ Bouncing Ball)**

$$\{x' = v, v' = -g\}$$

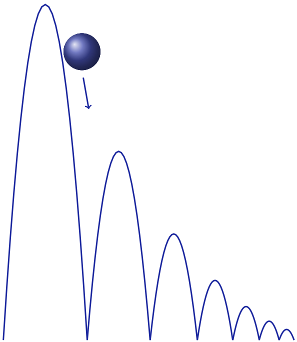
# Ex: The Acrophobic Bouncing Ball



**Example (▶ Bouncing Ball)**

$$\{x' = v, v' = -g \,\&\, x \geq 0\}$$

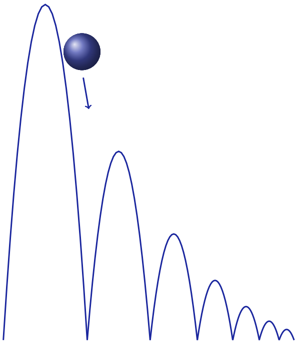
# Ex: The Acrophobic Bouncing Ball



**Example (▸ Bouncing Ball)**

$$\{x' = v, v' = -g \,\&\, x \geq 0\};$$
$$\mathrm{if}(x = 0)\; v := -cv$$

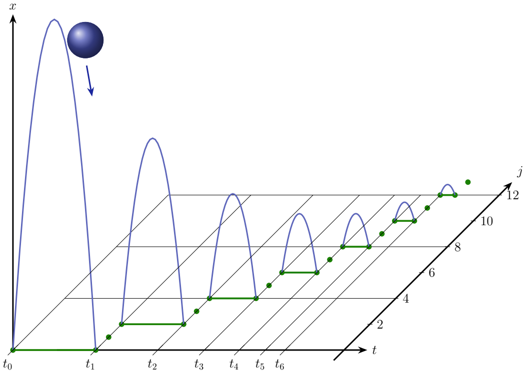
# Ex: The Acrophobic Bouncing Ball



**Example (▸ Bouncing Ball)**

$$\left(\{x' = v, v' = -g \,\&\, x \geq 0\};\right.$$
$$\left.\text{if}(x = 0)\, v := -cv\right)^*$$

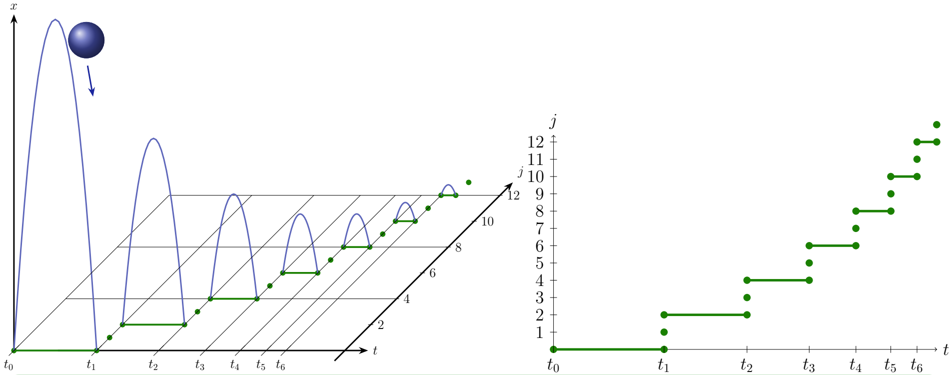
# Ex: The Ball Discovered a Crack in the Fabric of Time



## Example (▸ Bouncing Ball)

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

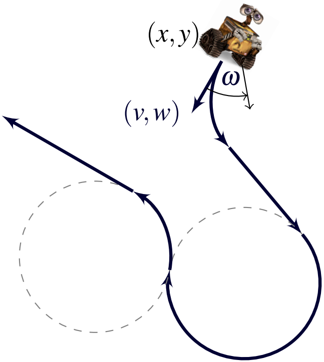
# Ex: The Ball Discovered a Crack in the Fabric of Time



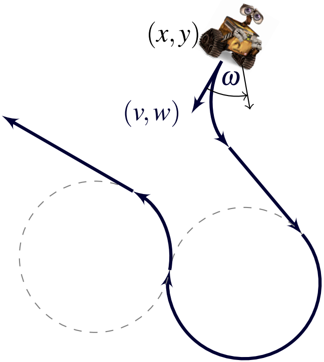
**Example (▸ Bouncing Ball)**

$$x = H \geq 0 \land \ldots \to \left[\left(\{x' = v, v' = -g \,\&\, x \geq 0\};\ \text{if}(x = 0)\, v := -cv\right)^*\right] 0 \leq x \leq H$$

# Ex: Runaround Robot



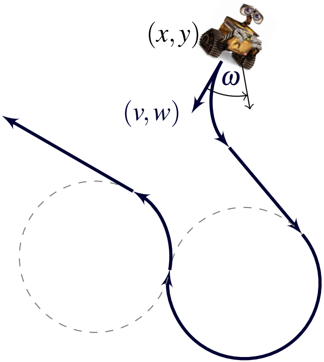
# Ex: Runaround Robot



**Example (Runaround Robot)**

$$\big((\omega := -1 \cup \omega := 1 \cup \omega := 0);$$
$$\{x' = v, y' = w, v' = \omega w, w' = -\omega v\}\big)^*$$

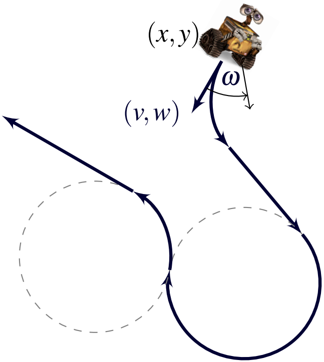
# Ex: Runaround Robot



**Example ( Runaround Robot)**

$$(x,y) \neq o \rightarrow \Big[\Big((\omega := -1 \cup \omega := 1 \cup \omega := 0); \\ \{x' = v, y' = w, v' = \omega w, w' = -\omega v\}\Big)^*\Big]\,(x,y) \neq o$$

# Ex: Runaround Robot



**Example ( Runaround Robot)**

$$(x,y) \neq o \rightarrow \Big[\Big(\big(?Q_{-1};\omega := -1 \cup ?Q_1;\omega := 1 \cup ?Q_0;\omega := 0\big);$$
$$\{x' = v, y' = w, v' = \omega w, w' = -\omega v\}\Big)^*\Big]\,(x,y) \neq o$$

# Ex: Car Control Design

## Example (▶ dL-based model-predictive control design)

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

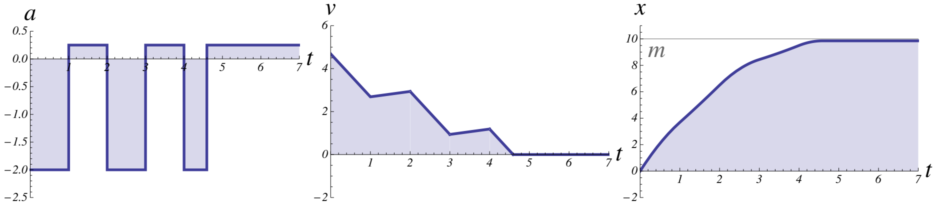
$$[(($$

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

$$a := A)$$

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

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



# Ex: Car Control Design

**Example (▶ dL-based model-predictive control design)**

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

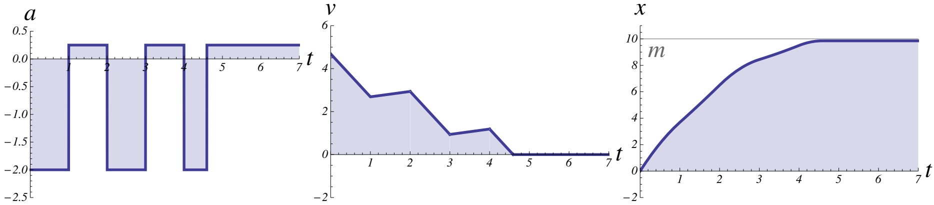
$$\Big[\Big(\Big($$

$$\Big(?\underline{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad};$$

$$a := A\Big)$$

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

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



# Ex: Car Control Design

**Example (▶ dL-based model-predictive control design)**

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

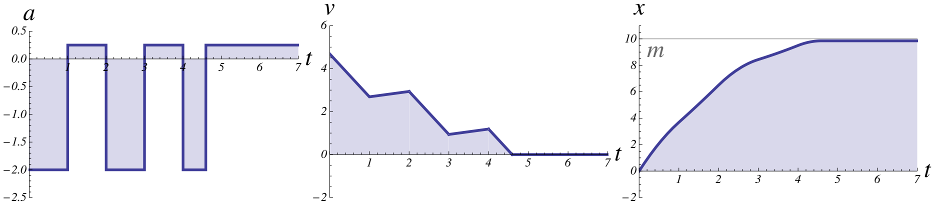
$$[((\,$$

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

$$a:=A)$$

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

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



# Ex: Car Control Design

**Example (▶ dL-based model-predictive control design)**

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

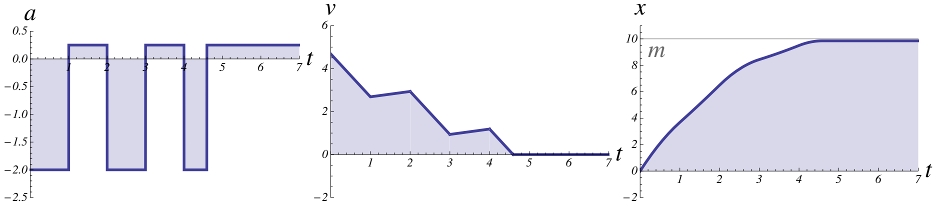
$$\Big[\Big(\Big($$

$$(?\ \underline{\quad {\color{red}???} \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad};$$

$$a:=A)$$

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

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



# Ex: Car Control Design

**Example (▶ dL-based model-predictive control design)**

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

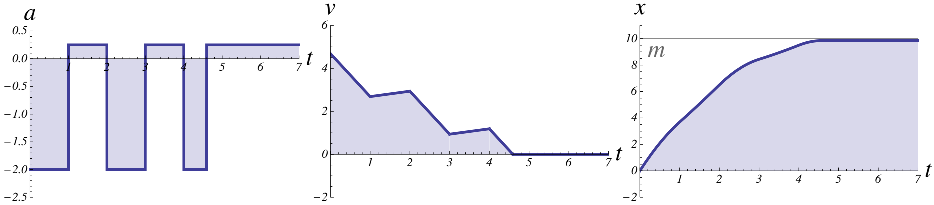
$$\Big[\Big(\Big($$

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

$$a:=A)$$

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

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



# Ex: Car Control Design

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

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

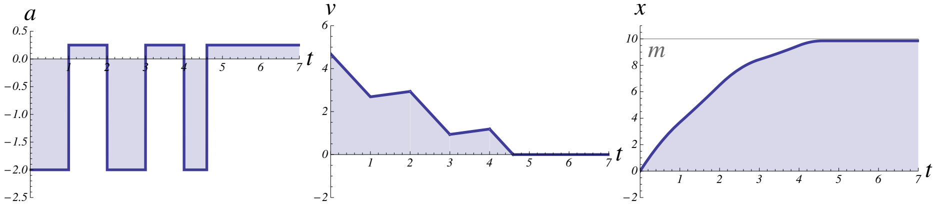
$$\Big[\Big(\Big($$

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

$$a := A)$$

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

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



# Ex: Car Control Design

**Example** (▸ dL-based model-predictive control design)

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

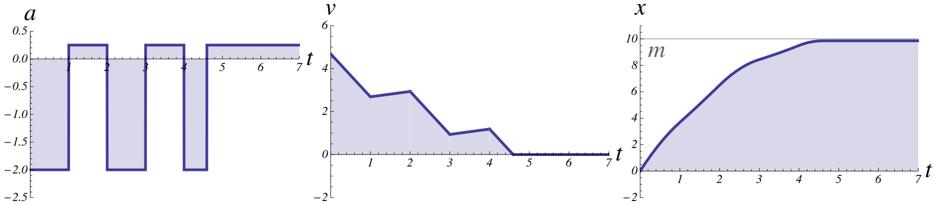
$$\Big[\Big(\Big($$

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

$$a := A)$$

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

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

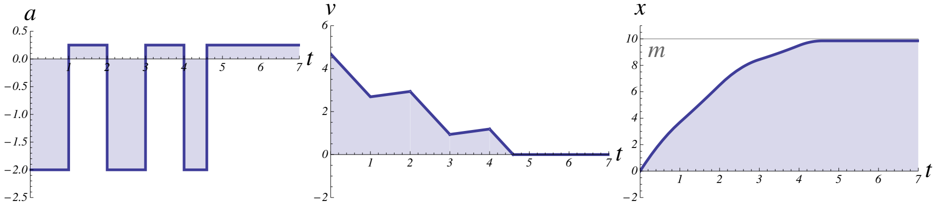


# Ex: Car Control Design

**Example (▶ dL-based model-predictive control design)**

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

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



# Ex: Car Control Design

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

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

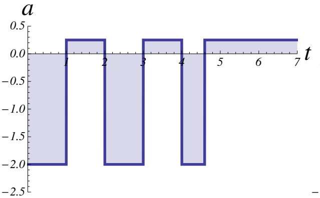
$$\Big[\Big(\Big($$

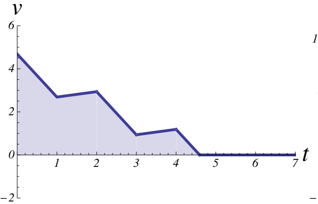
$$\big(?\underline{2b(m-x) \ge v^2 + (A+b)\left(A\varepsilon^2 + 2\varepsilon v\right) \qquad\qquad\qquad};$$

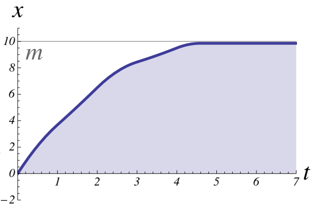
$$a := A)$$

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

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







# Outline (Proving CPS)

1. CPS are Multi-Dynamical Systems
   - Hybrid Systems / Games / Stochastic / Distributed Hybrid Systems
2. Differential Dynamic Logic
   - Syntax
   - Semantics
   - Example: Car Control Design
3. Dynamic Axioms for Dynamical Systems
   - Axiomatics
   - Example: Safe Car Control
   - Soundness and Completeness
4. Differential Invariants for Differential Equations
   - Differential Axioms
   - Example: Differential Ghosts
5. Applications
6. Summary

# Differential Dynamic Logic: Axiomatization

equations of truth

[:=] $[x := e]P(x) \leftrightarrow P(e)$

[?] $[?Q]P \leftrightarrow (Q \rightarrow P)$

['] $[x' = f(x)]P \leftrightarrow \forall t{\geq}0\,[x := y(t)]P$ $\quad (y'(t) = f(y))$

[∪] $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \land [\beta]P$

[;] $[\alpha;\beta]P \leftrightarrow [\alpha][\beta]P$

[*] $[\alpha^*]P \leftrightarrow P \land [\alpha][\alpha^*]P$

K $[\alpha](P \rightarrow Q) \rightarrow ([\alpha]P \rightarrow [\alpha]Q)$

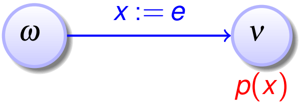
I $[\alpha^*]P \leftrightarrow P \land [\alpha^*](P \rightarrow [\alpha]P)$

C $[\alpha^*]\forall v{>}0\,(P(v) \rightarrow \langle\alpha\rangle P(v{-}1)) \rightarrow \forall v\,(P(v) \rightarrow \langle\alpha^*\rangle\exists v{\leq}0\,P(v))$

LICS'12,JAR'17

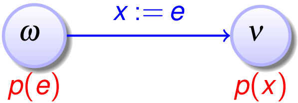
# Dynamic Axioms for Dynamical Systems

$[:=]\ [x := e]p(x) \leftrightarrow$

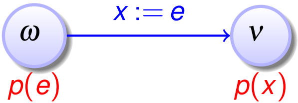


# Dynamic Axioms for Dynamical Systems

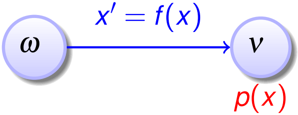
$[:=]\ [x := e]p(x) \leftrightarrow p(e)$



# Dynamic Axioms for Dynamical Systems



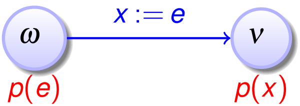
$[:=]$ $[x := e]p(x) \leftrightarrow p(e)$



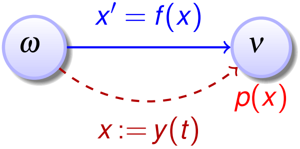
$[']$ $[x' = f(x)]p(x) \leftrightarrow$

# Dynamic Axioms for Dynamical Systems

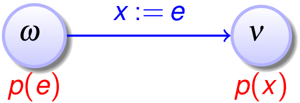
$[:=]\ \ [x := e]p(x) \leftrightarrow p(e)$



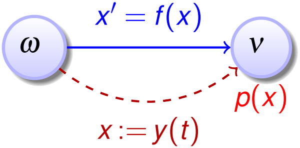
$[']\ \ [x' = f(x)]p(x) \leftrightarrow \qquad [x := y(t)]p(x)$



# Dynamic Axioms for Dynamical Systems

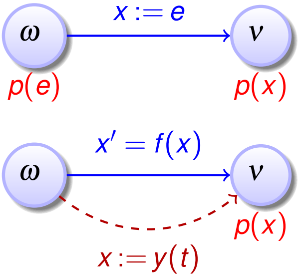


$[:=]$ $[x := e]p(x) \leftrightarrow p(e)$



$[']$ $[x' = f(x)]p(x) \leftrightarrow \forall t{\geq}0\,[x := y(t)]p(x)$

# Dynamic Axioms for Dynamical Systems

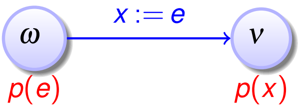


$[:=]$ $[x := e]p(x) \leftrightarrow p(e)$

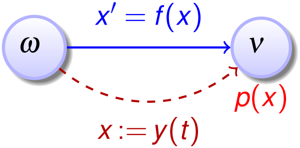
$[']$ $[x' = f(x)]p(x) \leftrightarrow \forall t \geq 0\, [x := y(t)]p(x)$

$[']$ $[x' = f(x) \,\&\, q(x)]p(x) \leftrightarrow \forall t \geq 0 \left([x := y(t)]p(x)\right)$

# Dynamic Axioms for Dynamical Systems



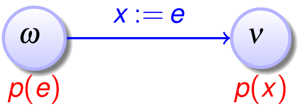
$[:=]\ [x := e]p(x) \leftrightarrow p(e)$



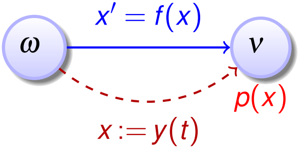
$[']\ [x' = f(x)]p(x) \leftrightarrow \forall t{\geq}0\, [x := y(t)]p(x)$

$[']\ [x' = f(x)\, \&\, q(x)]p(x) \leftrightarrow \forall t{\geq}0\, \big(\forall 0{\leq}s{\leq}t\, q(y(s)) \rightarrow [x := y(t)]p(x)\big)$

# Dynamic Axioms for Dynamical Systems

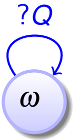


$[:=]$ $[x := e]p(x) \leftrightarrow p(e)$



$['] \ [x' = f(x)]p(x) \leftrightarrow \forall t{\geq}0\, [x := y(t)]p(x)$

$['] \ [x' = f(x)\,\&\, q(x)]p(x) \leftrightarrow \forall t{\geq}0\, \big(\forall 0{\leq}s{\leq}t\, q(y(s)) \rightarrow [x := y(t)]p(x)\big)$

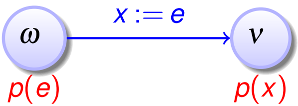


$[?] \ [?Q]P \leftrightarrow$

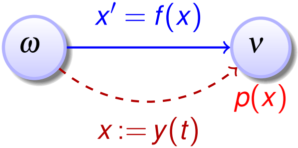
if $\omega \in [\![Q]\!]$

# Dynamic Axioms for Dynamical Systems

$[:=]$ $[x := e]p(x) \leftrightarrow p(e)$

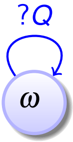


$[']$ $[x' = f(x)]p(x) \leftrightarrow \forall t{\geq}0\, [x := y(t)]p(x)$



$[']$ $[x' = f(x)\,\&\, q(x)]p(x) \leftrightarrow \forall t{\geq}0\, \big(\forall 0{\leq}s{\leq}t\; q(y(s)) \rightarrow [x := y(t)]p(x)\big)$

$[?]$ $[?Q]P \leftrightarrow (Q \rightarrow P)$



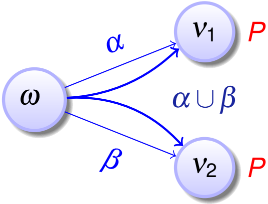
if $\omega \in [\![Q]\!]$

# Dynamic Axioms for Dynamical Systems

compositional semantics $\Rightarrow$ compositional proofs

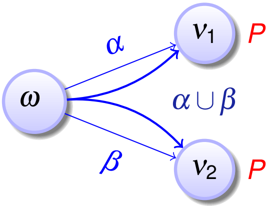
# Dynamic Axioms for Dynamical Systems

$[\cup]\ [\alpha \cup \beta]P \leftrightarrow$



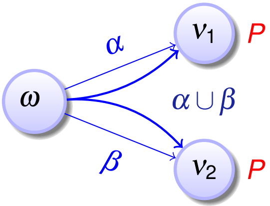
# Dynamic Axioms for Dynamical Systems

$[\cup]$ $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \land [\beta]P$

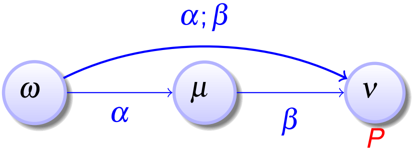


# Dynamic Axioms for Dynamical Systems

[∪] $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \land [\beta]P$

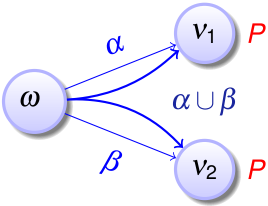


[;] $[\alpha;\beta]P \leftrightarrow$

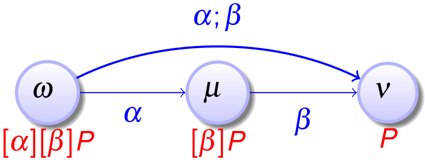


# Dynamic Axioms for Dynamical Systems

$[\cup]$ $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$

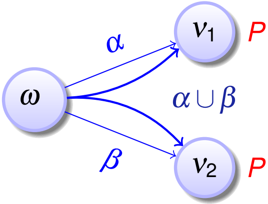


$[;]$ $[\alpha;\beta]P \leftrightarrow [\alpha][\beta]P$

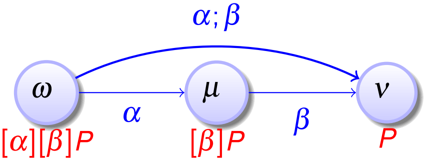


# Dynamic Axioms for Dynamical Systems

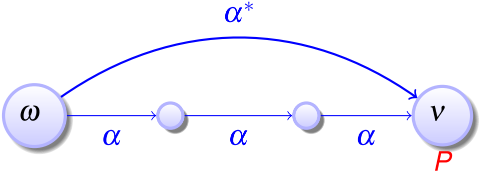
$[\cup]$ $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \land [\beta]P$



$[;]$ $[\alpha;\beta]P \leftrightarrow [\alpha][\beta]P$

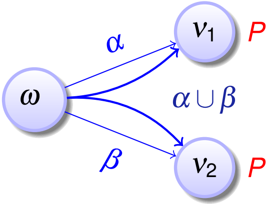


$[^*]$ $[\alpha^*]P \leftrightarrow$

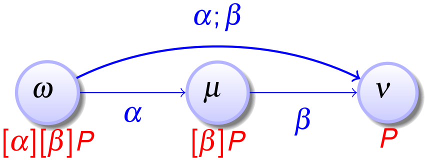


# Dynamic Axioms for Dynamical Systems

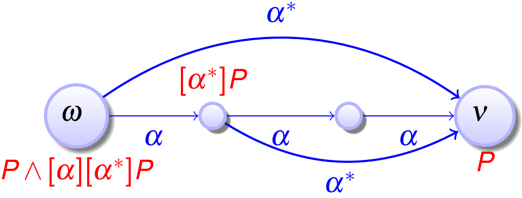
$[\cup]$ $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \land [\beta]P$



$[;]$ $[\alpha;\beta]P \leftrightarrow [\alpha][\beta]P$

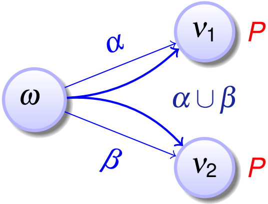


$[^*]$ $[\alpha^*]P \leftrightarrow P \land [\alpha][\alpha^*]P$

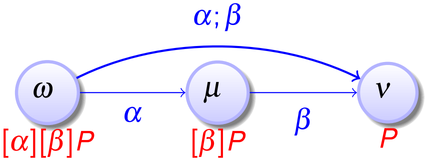


# Dynamic Axioms for Dynamical Systems

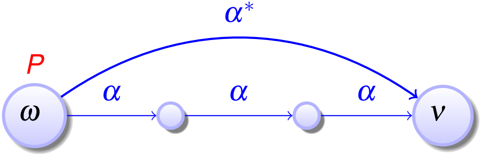
$[\cup]$ $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$



$[;]$ $[\alpha;\beta]P \leftrightarrow [\alpha][\beta]P$

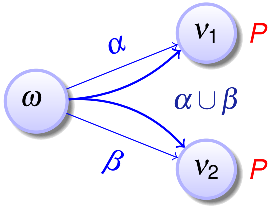


I $[\alpha^*]P \leftrightarrow P \wedge$

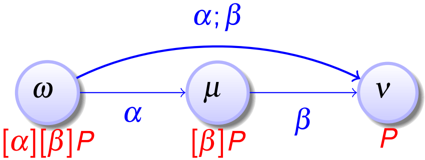


# Dynamic Axioms for Dynamical Systems

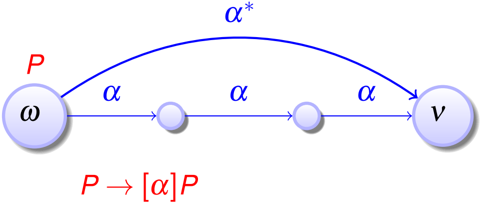
$[\cup]$ $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \land [\beta]P$



$[;]$ $[\alpha;\beta]P \leftrightarrow [\alpha][\beta]P$

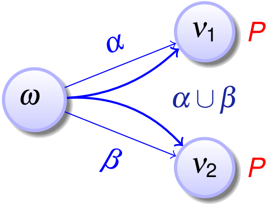


I $[\alpha^*]P \leftrightarrow P \land \qquad (P \rightarrow [\alpha]P)$

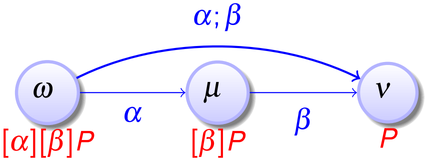


# Dynamic Axioms for Dynamical Systems

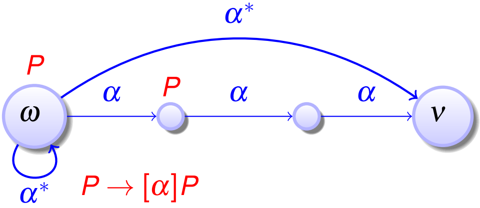
$[\cup]$ $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \land [\beta]P$



$[;]$ $[\alpha;\beta]P \leftrightarrow [\alpha][\beta]P$

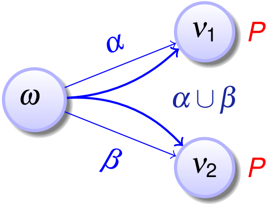


I $[\alpha^*]P \leftrightarrow P \land [\alpha^*](P \to [\alpha]P)$

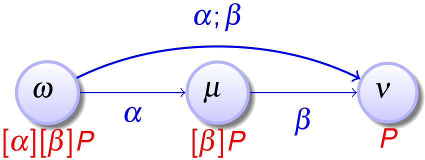


# Dynamic Axioms for Dynamical Systems

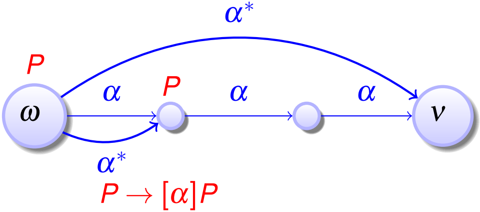
[∪] $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$



[;] $[\alpha;\beta]P \leftrightarrow [\alpha][\beta]P$

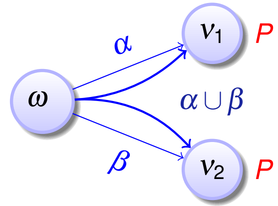


I $[\alpha^*]P \leftrightarrow P \wedge [\alpha^*](P \rightarrow [\alpha]P)$

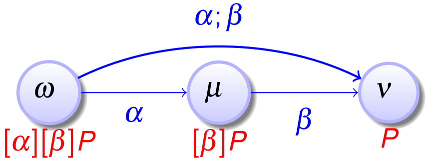


# Dynamic Axioms for Dynamical Systems

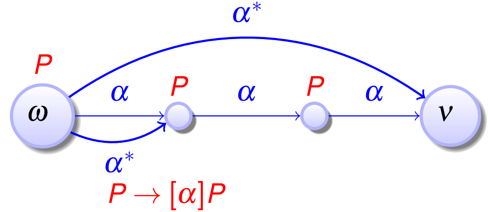
$[\cup]$ $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \land [\beta]P$



$[;]$ $[\alpha;\beta]P \leftrightarrow [\alpha][\beta]P$

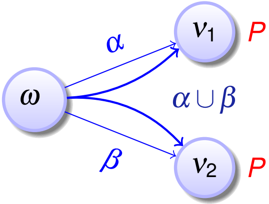


I $[\alpha^*]P \leftrightarrow P \land [\alpha^*](P \to [\alpha]P)$

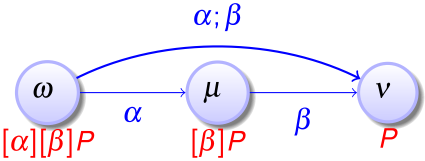


# Dynamic Axioms for Dynamical Systems

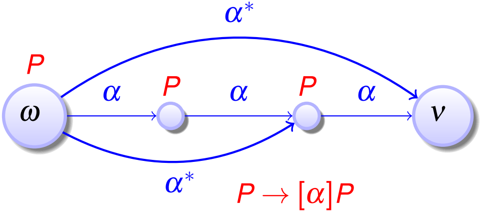
[∪] $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \land [\beta]P$



[;] $[\alpha;\beta]P \leftrightarrow [\alpha][\beta]P$

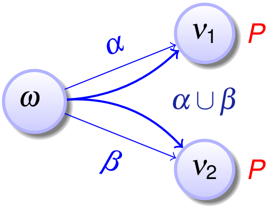


I $[\alpha^*]P \leftrightarrow P \land [\alpha^*](P \rightarrow [\alpha]P)$

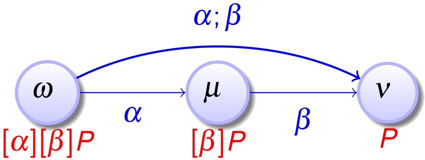


# Dynamic Axioms for Dynamical Systems

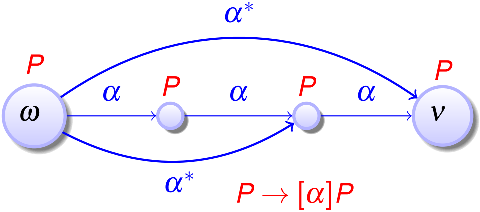
[∪] $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \land [\beta]P$



[;] $[\alpha;\beta]P \leftrightarrow [\alpha][\beta]P$

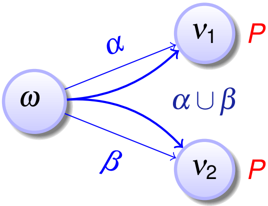


I $[\alpha^*]P \leftrightarrow P \land [\alpha^*](P \rightarrow [\alpha]P)$

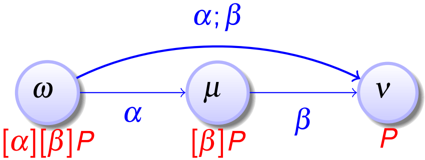


# Dynamic Axioms for Dynamical Systems

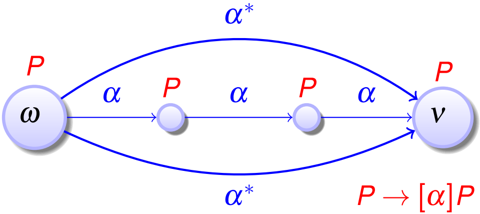
$[\cup]$ $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \land [\beta]P$



$[;]$ $[\alpha;\beta]P \leftrightarrow [\alpha][\beta]P$



I $[\alpha^*]P \leftrightarrow P \land [\alpha^*](P \to [\alpha]P)$

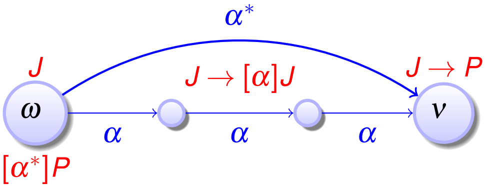


# Proof Rule: Loop Invariants

$$\text{G}\ \frac{P}{[\alpha]P} \qquad \text{I}\ [\alpha^*]P \leftrightarrow P \land [\alpha^*](P \rightarrow [\alpha]P) \qquad \text{M}[\cdot]\ \frac{P \rightarrow Q}{[\alpha]P \rightarrow [\alpha]Q}$$

**Lemma (Loop invariant rule is derived)**

$$\textit{loop}\ \frac{\Gamma \vdash J, \Delta \quad J \vdash [\alpha]J \quad J \vdash P}{\Gamma \vdash [\alpha^*]P, \Delta}$$



# Proof Rule: Loop Invariants

$$\text{G}\ \frac{P}{[\alpha]P} \qquad \text{I}\ [\alpha^*]P \leftrightarrow P \land [\alpha^*](P \to [\alpha]P) \qquad \text{M}[\cdot]\ \frac{P \to Q}{[\alpha]P \to [\alpha]Q}$$

## Lemma (Loop invariant rule is derived)

$$\mathit{loop}\ \frac{\Gamma \vdash J, \Delta \quad J \vdash [\alpha]J \quad J \vdash P}{\Gamma \vdash [\alpha^*]P, \Delta}$$

## Proof (Derived rule).

$$\text{cut}\,\dfrac{\Gamma \vdash J, \Delta \qquad \text{I}\,\dfrac{\text{G}\,\dfrac{J \vdash [\alpha]J}{J \vdash J \land [\alpha^*](J \to [\alpha]J)}}{J \vdash [\alpha^*]J} \qquad \text{M}[\cdot]\,\dfrac{J \vdash P}{[\alpha^*]J \vdash [\alpha^*]P}}{\Gamma \vdash [\alpha^*]P, \Delta}$$

□

# Proof Rule: Loop Invariants

$$\text{G}\ \dfrac{P}{[\alpha]P} \qquad \text{I}\ [\alpha^*]P \leftrightarrow P \land [\alpha^*](P \to [\alpha]P) \qquad \text{M}[\cdot]\ \dfrac{P \to Q}{[\alpha]P \to [\alpha]Q}$$

## Lemma (Loop invariant rule is derived)

$$\mathit{loop}\ \dfrac{\Gamma \vdash J, \Delta \quad J \vdash [\alpha]J \quad J \vdash P}{\Gamma \vdash [\alpha^*]P, \Delta}$$

## Proof (Derived rule).

$$\text{cut}\ \dfrac{\Gamma \vdash J, \Delta \qquad \text{I}\ \dfrac{\text{G}\ \dfrac{J \vdash [\alpha]J}{J \vdash J \land [\alpha^*](J \to [\alpha]J)}}{J \vdash [\alpha^*]J} \qquad \text{M}[\cdot]\ \dfrac{J \vdash P}{[\alpha^*]J \vdash [\alpha^*]P}}{\Gamma \vdash [\alpha^*]P, \Delta}$$

$\square$

Finding invariant $J$ can be a challenge.
Misplaced $[\alpha^*]$ suggests that $J$ needs to carry along info about $\alpha^*$ history.

# Variants & Invariants

The lion's share of understanding comes from understanding what does change (variants/progress measures) and what doesn't change (invariants).

Invariants are a fundamental force of CS

Variants are another fundamental force of CS

# Example Proof: Safe Braking

$J(x,v) \equiv x \leq m$

$$\text{[;]}\ \overline{J(x,v) \vdash [a := -b; (x' = v, v' = a)]J(x,v)}$$

1. $\Gamma \vdash \Delta$ shape of conjecture to prove — sequent
2. $\Gamma$ is list of all available assumptions — antecedent
3. $\Delta$ disjunction needs to be proved from assumptions $\Gamma$ — succedent
4. Proof reduces desired conclusion (at the bottom) to premises with remaining subgoals (top) until no more subgoals ($*$)

# Example Proof: Safe Braking

$J(x,v) \equiv x \le m$

$$\dfrac{\overline{J(x,v) \vdash [a := -b][x' = v, v' = a]J(x,v)}^{\;[:=]}}{J(x,v) \vdash [a := -b; (x' = v, v' = a)]J(x,v)}\;[;]$$

1. $\Gamma \vdash \Delta$ shape of conjecture to prove — sequent
2. $\Gamma$ is list of all available assumptions — antecedent
3. $\Delta$ disjunction needs to be proved from assumptions $\Gamma$ — succedent
4. Proof reduces desired conclusion (at the bottom) to premises with remaining subgoals (top) until no more subgoals ($*$)

# Example Proof: Safe Braking

$J(x,v) \equiv x \leq m$

$$\text{[;]}\;\dfrac{\text{[:=]}\;\dfrac{\text{[$'$]}\;\dfrac{}{J(x,v) \vdash [x'=v, v'={\color{red}-b}]J(x,v)}}{J(x,v) \vdash [{\color{red}a:=-b}][x'=v, v'={\color{red}a}]J(x,v)}}{J(x,v) \vdash [a:=-b; (x'=v, v'=a)]J(x,v)}$$

1. $\Gamma \vdash \Delta$ shape of conjecture to prove — sequent
2. $\Gamma$ is list of all available assumptions — antecedent
3. $\Delta$ disjunction needs to be proved from assumptions $\Gamma$ — succedent
4. Proof reduces desired conclusion (at the bottom) to premises with remaining subgoals (top) until no more subgoals ($*$)

# Example Proof: Safe Braking

$J(x,v) \equiv x \le m$

$$
\begin{array}{rl}
\hline
[:=] & J(x,v) \vdash \forall t{\ge}0\,[x:=-\frac{b}{2}t^2+vt+x]J(x,v) \\
\hline
['] & J(x,v) \vdash [x'=v, v'=-b]J(x,v) \\
\hline
[:=] & J(x,v) \vdash [a:=-b][x'=v, v'=a]J(x,v) \\
\hline
[;] & J(x,v) \vdash [a:=-b;(x'=v, v'=a)]J(x,v)
\end{array}
$$

1. $\Gamma \vdash \Delta$ shape of conjecture to prove sequent
2. $\Gamma$ is list of all available assumptions antecedent
3. $\Delta$ disjunction needs to be proved from assumptions $\Gamma$ succedent
4. Proof reduces desired conclusion (at the bottom) to premises with remaining subgoals (top) until no more subgoals ($*$)

# Example Proof: Safe Braking

$J(x,v) \equiv x \leq m$

$$\begin{array}{rl}
 & \\ \hline
\text{QE} & J(x,v) \vdash \forall t{\geq}0\,(-\frac{b}{2}t^2 + vt + x \leq m) \\ \hline
[:=] & J(x,v) \vdash \forall t{\geq}0\,[x := -\frac{b}{2}t^2 + vt + x]J(x,v) \\ \hline
['] & J(x,v) \vdash [x' = v, v' = -b]J(x,v) \\ \hline
[:=] & J(x,v) \vdash [a := -b][x' = v, v' = a]J(x,v) \\ \hline
[;] & J(x,v) \vdash [a := -b; (x' = v, v' = a)]J(x,v)
\end{array}$$

① $\Gamma \vdash \Delta$ shape of conjecture to prove — sequent

② $\Gamma$ is list of all available assumptions — antecedent

③ $\Delta$ disjunction needs to be proved from assumptions $\Gamma$ — succedent

④ Proof reduces desired conclusion (at the bottom) to premises with remaining subgoals (top) until no more subgoals ($*$)

# Example Proof: Safe Braking

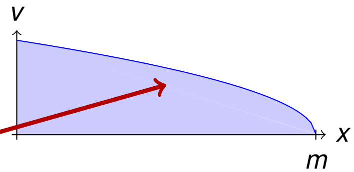
$J(x,v) \equiv x \le m$

$$\begin{array}{rl}
 & J(x,v) \vdash v^2 \le 2b(m-x) \\ \hline
\text{QE} & J(x,v) \vdash \forall t{\ge}0\,(-\frac{b}{2}t^2+vt+x \le m) \\ \hline
[:=] & J(x,v) \vdash \forall t{\ge}0\,[x := -\frac{b}{2}t^2+vt+x]J(x,v) \\ \hline
['] & J(x,v) \vdash [x'=v, v'=-b]J(x,v) \\ \hline
[:=] & J(x,v) \vdash [a:=-b][x'=v, v'=a]J(x,v) \\ \hline
[;] & J(x,v) \vdash [a:=-b; (x'=v, v'=a)]J(x,v)
\end{array}$$

1. $\Gamma \vdash \Delta$ shape of conjecture to prove — sequent
2. $\Gamma$ is list of all available assumptions — antecedent
3. $\Delta$ disjunction needs to be proved from assumptions $\Gamma$ — succedent
4. Proof reduces desired conclusion (at the bottom) to premises with remaining subgoals (top) until no more subgoals ($*$)

# Example Proof: Safe Braking

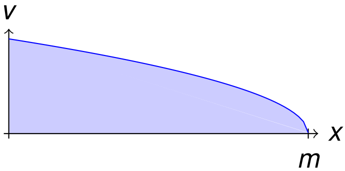
$J(x,v) \equiv v^2 \le 2b(m-x)$



$$\begin{array}{rl}
 & J(x,v) \vdash v^2 \le 2b(m-x) \\ \hline
\text{QE} & J(x,v) \vdash \forall t{\ge}0\, (-\frac{b}{2}t^2 + vt + x \le m) \\ \hline
[:=] & J(x,v) \vdash \forall t{\ge}0\, [x := -\frac{b}{2}t^2 + vt + x] J(x,v) \\ \hline
['] & J(x,v) \vdash [x' = v, v' = -b] J(x,v) \\ \hline
[:=] & J(x,v) \vdash [a := -b][x' = v, v' = a] J(x,v) \\ \hline
[;] & J(x,v) \vdash [a := -b; (x' = v, v' = a)] J(x,v)
\end{array}$$

# Example Proof: Safe Acceleration

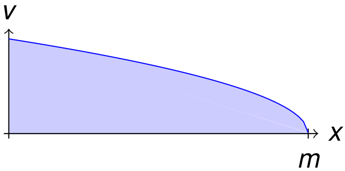
$J(x,v) \equiv v^2 \le 2b(m-x)$



$$\text{[;]}\ \frac{}{J(x,v) \vdash [?\neg \mathrm{SB}; a := A; (x' = v, v' = a, t' = 1 \,\&\, t \le \varepsilon)]J(x,v)}$$

# Example Proof: Safe Acceleration

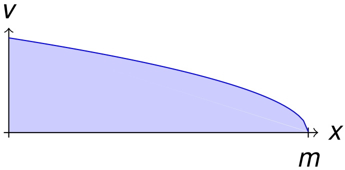
$J(x,v) \equiv v^2 \leq 2b(m-x)$



$$\dfrac{\dfrac{}{J(x,v) \vdash [?\neg \mathrm{SB}][a := A;(x'=v,v'=a,t'=1\,\&\,t \leq \varepsilon)]J(x,v)}[?]}{J(x,v) \vdash [?\neg \mathrm{SB}; a := A;(x'=v,v'=a,t'=1\,\&\,t \leq \varepsilon)]J(x,v)}[;]$$

# Example Proof: Safe Acceleration

$J(x,v) \equiv v^2 \leq 2b(m-x)$

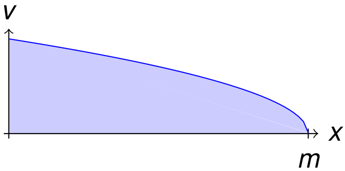


$$\dfrac{\dfrac{\dfrac{}{J(x,v) \vdash \neg\text{SB} \rightarrow [a:=A;(x'=v,v'=a,t'=1\,\&\,t\leq\varepsilon)]J(x,v)}}{J(x,v) \vdash [?\neg\text{SB}][a:=A;(x'=v,v'=a,t'=1\,\&\,t\leq\varepsilon)]J(x,v)}\;[?]}{J(x,v) \vdash [?\neg\text{SB};a:=A;(x'=v,v'=a,t'=1\,\&\,t\leq\varepsilon)]J(x,v)}\;[;]$$

[;]

# Example Proof: Safe Acceleration

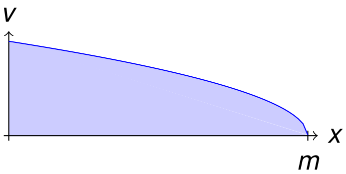
$J(x,v) \equiv v^2 \le 2b(m-x)$



$$\dfrac{\dfrac{\dfrac{\dfrac{}{J(x,v) \vdash \neg SB \to [a:=A][x'=v,v'=a,t'=1\,\&\,t\le\varepsilon]J(x,v)}{\scriptstyle[:=]}}{J(x,v) \vdash \neg SB \to [{\color{red}a:=A;(x'=v,v'=a,t'=1\,\&\,t\le\varepsilon)}]J(x,v)}{\scriptstyle[;]}}{J(x,v) \vdash [?\neg SB][a:=A;(x'=v,v'=a,t'=1\,\&\,t\le\varepsilon)]J(x,v)}{\scriptstyle[?]}}{J(x,v) \vdash [?\neg SB;a:=A;(x'=v,v'=a,t'=1\,\&\,t\le\varepsilon)]J(x,v)}{\scriptstyle[;]}$$

# Example Proof: Safe Acceleration

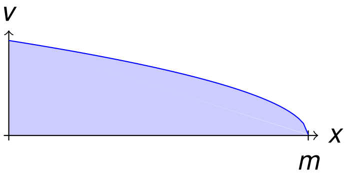
$$J(x,v) \equiv v^2 \leq 2b(m-x)$$



$$\begin{array}{rl}
 & \\ \hline
['] & J(x,v) \vdash \neg SB \rightarrow [x'=v, v'=A, t'=1 \,\&\, t \leq \varepsilon]J(x,v) \\ \hline
[:=] & J(x,v) \vdash \neg SB \rightarrow [a:=A][x'=v, v'=a, t'=1 \,\&\, t \leq \varepsilon]J(x,v) \\ \hline
[;] & J(x,v) \vdash \neg SB \rightarrow [a:=A;(x'=v, v'=a, t'=1 \,\&\, t \leq \varepsilon)]J(x,v) \\ \hline
[?] & J(x,v) \vdash [?\neg SB][a:=A;(x'=v, v'=a, t'=1 \,\&\, t \leq \varepsilon)]J(x,v) \\ \hline
[;] & J(x,v) \vdash [?\neg SB; a:=A;(x'=v, v'=a, t'=1 \,\&\, t \leq \varepsilon)]J(x,v)
\end{array}$$

# Example Proof: Safe Acceleration

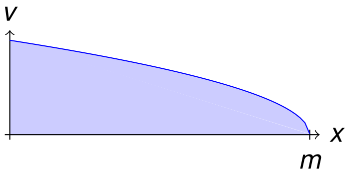
$J(x,v) \equiv v^2 \leq 2b(m-x)$



$$\begin{array}{rl}
\hline
[:=] & J(x,v) \vdash \neg SB \to \forall t{\geq}0\,(t \leq \varepsilon \to [x := \frac{A}{2}t^2 + vt + x]J(x,v)) \\
\hline
['] & J(x,v) \vdash \neg SB \to [x' = v, v' = A, t' = 1\,\&\,t \leq \varepsilon]J(x,v) \\
\hline
[:=] & J(x,v) \vdash \neg SB \to [a := A][x' = v, v' = a, t' = 1\,\&\,t \leq \varepsilon]J(x,v) \\
\hline
[;] & J(x,v) \vdash \neg SB \to [a := A; (x' = v, v' = a, t' = 1\,\&\,t \leq \varepsilon)]J(x,v) \\
\hline
[?] & J(x,v) \vdash [?\neg SB][a := A; (x' = v, v' = a, t' = 1\,\&\,t \leq \varepsilon)]J(x,v) \\
\hline
[;] & J(x,v) \vdash [?\neg SB; a := A; (x' = v, v' = a, t' = 1\,\&\,t \leq \varepsilon)]J(x,v)
\end{array}$$

# Example Proof: Safe Acceleration

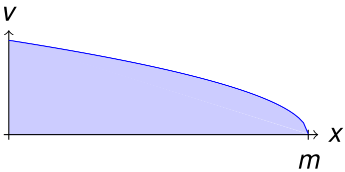
$J(x,v) \equiv v^2 \leq 2b(m-x)$



$$
\begin{array}{ll}
\hline
 & J(x,v) \vdash \neg SB \rightarrow \forall t{\geq}0\,(t \leq \varepsilon \rightarrow J(\frac{A}{2}t^2+vt+x, At+v)) \\
\hline
[:=] & J(x,v) \vdash \neg SB \rightarrow \forall t{\geq}0\,(t \leq \varepsilon \rightarrow [x := \frac{A}{2}t^2+vt+x]J(x,v)) \\
\hline
['] & J(x,v) \vdash \neg SB \rightarrow [x'=v, v'=A, t'=1\,\&\,t \leq \varepsilon]J(x,v) \\
\hline
[:=] & J(x,v) \vdash \neg SB \rightarrow [a:=A][x'=v, v'=a, t'=1\,\&\,t \leq \varepsilon]J(x,v) \\
\hline
[;] & J(x,v) \vdash \neg SB \rightarrow [a:=A; (x'=v, v'=a, t'=1\,\&\,t \leq \varepsilon)]J(x,v) \\
\hline
[?] & J(x,v) \vdash [?\neg SB][a:=A; (x'=v, v'=a, t'=1\,\&\,t \leq \varepsilon)]J(x,v) \\
\hline
[;] & J(x,v) \vdash [?\neg SB; a:=A; (x'=v, v'=a, t'=1\,\&\,t \leq \varepsilon)]J(x,v)
\end{array}
$$

# Example Proof: Safe Acceleration

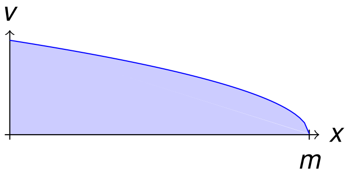
$J(x,v) \equiv v^2 \leq 2b(m-x)$



$$\begin{array}{ll}
\text{QE} & \\ \hline
 & J(x,v) \vdash \neg \mathrm{SB} \to \forall t{\geq}0\,(t \leq \varepsilon \to (At+v)^2 \leq 2b(m-\frac{A}{2}t^2-vt-x)) \\ \hline
 & J(x,v) \vdash \neg \mathrm{SB} \to \forall t{\geq}0\,(t \leq \varepsilon \to J(\frac{A}{2}t^2+vt+x, At+v)) \\ \hline
[:=] & J(x,v) \vdash \neg \mathrm{SB} \to \forall t{\geq}0\,(t \leq \varepsilon \to [x := \frac{A}{2}t^2+vt+x]J(x,v)) \\ \hline
['] & J(x,v) \vdash \neg \mathrm{SB} \to [x'=v, v'=A, t'=1\,\&\,t \leq \varepsilon]J(x,v) \\ \hline
[:=] & J(x,v) \vdash \neg \mathrm{SB} \to [a:=A][x'=v, v'=a, t'=1\,\&\,t \leq \varepsilon]J(x,v) \\ \hline
[;] & J(x,v) \vdash \neg \mathrm{SB} \to [a:=A;(x'=v, v'=a, t'=1\,\&\,t \leq \varepsilon)]J(x,v) \\ \hline
[?] & J(x,v) \vdash [?\neg \mathrm{SB}][a:=A;(x'=v, v'=a, t'=1\,\&\,t \leq \varepsilon)]J(x,v) \\ \hline
[;] & J(x,v) \vdash [?\neg \mathrm{SB}; a:=A;(x'=v, v'=a, t'=1\,\&\,t \leq \varepsilon)]J(x,v)
\end{array}$$

# Example Proof: Safe Acceleration

$$J(x,v) \equiv v^2 \le 2b(m-x)$$

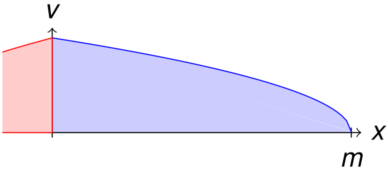


$$
\begin{array}{rl}
 & J(x,v) \vdash \neg\mathrm{SB} \to (A\varepsilon+v)^2 \le 2b(m-\frac{A}{2}\varepsilon^2 - v\varepsilon - x) \\ \hline
\text{QE} & J(x,v) \vdash \neg\mathrm{SB} \to \forall t{\ge}0\,(t \le \varepsilon \to (At+v)^2 \le 2b(m-\frac{A}{2}t^2 - vt - x)) \\ \hline
 & J(x,v) \vdash \neg\mathrm{SB} \to \forall t{\ge}0\,(t \le \varepsilon \to J(\frac{A}{2}t^2+vt+x, At+v)) \\ \hline
[:=] & J(x,v) \vdash \neg\mathrm{SB} \to \forall t{\ge}0\,(t \le \varepsilon \to [x := \frac{A}{2}t^2+vt+x]J(x,v)) \\ \hline
['] & J(x,v) \vdash \neg\mathrm{SB} \to [x' = v, v' = A, t' = 1 \,\&\, t \le \varepsilon]J(x,v) \\ \hline
[:=] & J(x,v) \vdash \neg\mathrm{SB} \to [a := A][x' = v, v' = a, t' = 1 \,\&\, t \le \varepsilon]J(x,v) \\ \hline
[;] & J(x,v) \vdash \neg\mathrm{SB} \to [a := A; (x' = v, v' = a, t' = 1 \,\&\, t \le \varepsilon)]J(x,v) \\ \hline
[?] & J(x,v) \vdash [?\neg\mathrm{SB}][a := A; (x' = v, v' = a, t' = 1 \,\&\, t \le \varepsilon)]J(x,v) \\ \hline
[;] & J(x,v) \vdash [?\neg\mathrm{SB}; a := A; (x' = v, v' = a, t' = 1 \,\&\, t \le \varepsilon)]J(x,v)
\end{array}
$$

# Example Proof: Safe Acceleration

$$J(x,v) \equiv v^2 \le 2b(m-x)$$

$$\mathrm{SB} \equiv 2b(m-x) < v^2 + (A+b)(A\varepsilon^2 + 2\varepsilon v)$$

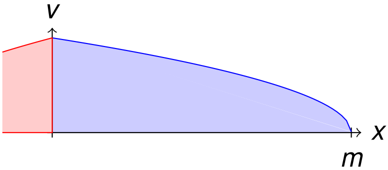


$$\begin{array}{rl}
 & J(x,v) \vdash \neg \mathrm{SB} \to (A\varepsilon+v)^2 \le 2b(m - \frac{A}{2}\varepsilon^2 - v\varepsilon - x) \\ \hline
\text{QE} & J(x,v) \vdash \neg \mathrm{SB} \to \forall t{\ge}0\, (t \le \varepsilon \to (At+v)^2 \le 2b(m - \frac{A}{2}t^2 - vt - x)) \\ \hline
 & J(x,v) \vdash \neg \mathrm{SB} \to \forall t{\ge}0\, (t \le \varepsilon \to J(\frac{A}{2}t^2 + vt + x, At + v)) \\ \hline
[:=] & J(x,v) \vdash \neg \mathrm{SB} \to \forall t{\ge}0\, (t \le \varepsilon \to [x := \frac{A}{2}t^2 + vt + x]J(x,v)) \\ \hline
['] & J(x,v) \vdash \neg \mathrm{SB} \to [x' = v, v' = A, t' = 1 \,\&\, t \le \varepsilon]J(x,v) \\ \hline
[:=] & J(x,v) \vdash \neg \mathrm{SB} \to [a := A][x' = v, v' = a, t' = 1 \,\&\, t \le \varepsilon]J(x,v) \\ \hline
[;] & J(x,v) \vdash \neg \mathrm{SB} \to [a := A; (x' = v, v' = a, t' = 1 \,\&\, t \le \varepsilon)]J(x,v) \\ \hline
[?] & J(x,v) \vdash [?\neg \mathrm{SB}][a := A; (x' = v, v' = a, t' = 1 \,\&\, t \le \varepsilon)]J(x,v) \\ \hline
[;] & J(x,v) \vdash [?\neg \mathrm{SB}; a := A; (x' = v, v' = a, t' = 1 \,\&\, t \le \varepsilon)]J(x,v)
\end{array}$$

# Example Proof: Safe Driving

$J(x,v) \equiv v^2 \leq 2b(m-x)$

$\mathrm{SB} \equiv 2b(m-x) < v^2 + (A+b)(A\varepsilon^2 + 2\varepsilon v)$

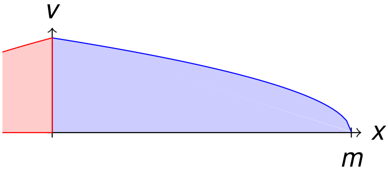


$$\text{loop}\,\overline{J(x,v) \vdash [\big((a:=-b \cup ?\neg \mathrm{SB}; a:=A); x''=a, t'=1 \,\&\, t \leq \varepsilon\big)^*]J(x,v)}$$

# Example Proof: Safe Driving

$J(x,v) \equiv v^2 \leq 2b(m-x)$

$\mathrm{SB} \equiv 2b(m-x) < v^2 + (A+b)(A\varepsilon^2 + 2\varepsilon v)$

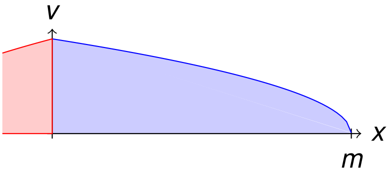


$$\dfrac{\dfrac{}{J(x,v) \vdash [(a := -b \cup ?\neg\mathrm{SB}; a := A); x'' = a, t' = 1 \,\&\, t \leq \varepsilon]J(x,v)}[;]}{J(x,v) \vdash [\big((a := -b \cup ?\neg\mathrm{SB}; a := A); x'' = a, t' = 1 \,\&\, t \leq \varepsilon\big)^*]J(x,v)}\text{loop}$$

# Example Proof: Safe Driving

$J(x,v) \equiv v^2 \le 2b(m-x)$

$\mathrm{SB} \equiv 2b(m-x) < v^2 + (A+b)(A\varepsilon^2 + 2\varepsilon v)$

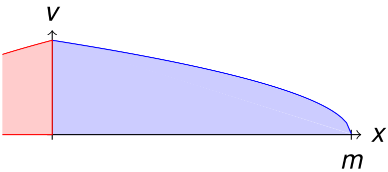


$$\dfrac{\dfrac{\dfrac{}{J(x,v) \vdash [a:=-b \cup ?\neg \mathrm{SB}; a:=A][x''=a, t'=1 \,\&\, t \le \varepsilon]J(x,v)}[\cup]}{J(x,v) \vdash [(a:=-b \cup ?\neg \mathrm{SB}; a:=A); x''=a, t'=1 \,\&\, t \le \varepsilon]J(x,v)}[;]}{J(x,v) \vdash [\big((a:=-b \cup ?\neg \mathrm{SB}; a:=A); x''=a, t'=1 \,\&\, t \le \varepsilon\big)^*]J(x,v)}\text{loop}$$

# Example Proof: Safe Driving

$J(x,v) \equiv v^2 \leq 2b(m-x)$

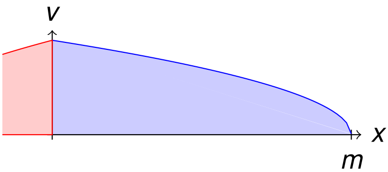
$\mathrm{SB} \equiv 2b(m-x) < v^2 + (A+b)(A\varepsilon^2 + 2\varepsilon v)$



$$\text{loop}\;\dfrac{[;]\;\dfrac{[\cup]\;\dfrac{\overline{J(x,v) \vdash [a:=-b][x''=a..]J(x,v) \land [?\neg\mathrm{SB};a:=A][x''=a..]J(x,v)}}{J(x,v) \vdash [a:=-b \cup ?\neg\mathrm{SB};a:=A][x''=a,t'=1\,\&\,t\leq\varepsilon]J(x,v)}}{J(x,v) \vdash [(a:=-b \cup ?\neg\mathrm{SB};a:=A);x''=a,t'=1\,\&\,t\leq\varepsilon]J(x,v)}}{J(x,v) \vdash [\big((a:=-b \cup ?\neg\mathrm{SB};a:=A);x''=a,t'=1\,\&\,t\leq\varepsilon\big)^*]J(x,v)}$$

# Example Proof: Safe Driving

$$J(x,v) \equiv v^2 \leq 2b(m-x)$$
$$\mathrm{SB} \equiv 2b(m-x) < v^2 + (A+b)(A\varepsilon^2 + 2\varepsilon v)$$

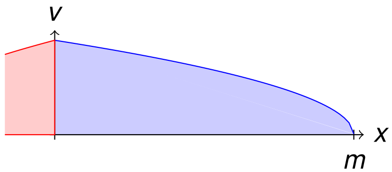


$$\begin{array}{ll}
\hline
\mathbb{R} & \text{previous proofs for braking and acceleration}\\
\hline
 & J(x,v) \vdash [a:=-b][x''=a..]J(x,v) \land [?\neg\mathrm{SB}; a:=A][x''=a..]J(x,v)\\
\hline
[\cup] & J(x,v) \vdash [a:=-b \cup ?\neg\mathrm{SB}; a:=A][x''=a, t'=1 \,\&\, t\leq\varepsilon]J(x,v)\\
\hline
[;] & J(x,v) \vdash [(a:=-b \cup ?\neg\mathrm{SB}; a:=A); x''=a, t'=1 \,\&\, t\leq\varepsilon]J(x,v)\\
\hline
\text{loop} & J(x,v) \vdash [\big((a:=-b \cup ?\neg\mathrm{SB}; a:=A); x''=a, t'=1 \,\&\, t\leq\varepsilon\big)^*]J(x,v)
\end{array}$$

# Example Proof: Safe Driving

$J(x,v) \equiv v^2 \leq 2b(m-x)$

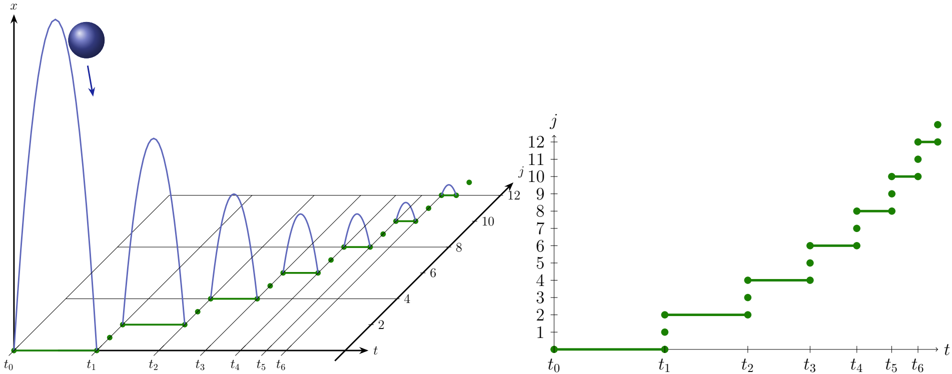
$\mathrm{SB} \equiv 2b(m-x) < v^2 + (A+b)(A\varepsilon^2 + 2\varepsilon v)$



$$
\text{loop}\,\dfrac{[;]\,\dfrac{[\cup]\,\dfrac{\dfrac{\mathbb{R}\,\dfrac{*}{\text{previous proofs for braking and acceleration}}}{J(x,v) \vdash [a:=-b][x''=a..]J(x,v) \land [?\neg \mathrm{SB}; a:=A][x''=a..]J(x,v)}}{J(x,v) \vdash [a:=-b \cup ?\neg \mathrm{SB}; a:=A][x''=a, t'=1 \,\&\, t\leq\varepsilon]J(x,v)}}{J(x,v)\vdash [(a:=-b\cup ?\neg \mathrm{SB}; a:=A); x''=a, t'=1\,\&\, t\leq\varepsilon]J(x,v)}}{J(x,v)\vdash\big[\big((a:=-b\cup?\neg \mathrm{SB};a:=A);x''=a,t'=1\,\&\,t\leq\varepsilon\big)^*\big]J(x,v)}
$$

1. Proof is deterministic “follow your nose”.
2. Synthesize invariant $J(x,v)$ and parameter constraint SB.
3. $J(x,v)$ is a predicate symbol to prove only once and instantiate later.
4. First looking at proofs of smaller pieces is often effective.

# Ex: The Ball Discovered a Crack in the Fabric of Time

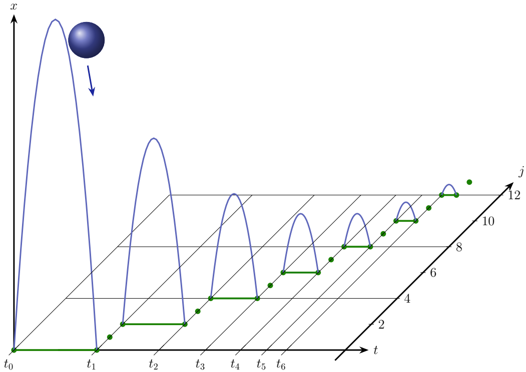


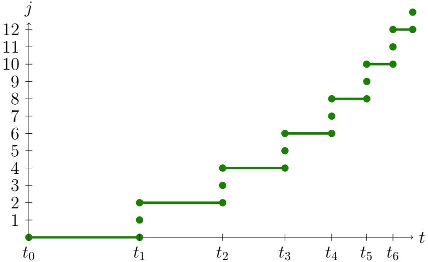
**Example (▸ Bouncing Ball)**

$$x=H\geq 0 \land \ldots \rightarrow \Big[\big(\{x'=v, v'=-g \,\&\, x\geq 0\};$$

$$\text{if}(x=0)\, v:=-cv\big)^*\Big]\, 0\leq x\leq H$$

# Ex: The Ball Discovered a Crack in the Fabric of Time

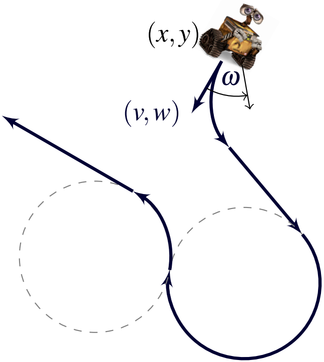




**Example** (▸ Bouncing Ball if $g > 0 \land 1 \geq c \geq 0 \land v = 0$)

$$x{=}H{\geq}0 \land \ldots \rightarrow \Big[\big(\{x' = v, v' = -g \,\&\, x \geq 0\}; \\ \text{if}(x = 0)\, v := -cv\big)^*\Big]\, 0{\leq}x{\leq}H$$

# Ex: Runaround Robot



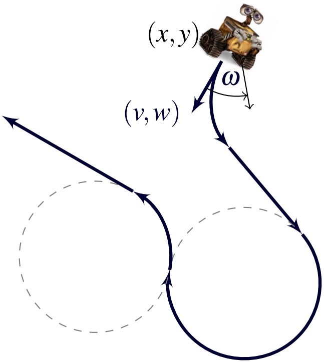
**Example (Runaround Robot)**

$$(x,y) \neq o \rightarrow \Big[\Big(\big(?Q_{-1}; \omega := -1 \cup ?Q_1; \omega := 1 \cup ?Q_0; \omega := 0\big);$$
$$\{x' = v, y' = w, v' = \omega w, w' = -\omega v\}\Big)^*\Big]\,(x,y) \neq o$$

# Ex: Runaround Robot

$$Q_\omega \equiv \left(x+\frac{w}{\omega}-o_x\right)^2+\left(y-\frac{v}{\omega}-o_y\right)^2 \neq v^2+w^2$$

$$Q_0 \equiv (o_x-x)w \neq (o_y-y)v$$



1. Obstacle not on tangential circle
2. Obstacle not on ray $(x,y)+\mathbb{R}(v,w)$

**Example (▶ Runaround Robot)**

$$(x,y)\neq o \to \Big[\Big(\big(?Q_{-1};\omega:=-1 \cup ?Q_1;\omega:=1 \cup ?Q_0;\omega:=0\big);\ \{x'=v,y'=w,v'=\omega w,w'=-\omega v\}\Big)^*\Big](x,y)\neq o$$

# Complete Proof Theory of Hybrid Systems

**Theorem (Sound & Complete)** (JAR’08, LICS’12, JAR’17)

dL *calculus is a sound & complete axiomatization of hybrid systems relative to either differential equations* ***or*** *to discrete dynamics.*

**Corollary (Complete Proof-theoretical Bridge)**

proving continuous = proving hybrid = proving discrete

$$\vDash P \text{ iff } \mathrm{FODE} \vdash_{\mathrm{dL}} P$$

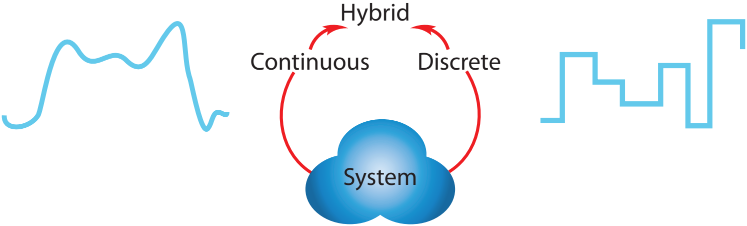
# Complete Proof Theory of Hybrid Systems

**Theorem (Sound & Complete)** (JAR'08, LICS'12, JAR'17)

dL *calculus is a sound & complete axiomatization of hybrid systems relative to either differential equations* ***or*** *to discrete dynamics.*

**Corollary (Complete Proof-theoretical Bridge)**

proving continuous = proving hybrid = proving discrete



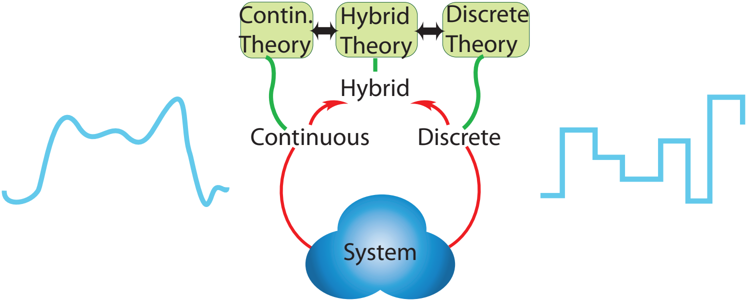
# Complete Proof Theory of Hybrid Systems

**Theorem (Sound & Complete)** (JAR'08, LICS'12, JAR'17)

dL *calculus is a sound & complete axiomatization of hybrid systems relative to either differential equations* ***or*** *to discrete dynamics.*

**Corollary (Complete Proof-theoretical Bridge)**

proving continuous = proving hybrid = proving discrete



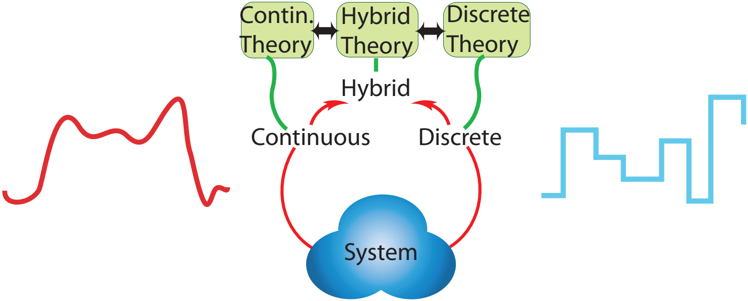
# Complete Proof Theory of Hybrid Systems

**Theorem (Sound & Complete)** (JAR'08, LICS'12, JAR'17)

dL *calculus is a sound & complete axiomatization of hybrid systems relative to either differential equations* ***or*** *to discrete dynamics.*

**Corollary (Complete Proof-theoretical Bridge)**

proving continuous = proving hybrid = proving discrete



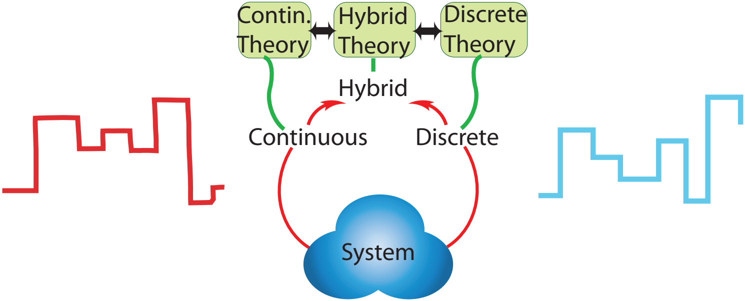
# Complete Proof Theory of Hybrid Systems

**Theorem (Sound & Complete)** (JAR'08, LICS'12, JAR'17)

dL *calculus is a sound & complete axiomatization of hybrid systems relative to either differential equations* ***or*** *to discrete dynamics.*

**Corollary (Complete Proof-theoretical Bridge)**

proving continuous = proving hybrid = proving discrete



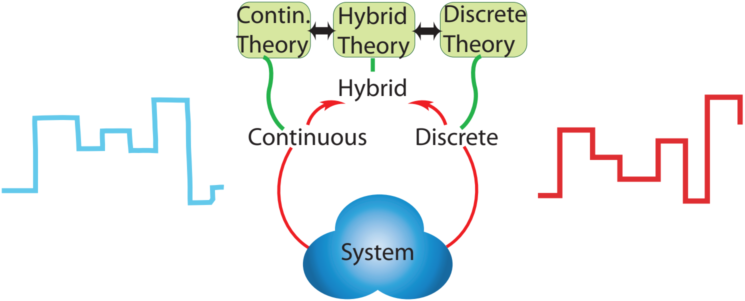
# Complete Proof Theory of Hybrid Systems

**Theorem (Sound & Complete)** (JAR'08, LICS'12, JAR'17)

dL *calculus is a sound & complete axiomatization of hybrid systems relative to either differential equations* ***or*** *to discrete dynamics.*

**Corollary (Complete Proof-theoretical Bridge)**

proving continuous = proving hybrid = proving discrete



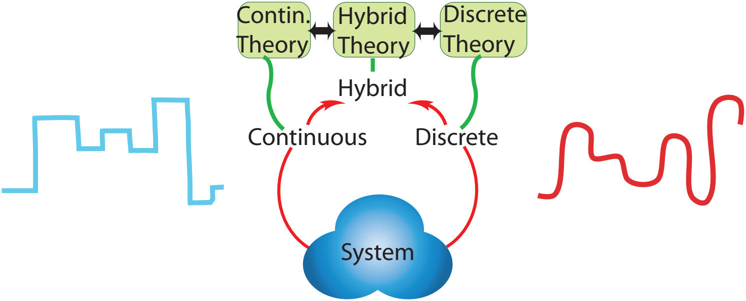
# Complete Proof Theory of Hybrid Systems

**Theorem (Sound & Complete)** (JAR'08, LICS'12, JAR'17)

dL *calculus is a sound & complete axiomatization of hybrid systems relative to either differential equations* ***or*** *to discrete dynamics.*

**Corollary (Complete Proof-theoretical Bridge)**

proving continuous = proving hybrid = proving discrete



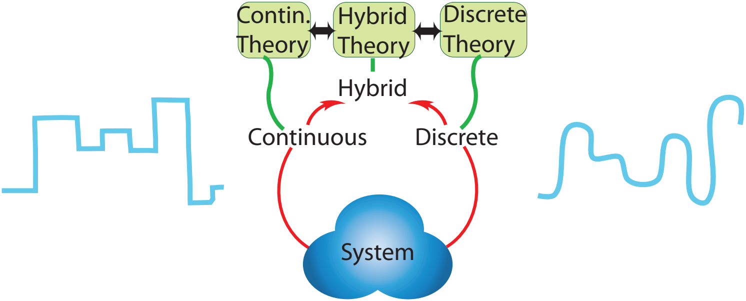
# Complete Proof Theory of Hybrid Systems

**Theorem (Sound & Complete)** (JAR'08, LICS'12, JAR'17)

dL *calculus is a sound & complete axiomatization of hybrid systems relative to either differential equations* ***or*** *to discrete dynamics.*

**Corollary (Complete Proof-theoretical Bridge)**

proving continuous = proving hybrid = proving discrete



# Complete Proof Theory of Hybrid Systems

**Theorem (Sound & Complete)** (JAR'08, LICS'12, JAR'17)

dL *calculus is a sound & complete axiomatization of hybrid systems relative to either differential equations* ***or*** *to discrete dynamics.*

**Corollary (Complete Proof-theoretical Bridge)**

proving continuous = proving hybrid = proving discrete

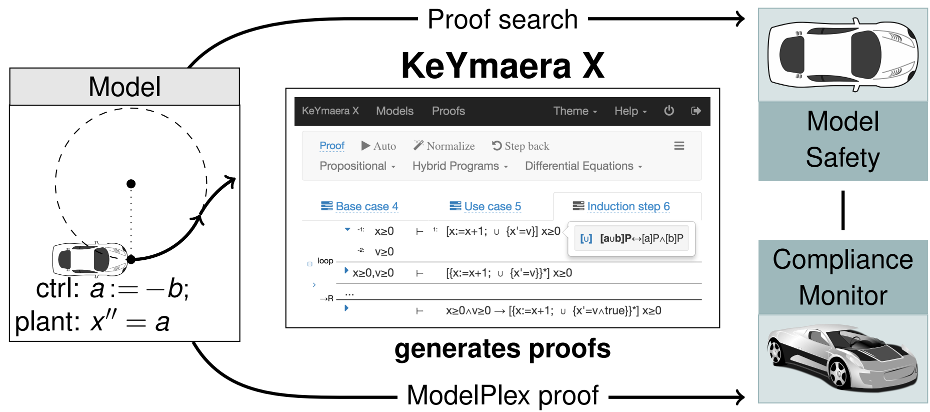
**Theorem (Equi-expressibility)** (LICS'12)

$$\forall P \in \mathrm{dL}\ \exists P^\flat \in FODE\ \vDash P \leftrightarrow P^\flat$$
$$\forall P \in \mathrm{dL}\ \exists P^\# \in DL\quad \vDash P \leftrightarrow P^\#$$

**Theorem (Relative Decidability)** (LICS'12)

*Validity of* dL *sentences is decidable relative to FOD or DL.*

# KeYmaera X aXiomatic Tactical Theorem Prover for CPS



$-1{:}\ x\geq 0$ ⊢ $1{:}\ [x:=x+1;\ \cup\ \{x'=v\}]\,x\geq 0$

$-2{:}\ v\geq 0$

[∪] **$[a\cup b]P$**$\leftrightarrow[a]P\wedge[b]P$

loop

$x\geq 0, v\geq 0$ ⊢ $[\{x:=x+1;\ \cup\ \{x'=v\}\}^*]\,x\geq 0$

→R …

⊢ $x\geq 0\wedge v\geq 0 \rightarrow [\{x:=x+1;\ \cup\ \{x'=v\wedge true\}\}^*]\,x\geq 0$

## Trustworthy

- Uniform substitution
- Sound & complete
- Small core: 1700 LOC

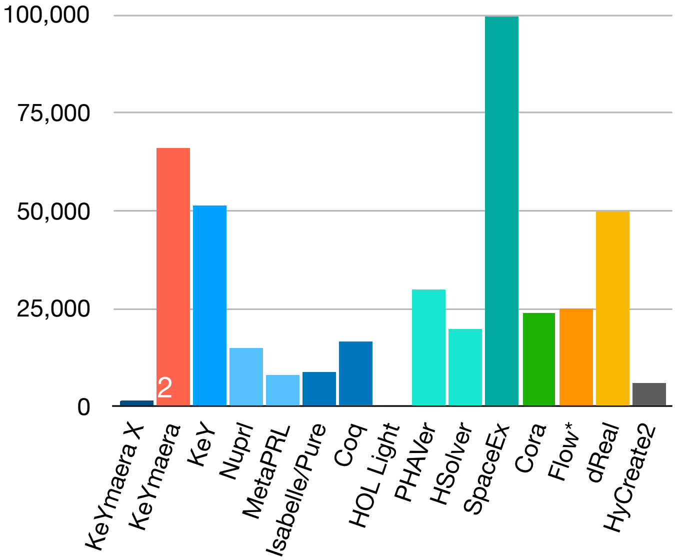
## Flexible

- Proof automation
- Interactive UI
- Programmable

## Customizable

- Scala+Java API
- Command line
- REST API

# KeYmaera X Small Kernel for Soundness 1 700 LOC



Disclaimer: Self-reported estimates of the soundness-critical lines of code + rules

# Uniform Substitution

**Theorem (Soundness)** replace all occurrences of $p(\cdot)$

$$\text{US}\ \frac{\phi}{\sigma(\phi)}$$

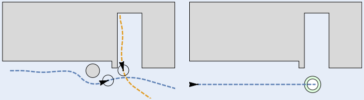
*provided* $FV(\sigma|_{\Sigma(\theta)}) \cap BV(\otimes(\cdot)) = \emptyset$ *for each operation* $\otimes(\theta)$ *in* $\phi$

i.e. bound variables $U = \mathrm{BV}(\otimes(\cdot))$ of operator $\otimes$
are not free in the substitution on its argument $\theta$ ($U$-admissible)

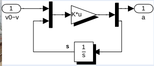
$$\text{US}\ \frac{[a \cup b]p(\bar{x}) \leftrightarrow [a]p(\bar{x}) \wedge [b]p(\bar{x})}{[x := x+1 \cup x' = 1]x \geq 0 \leftrightarrow [x := x+1]x \geq 0 \wedge [x' = 1]x \geq 0}$$

# Application Highlights

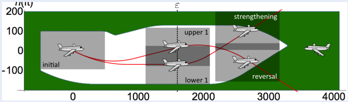
## Obstacle Avoidance + Ground Navigation



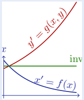
## Train Control Brakes



## Airborne Collision Avoidance (ACAS X)



## Ship Cooling



NSF DARPA

BOSCH SIEMENS

APL
JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

# Outline (Proving ODEs in CPSs)

1. CPS are Multi-Dynamical Systems
   - Hybrid Systems / Games / Stochastic / Distributed Hybrid Systems
2. Differential Dynamic Logic
   - Syntax
   - Semantics
   - Example: Car Control Design
3. Dynamic Axioms for Dynamical Systems
   - Axiomatics
   - Example: Safe Car Control
   - Soundness and Completeness
4. Differential Invariants for Differential Equations
   - Differential Axioms
   - Example: Differential Ghosts
5. Applications
6. Summary

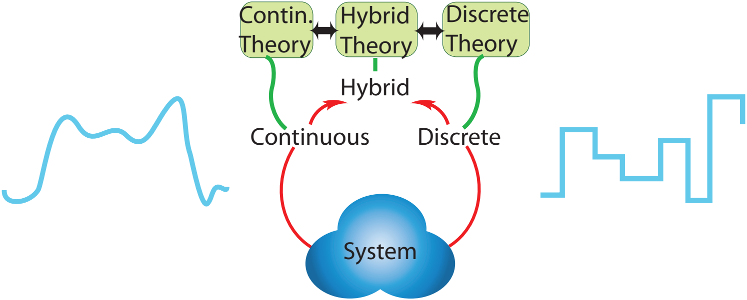
# Complete Proof Theory of Hybrid Systems

**Theorem (Sound & Complete)** (JAR'08, LICS'12, JAR'17)

dL *calculus is a sound & complete axiomatization of hybrid systems relative to either differential equations* ***or*** *to discrete dynamics.*

**Corollary (Complete Proof-theoretical Bridge)**

proving continuous = proving hybrid = proving discrete



# Complete Proof Theory of Hybrid Systems

**Theorem (Sound & Complete)** (JAR'08, LICS'12, JAR'17)

dL *calculus is a sound & complete axiomatization of hybrid systems relative to either differential equations* ***or*** *to discrete dynamics.*

**Corollary (Complete Proof-theoretical Bridge)**

proving continuous = proving hybrid = proving discrete

**Theorem (Equi-expressibility)** (LICS'12)

$$\forall P \in \mathrm{dL}\ \exists P^\flat \in FODE\ \vDash P \leftrightarrow P^\flat$$
$$\forall P \in \mathrm{dL}\ \exists P^\# \in DL\ \vDash P \leftrightarrow P^\#$$

**Theorem (Relative Decidability)** (LICS'12)

*Validity of* dL *sentences is decidable relative to FOD or DL.*

# Global Descriptive Power of Local Differential Equations

**Descriptive power of differential equations**

1. Simple differential equations describe complex physical processes.
2. Solution is a global description of the system evolution.
3. ODE is a local characterization.
4. Complexity difference between local description and global behavior.
5. Let's exploit that phenomenon for proofs!
6. Reason locally about global behavior.

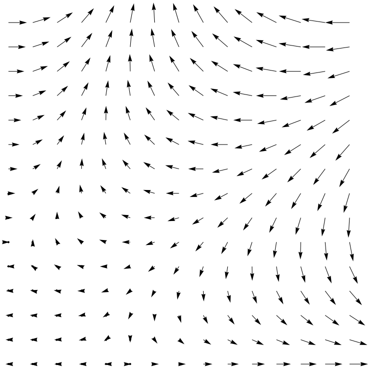
$$x'' = -x \qquad \text{has } x(t) = \sin(t) = t - \frac{t^3}{3!} + \frac{t^5}{5!} - \frac{t^7}{7!} + \frac{t^9}{9!} - \dots$$

$$x''(t) = e^{t^2} \qquad \text{has no elementary closed-form solution}$$

# Intuition for Differential Invariants

**Differential Invariant**

$$\frac{\Gamma \vdash J, \Delta \quad J \vdash \,???J \quad J \vdash P}{\Gamma \vdash [x' = f(x)]P, \Delta}$$

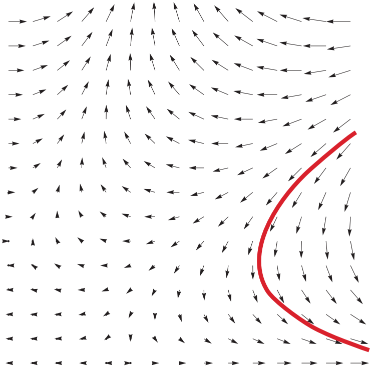


$$['] \; [x' = f(x)]P \leftrightarrow \forall t{\geq}0\, [x := y(t)]P \qquad (y' = f(y),\ y(0) = x)$$

# Intuition for Differential Invariants

**Differential Invariant**

$$\frac{\Gamma \vdash J, \Delta \quad J \vdash ???J \quad J \vdash P}{\Gamma \vdash [x' = f(x)]P, \Delta}$$

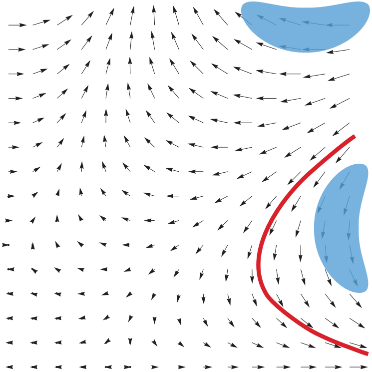


$$['] \; [x' = f(x)]P \leftrightarrow \forall t{\geq}0\,[x := y(t)]P$$ (y' =f(y), y(0)=x)

# Intuition for Differential Invariants

**Differential Invariant**

$$\frac{\Gamma \vdash J, \Delta \quad J \vdash {\color{red}???} J \quad J \vdash P}{\Gamma \vdash [x' = f(x)]P, \Delta}$$



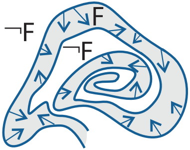
$$['] \; [x' = f(x)]P \leftrightarrow \forall t \geq 0 \, [x := y(t)]P \qquad (y' = f(y),\ y(0) = x)$$

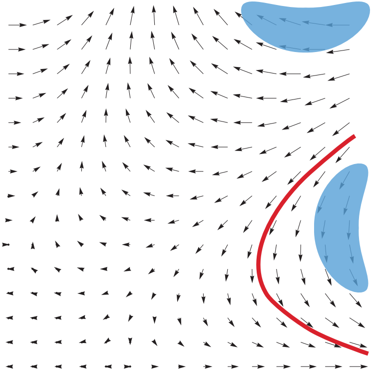
# Intuition for Differential Invariants

**Differential Invariant**

$$\frac{\Gamma \vdash J, \Delta \quad J \vdash \textcolor{red}{???}J \quad J \vdash P}{\Gamma \vdash [x' = f(x)]P, \Delta}$$

Want: formula $J$ remains true in the direction of the dynamics





$$['] \; [x' = f(x)]P \leftrightarrow \forall t{\geq}0 \, [x := y(t)]P \qquad (y' = f(y), y(0) = x)$$

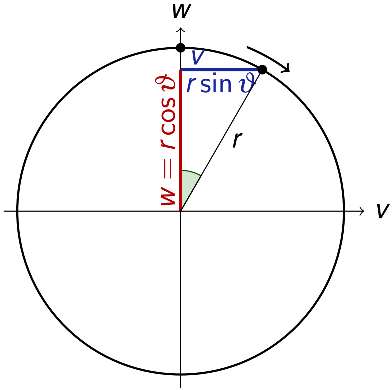
Next step is undefined for ODEs. But don't need to know where exactly the system evolves to. Just that it remains somewhere in $J$.
Show: only evolves into directions in which formula $J$ stays true.

# Guiding Example

$$v^2+w^2=r^2 \rightarrow [v'=w, w'=-v]\, v^2+w^2=r^2$$

# Guiding Example: Rotational Dynamics

$$v^2 + w^2 = r^2 \rightarrow [v' = w, w' = -v]\, v^2 + w^2 = r^2$$



# Guiding Example: Rotational Dynamics

$$v^2+w^2=r^2 \to [v'=w, w'=-v]\, v^2+w^2=r^2$$

$$\dfrac{}{\vdash v^2+w^2-r^2=0 \to [v'=w, w'=-v]\, v^2+w^2-r^2=0}\;{\to}\mathrm{R}$$

# Guiding Example: Rotational Dynamics

$$v^2 + w^2 = r^2 \rightarrow [v' = w, w' = -v]\, v^2 + w^2 = r^2$$

$$\dfrac{\text{dI}\ \dfrac{}{v^2+w^2-r^2=0 \vdash [v' = w, w' = -v]\, v^2 + w^2 - r^2 = 0}}{\rightarrow\text{R}\ \vdash v^2+w^2-r^2=0 \rightarrow [v' = w, w' = -v]\, v^2+w^2-r^2=0}$$

# Guiding Example: Rotational Dynamics

$$v^2+w^2=r^2 \rightarrow [v'=w, w'=-v]\,v^2+w^2=r^2$$

$$\rightarrow\mathrm{R}\;\dfrac{\mathrm{dI}\;\dfrac{[':=]\;\dfrac{}{\vdash [v':=w][w':=-v]\,2vv'+2ww'-2rr'=0}}{v^2+w^2-r^2=0 \vdash [v'=w, w'=-v]\,v^2+w^2-r^2=0}}{\vdash v^2+w^2-r^2=0 \rightarrow [v'=w, w'=-v]\,v^2+w^2-r^2=0}$$

# Guiding Example: Rotational Dynamics

$$v^2+w^2=r^2 \to [v'=w,w'=-v]\,v^2+w^2=r^2$$

$$\to\!\text{R}\;\dfrac{\text{dI}\;\dfrac{[':=]\;\dfrac{\mathbb{R}\;\dfrac{}{\vdash 2v(w)+2w(-v)=0}}{\vdash [v':=w][w':=-v]2vv'+2ww'-2rr'=0}}{v^2+w^2-r^2=0 \vdash [v'=w,w'=-v]\,v^2+w^2-r^2=0}}{\vdash v^2+w^2-r^2=0 \to [v'=w,w'=-v]\,v^2+w^2-r^2=0}$$

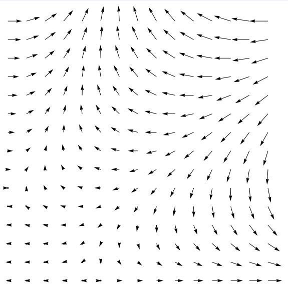
# Guiding Example: Rotational Dynamics

$$v^2+w^2=r^2 \rightarrow [v'=w, w'=-v]\, v^2+w^2=r^2$$

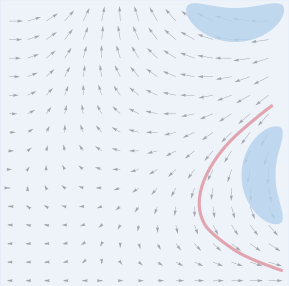
$$\begin{array}{l}
\qquad\qquad\qquad\qquad * \\
\mathbb{R}\ \overline{\qquad\qquad\qquad\quad \vdash 2v(w)+2w(-v)=0 \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad} \\
[':=]\ \overline{\qquad\qquad\qquad \vdash [v':=w][w':=-v]\,2vv'+2ww'-2rr'=0 \qquad\qquad\qquad\qquad} \\
\text{dI}\ \overline{v^2+w^2-r^2=0 \vdash [v'=w, w'=-v]\, v^2+w^2-r^2=0 \qquad\qquad\qquad\qquad} \\
\rightarrow\text{R}\ \overline{\qquad\qquad\qquad \vdash v^2+w^2-r^2=0 \rightarrow [v'=w, w'=-v]\, v^2+w^2-r^2=0}
\end{array}$$

# Differential Invariants for Differential Equations

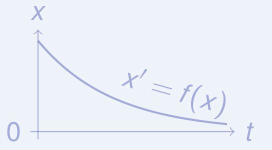
## Differential Invariant



## Differential Cut



## Differential Ghost



$$\begin{tikzcd}
\mathcal{DI}_{\geq} \arrow[rrr, hook] \arrow[dd, squiggly, dash] & & & \mathcal{DI}_{\geq,\wedge,\vee} \arrow[r, equal] \arrow[dd, squiggly, dash] & \mathcal{DI}_{\geq,=,\wedge,\vee} \arrow[dr, hook] \arrow[dd, squiggly, dash] & \\
& \mathcal{DI}_{=} \arrow[ul, hook] \arrow[r, equal] \arrow[dl, dash] & \mathcal{DI}_{=,\wedge,\vee} \arrow[ur, hook] \arrow[rrr, hook] \arrow[drr, hook, bend left] \arrow[dr, dash] & & & \mathcal{DI} \\
\mathcal{DI}_{>} \arrow[rrr, hook] & & & \mathcal{DI}_{>,\wedge,\vee} \arrow[r, hook] & \mathcal{DI}_{>,=,\wedge,\vee} \arrow[ur, hook] &
\end{tikzcd}$$

## Logic

Provability theory

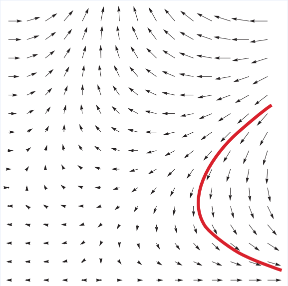
## Math

Character-istic PDE

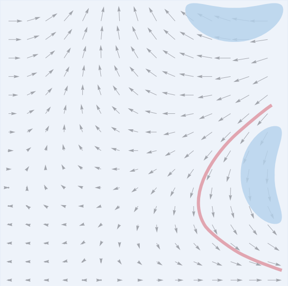
JLogComput'10,FMSD'09,LMCS'12,LICS'12,ITP'12,JAR'17,LICS'18

# Differential Invariants for Differential Equations

## Differential Invariant



## Differential Cut



## Differential Ghost

$$\begin{tikzcd}
\mathcal{DI}_{\geq} \arrow[rrr, hook] \arrow[dd, squiggly, no head] & & & \mathcal{DI}_{\geq,\wedge,\vee} \arrow[r, equal] \arrow[dd, squiggly, no head] & \mathcal{DI}_{\geq,=,\wedge,\vee} \arrow[dr, hook] \arrow[dd, squiggly, no head] & \\
& \mathcal{DI}_{=} \arrow[ul, hook] \arrow[r, equal] \arrow[dl, dash] & \mathcal{DI}_{=,\wedge,\vee} \arrow[ur, hook] \arrow[rrr, hook] \arrow[drr, hook, bend left] \arrow[dr, dash] & & & \mathcal{DI} \\
\mathcal{DI}_{>} \arrow[rrr, hook] & & & \mathcal{DI}_{>,\wedge,\vee} \arrow[r, hook] & \mathcal{DI}_{>,=,\wedge,\vee} \arrow[ur, hook] &
\end{tikzcd}$$

## Logic

Provability theory

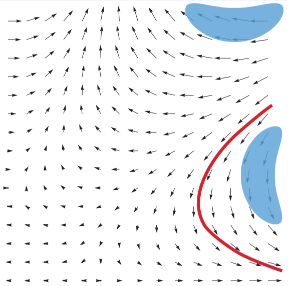
## Math

Characteristic PDE

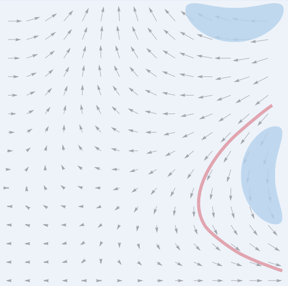
JLogComput'10,FMSD'09,LMCS'12,LICS'12,ITP'12,JAR'17,LICS'18

# Differential Invariants for Differential Equations

## Differential Invariant



## Differential Cut



## Differential Ghost

$$\begin{tikzcd}
\mathcal{DI}_{\geq} \arrow[rrr, hook] \arrow[dd, squiggly, no head] & & & \mathcal{DI}_{\geq,\wedge,\vee} \arrow[r, equal] \arrow[dd, squiggly, no head] & \mathcal{DI}_{\geq,=,\wedge,\vee} \arrow[dr, hook] \arrow[dd, squiggly, no head] & \\
& \mathcal{DI}_{=} \arrow[ul, hook] \arrow[r, equal] \arrow[dl, no head] & \mathcal{DI}_{=,\wedge,\vee} \arrow[ur, hook] \arrow[rrr, hook] \arrow[ddrr, hook, bend left] \arrow[dr, no head] & & & \mathcal{DI} \\
\mathcal{DI}_{>} \arrow[rrr, hook] & & & \mathcal{DI}_{>,\wedge,\vee} \arrow[r, hook] & \mathcal{DI}_{>,=,\wedge,\vee} \arrow[ur, hook] &
\end{tikzcd}$$

## Logic

Provability theory

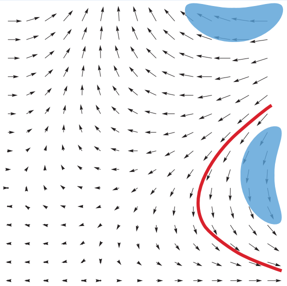
## Math

Character-istic PDE

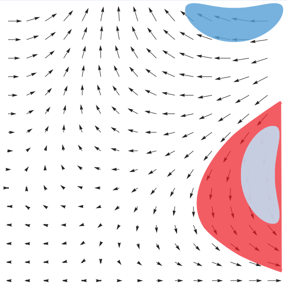
JLogComput'10,FMSD'09,LMCS'12,LICS'12,ITP'12,JAR'17,LICS'18

# Differential Invariants for Differential Equations

### Differential Invariant



### Differential Cut



### Differential Ghost

$$\begin{tikzcd}
\mathcal{DI}_{\geq} \arrow[rrr, hook] \arrow[dd, squiggly, no head] & & & \mathcal{DI}_{\geq,\wedge,\vee} \arrow[r, equal] \arrow[dd, squiggly, no head] & \mathcal{DI}_{\geq,=,\wedge,\vee} \arrow[dr, hook] \arrow[dd, squiggly, no head] & \\
& \mathcal{DI}_{=} \arrow[ul, hook] \arrow[r, equal] \arrow[dl, dash] & \mathcal{DI}_{=,\wedge,\vee} \arrow[ur, hook] \arrow[rrr, hook] \arrow[drr, hook, bend left] \arrow[dr, dash] & & & \mathcal{DI} \\
\mathcal{DI}_{>} \arrow[rrr, hook] & & & \mathcal{DI}_{>,\wedge,\vee} \arrow[r, hook] & \mathcal{DI}_{>,=,\wedge,\vee} \arrow[ur, hook] &
\end{tikzcd}$$

**Logic**

Provability theory

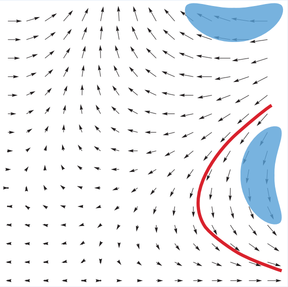
**Math**

Characteristic PDE

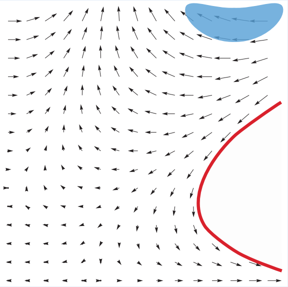
JLogComput'10,FMSD'09,LMCS'12,LICS'12,ITP'12,JAR'17,LICS'18

# Differential Invariants for Differential Equations

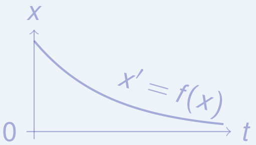
### Differential Invariant



### Differential Cut



### Differential Ghost



$$\begin{tikzcd}
\mathcal{DI}_{\geq} \arrow[rrr, hook] \arrow[dd, squiggly, no head] & & & \mathcal{DI}_{\geq,\wedge,\vee} \arrow[r, equal] \arrow[dd, squiggly, no head] & \mathcal{DI}_{\geq,=,\wedge,\vee} \arrow[dr, hook] \arrow[dd, squiggly, no head] & \\
& \mathcal{DI}_{=} \arrow[ul, hook] \arrow[r, equal] \arrow[dl, no head] & \mathcal{DI}_{=,\wedge,\vee} \arrow[ur, hook] \arrow[rrr, hook] \arrow[drr, hook, bend left] \arrow[dr, no head] & & & \mathcal{DI} \\
\mathcal{DI}_{>} \arrow[rrr, hook] & & & \mathcal{DI}_{>,\wedge,\vee} \arrow[r, hook] & \mathcal{DI}_{>,=,\wedge,\vee} \arrow[ur, hook] &
\end{tikzcd}$$

### Logic

Provability theory

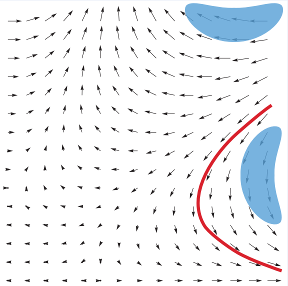
### Math

Characteristic PDE

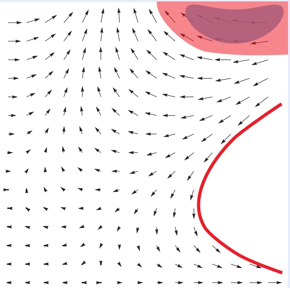
JLogComput'10,FMSD'09,LMCS'12,LICS'12,ITP'12,JAR'17,LICS'18

# Differential Invariants for Differential Equations

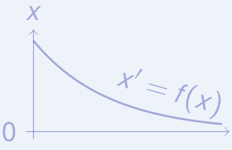
### Differential Invariant



### Differential Cut



### Differential Ghost



$$\begin{tikzcd}
\mathcal{DI}_{\geq} \arrow[rrr, hook] \arrow[dd, squiggly, dash] & & & \mathcal{DI}_{\geq,\wedge,\vee} \arrow[r, equal] \arrow[dd, squiggly, dash] & \mathcal{DI}_{\geq,=,\wedge,\vee} \arrow[dr, hook] \arrow[dd, squiggly, dash] & \\
& \mathcal{DI}_{=} \arrow[ul, hook] \arrow[r, equal] \arrow[dl, dash] & \mathcal{DI}_{=,\wedge,\vee} \arrow[ur, hook] \arrow[rrr, hook] \arrow[dr, dash] \arrow[drr, hook, bend left] & & & \mathcal{DI} \\
\mathcal{DI}_{>} \arrow[rrr, hook] & & & \mathcal{DI}_{>,\wedge,\vee} \arrow[r, hook] & \mathcal{DI}_{>,=,\wedge,\vee} \arrow[ur, hook] &
\end{tikzcd}$$

### Logic

Provability theory

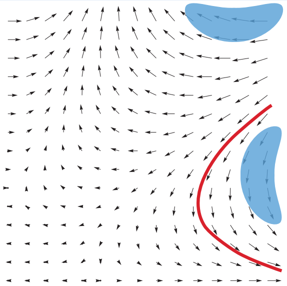
### Math

Characteristic PDE

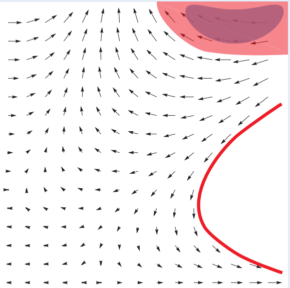
JLogComput'10,FMSD'09,LMCS'12,LICS'12,ITP'12,JAR'17,LICS'18

# Differential Invariants for Differential Equations

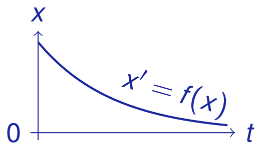
## Differential Invariant



## Differential Cut



## Differential Ghost



$$\begin{tikzcd}
\mathcal{DI}_{\geq} \arrow[rr, hook] \arrow[dd, squiggly, no head] & & \mathcal{DI}_{\geq,\wedge,\vee} \arrow[r, equal] \arrow[dd, squiggly, no head] & \mathcal{DI}_{\geq,=,\wedge,\vee} \arrow[dr, hook] \arrow[dd, squiggly, no head] & \\
& \mathcal{DI}_{=} \arrow[ul, hook] \arrow[r, equal] \arrow[dl, dash] & \mathcal{DI}_{=,\wedge,\vee} \arrow[u, hook] \arrow[rr, hook] \arrow[d, dash] \arrow[dr, bend left] & & \mathcal{DI} \\
\mathcal{DI}_{>} \arrow[rr, hook] & & \mathcal{DI}_{>,\wedge,\vee} \arrow[r, hook] & \mathcal{DI}_{>,=,\wedge,\vee} \arrow[ur, hook] &
\end{tikzcd}$$

### Logic

Provability theory

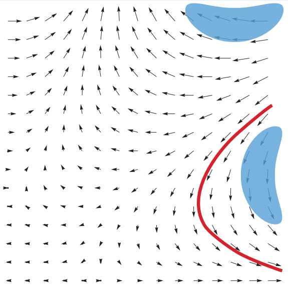
### Math

Character-istic PDE

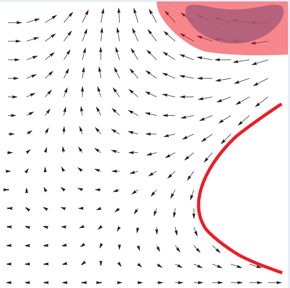
JLogComput’10,FMSD’09,LMCS’12,LICS’12,ITP’12,JAR’17,LICS’18

# Differential Invariants for Differential Equations

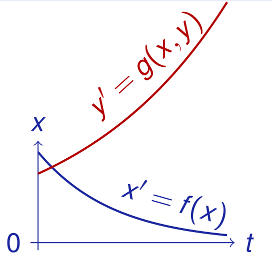
## Differential Invariant



## Differential Cut



## Differential Ghost



$$\begin{tikzcd}
\mathcal{DI}_{\geq} \arrow[rrr, hook] \arrow[dd, squiggly, no head] & & & \mathcal{DI}_{\geq,\land,\lor} \arrow[r, equal] \arrow[dd, squiggly, no head] & \mathcal{DI}_{\geq,=,\land,\lor} \arrow[dr, hook] \arrow[dd, squiggly, no head] & \\
& \mathcal{DI}_{=} \arrow[ul, hook] \arrow[r, equal] \arrow[dl, dash] & \mathcal{DI}_{=,\land,\lor} \arrow[ur, hook] \arrow[rrr, hook] \arrow[drr, hook, bend left=10] \arrow[dr, dash] & & & \mathcal{DI} \\
\mathcal{DI}_{>} \arrow[rrr, hook] & & & \mathcal{DI}_{>,\land,\lor} \arrow[r, hook] & \mathcal{DI}_{>,=,\land,\lor} \arrow[ur, hook] &
\end{tikzcd}$$

## Logic

Provability theory

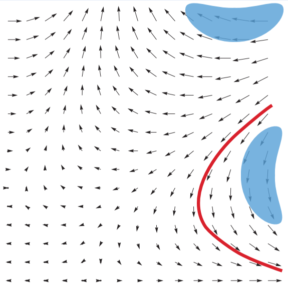
## Math

Character-istic PDE

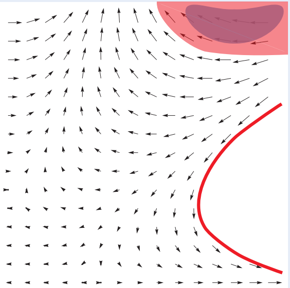
JLogComput'10,FMSD'09,LMCS'12,LICS'12,ITP'12,JAR'17,LICS'18

# Differential Invariants for Differential Equations

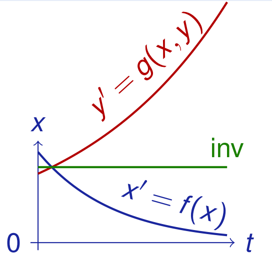
## Differential Invariant



## Differential Cut



## Differential Ghost



$$\begin{tikzcd}
\mathcal{DI}_{\geq} \arrow[rrr, hook] \arrow[dd, squiggly, dash] & & & \mathcal{DI}_{\geq,\wedge,\vee} \arrow[r, equal] \arrow[dd, squiggly, dash] & \mathcal{DI}_{\geq,=,\wedge,\vee} \arrow[dd, squiggly, dash] \arrow[dr, hook] & \\
& \mathcal{DI}_{=} \arrow[ul, hook] \arrow[r, equal] \arrow[dl, squiggly, dash] & \mathcal{DI}_{=,\wedge,\vee} \arrow[ur, hook] \arrow[rrr, hook] \arrow[drr, hook, bend left] \arrow[dr, squiggly, dash] & & & \mathcal{DI} \\
\mathcal{DI}_{>} \arrow[rrr, hook] & & & \mathcal{DI}_{>,\wedge,\vee} \arrow[r, hook] & \mathcal{DI}_{>,=,\wedge,\vee} \arrow[ur, hook] &
\end{tikzcd}$$

## Logic

Provability theory

## Math

Characteristic PDE

JLogComput'10,FMSD'09,LMCS'12,LICS'12,ITP'12,JAR'17,LICS'18

# Differential Invariants for Differential Equations

**Differential Invariant**

$$\frac{Q \vdash [x' := f(x)](P)'}{P \vdash [x' = f(x) \,\&\, Q]P}$$

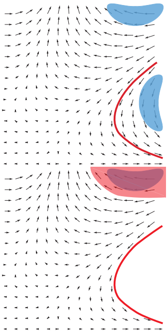
**Differential Cut**

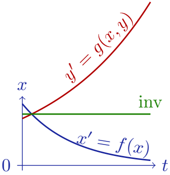
$$\frac{P \vdash [x' = f(x) \,\&\, Q]C \quad P \vdash [x' = f(x) \,\&\, Q \land C]P}{P \vdash [x' = f(x) \,\&\, Q]P}$$

**Differential Ghost**

$$\frac{P \leftrightarrow \exists y\, G \quad G \vdash [x' = f(x), y' = g(x,y) \,\&\, Q]G}{P \vdash [x' = f(x) \,\&\, Q]P}$$

deductive power adds DI $\prec$ DC $\prec$ DG



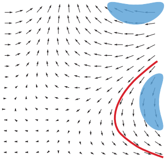


JLogComput'10,LMCS'12, LICS'12,JAR'17,LICS'18

# Differential Invariants for Differential Equations

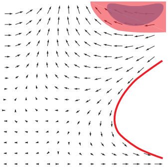
## Differential Invariant

$$\frac{Q \vdash [x' := f(x)](P)'}{P \vdash [x' = f(x) \,\&\, Q]P}$$



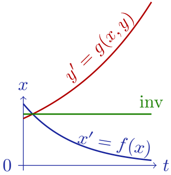
## Differential Cut

$$\frac{P \vdash [x' = f(x) \,\&\, Q]C \quad P \vdash [x' = f(x) \,\&\, Q \land C]P}{P \vdash [x' = f(x) \,\&\, Q]P}$$



## Differential Ghost

$$\frac{P \leftrightarrow \exists y\, G \quad G \vdash [x' = f(x), y' = g(x,y) \,\&\, Q]G}{P \vdash [x' = f(x) \,\&\, Q]P}$$

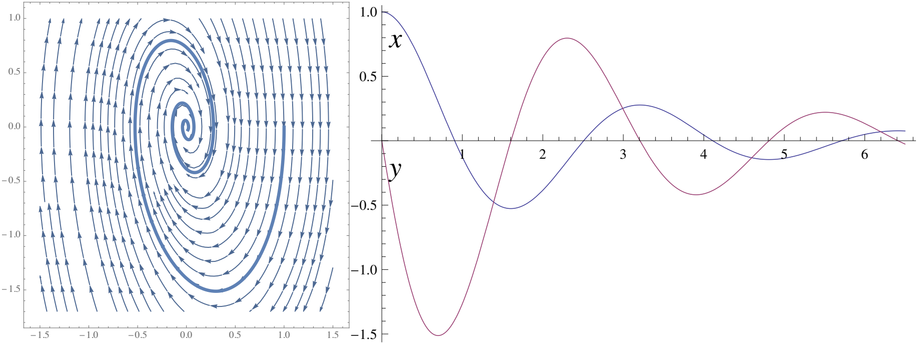


if new $y' = g(x,y)$ has long enough solution

JLogComput'10,LMCS'12, LICS'12,JAR'17,LICS'18

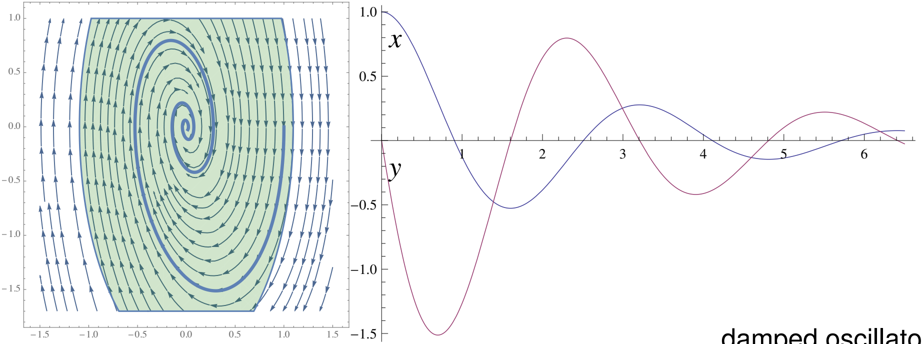
# Differential Invariants for Differential Equations

$$\frac{}{\omega^2x^2+y^2\le c^2 \vdash [x'=y, y'=-\omega^2x-2d\omega y \,\&\, \omega\ge 0\land d\ge 0]\,\omega^2x^2+y^2\le c^2}$$



# Differential Invariants for Differential Equations

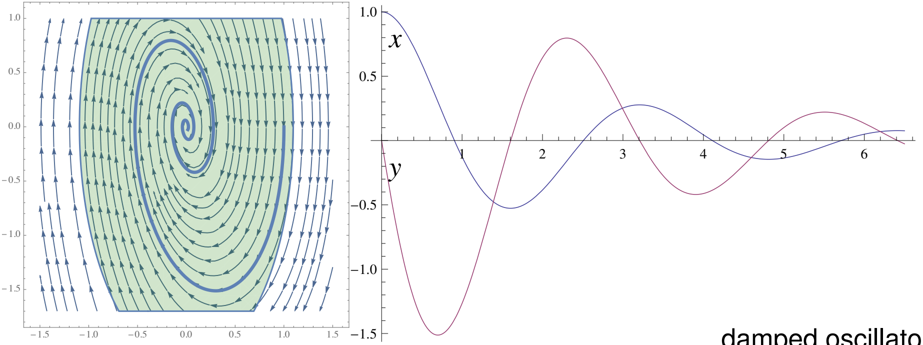
$$\frac{}{\omega^2x^2+y^2\leq c^2 \vdash [x'=y, y'=-\omega^2x-2d\omega y \,\&\, \omega\geq 0 \land d\geq 0]\, \omega^2x^2+y^2\leq c^2}$$



damped oscillator

# Differential Invariants for Differential Equations

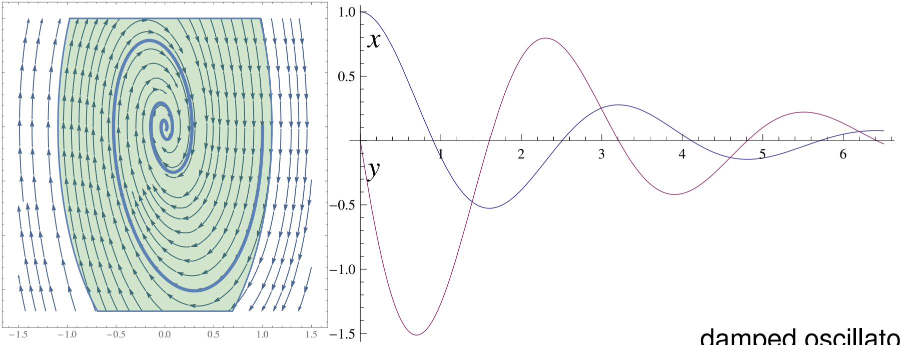
$$\frac{\omega\geq 0 \land d\geq 0 \vdash [x':=y][y':=-\omega^2x - 2d\omega y]\, 2\omega^2 x x' + 2yy' \leq 0}{\omega^2x^2+y^2\leq c^2 \vdash [x' = y, y' = -\omega^2 x - 2d\omega y \,\&\, \omega\geq 0 \land d\geq 0]\, \omega^2x^2+y^2\leq c^2}$$



damped oscillator

# Differential Invariants for Differential Equations

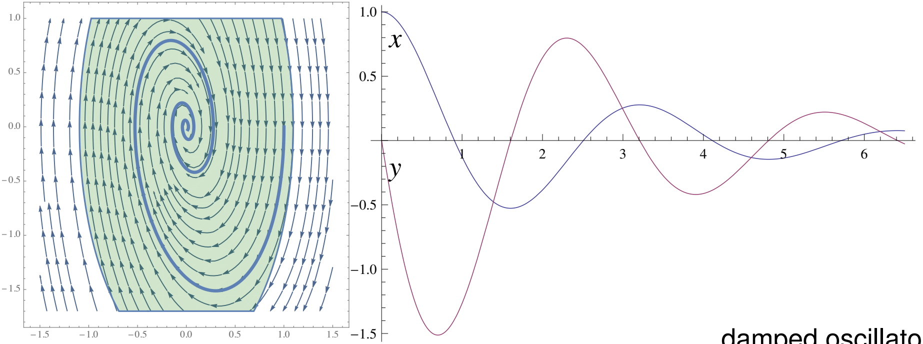
$$\dfrac{\dfrac{\dfrac{}{\omega\ge0\land d\ge0\vdash 2\omega^2xy+2y(-\omega^2x-2d\omega y)\le0}}{\omega\ge0\land d\ge0\vdash [x':=y][y':=-\omega^2x-2d\omega y]2\omega^2xx'+2yy'\le0}}{\omega^2x^2+y^2\le c^2\vdash [x'=y,y'=-\omega^2x-2d\omega y\,\&\,\omega\ge0\land d\ge0]\,\omega^2x^2+y^2\le c^2}$$



damped oscillator

# Differential Invariants for Differential Equations

$$\dfrac{\dfrac{\dfrac{*}{\omega\geq 0 \land d\geq 0 \vdash 2\omega^2 xy + 2y(-\omega^2 x - 2d\omega y) \leq 0}}{\omega\geq 0 \land d\geq 0 \vdash [x':=y][y':=-\omega^2 x - 2d\omega y]\, 2\omega^2 x x' + 2 y y' \leq 0}}{\omega^2 x^2 + y^2 \leq c^2 \vdash [x' = y, y' = -\omega^2 x - 2d\omega y \,\&\, \omega\geq 0 \land d\geq 0]\, \omega^2 x^2 + y^2 \leq c^2}$$

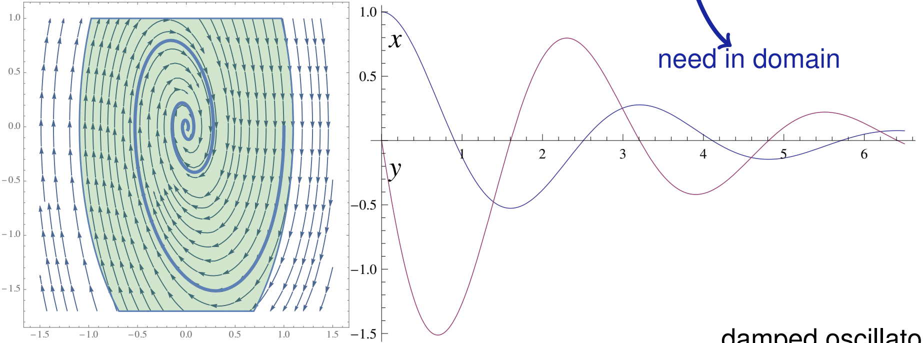


damped oscillator

# Differential Invariants for Differential Equations

$$\cfrac{\cfrac{\cfrac{*}{\omega\geq0 \land d\geq0 \vdash 2\omega^2xy+2y(-\omega^2x-2d\omega y)\leq 0}}{\omega\geq0\land d\geq0 \vdash [x':=y][y':=-\omega^2x-2d\omega y]2\omega^2xx'+2yy'\leq 0}}{\omega^2x^2+y^2\leq c^2 \vdash [x'=y,y'=-\omega^2x-2d\omega y \,\&\, \omega\geq0\land d\geq0]\,\omega^2x^2+y^2\leq c^2}$$

need in domain



damped oscillator

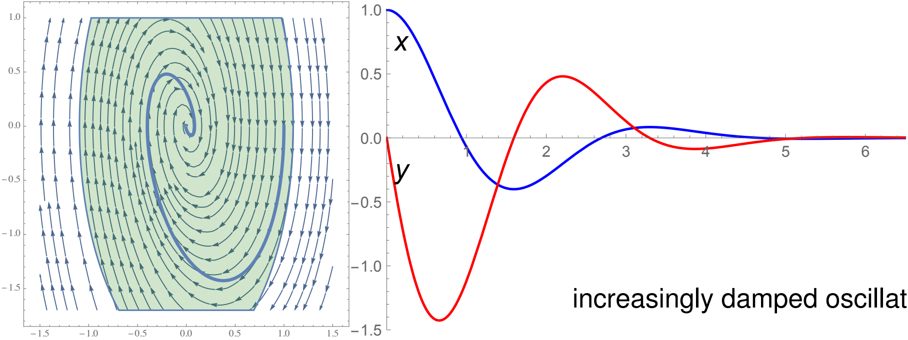
# Differential Cuts for Differential Equations

$$\frac{}{\omega^2x^2+y^2\leq c^2 \vdash [x'=y, y'=-\omega^2x-2d\omega y, \textcolor{red}{d'=7}\,\&\,\omega\geq 0]\,\omega^2x^2+y^2\leq c^2}$$

# Differential Cuts for Differential Equations

---

$$\omega^2x^2+y^2\le c^2 \vdash [x'=y, y'=-\omega^2x-2d\omega y, d'=7 \,\&\, \omega\ge 0]\,\omega^2x^2+y^2\le c^2$$



increasingly damped oscillator

# Differential Cuts for Differential Equations

$$\dfrac{\omega^2x^2+y^2\leq c^2 \vdash [x'=y, y'=-\omega^2x-2d\omega y, d'=7\ \&\ \omega\geq 0\land d\geq 0]\,\omega^2x^2+y^2\leq c^2}{\omega^2x^2+y^2\leq c^2 \vdash [x'=y, y'=-\omega^2x-2d\omega y, d'=7\ \&\ \omega\geq 0]\,\omega^2x^2+y^2\leq c^2}$$

increasingly damped oscillator

# Differential Cuts for Differential Equations

$$\cfrac{\cfrac{}{\omega^2x^2+y^2\le c^2 \vdash [x'=y,y'=-\omega^2x-2d\omega y,d'=7\,\&\,\omega\ge0\land d\ge0]\,\omega^2x^2+y^2\le c^2}}{\omega^2x^2+y^2\le c^2 \vdash [x'=y,y'=-\omega^2x-2d\omega y,d'=7\,\&\,\omega\ge0]\,\omega^2x^2+y^2\le c^2}$$

ask

$$\cfrac{}{d\ge0 \vdash [x'=y,y'=-\omega^2x-2d\omega y,d'=7\,\&\,\omega\ge0]\,d\ge0}$$

increasingly damped oscillator

# Differential Cuts for Differential Equations

$$\frac{\omega^2x^2+y^2\le c^2 \vdash [x'=y, y'=-\omega^2x-2d\omega y, d'=7\,\&\,\omega\ge0\land d\ge0]\,\omega^2x^2+y^2\le c^2}{\omega^2x^2+y^2\le c^2 \vdash [x'=y, y'=-\omega^2x-2d\omega y, d'=7\,\&\,\omega\ge0]\,\omega^2x^2+y^2\le c^2}$$

$$\frac{\omega\ge0 \vdash [d':=7]\,d'\ge0}{d\ge0 \vdash [x'=y, y'=-\omega^2x-2d\omega y, d'=7\,\&\,\omega\ge0]\,d\ge0}$$

increasingly damped oscillator

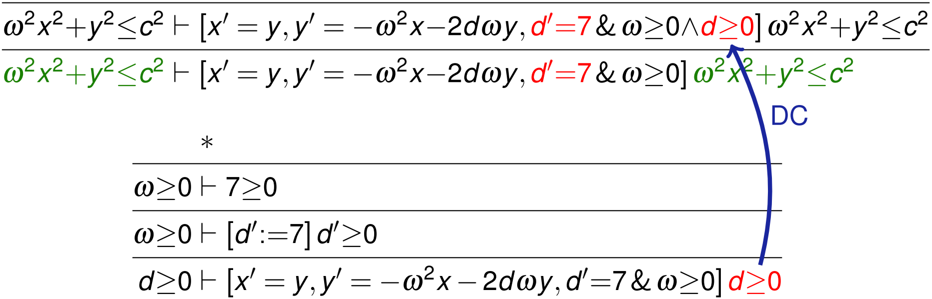
# Differential Cuts for Differential Equations

$$\cfrac{\cfrac{}{\omega^2x^2+y^2\le c^2 \vdash [x'=y, y'=-\omega^2x-2d\omega y, d'=7\,\&\,\omega\ge 0\land d\ge 0]\,\omega^2x^2+y^2\le c^2}}{\omega^2x^2+y^2\le c^2 \vdash [x'=y, y'=-\omega^2x-2d\omega y, d'=7\,\&\,\omega\ge 0]\,\omega^2x^2+y^2\le c^2}$$

$$\cfrac{\cfrac{\cfrac{}{\omega\ge 0 \vdash 7\ge 0}}{\omega\ge 0 \vdash [d':=7]\,d'\ge 0}}{d\ge 0 \vdash [x'=y, y'=-\omega^2x-2d\omega y, d'=7\,\&\,\omega\ge 0]\,d\ge 0}$$

increasingly damped oscillator

# Differential Cuts for Differential Equations



$$\dfrac{\overline{\omega^2x^2+y^2\le c^2 \vdash [x'=y,y'=-\omega^2x-2d\omega y,d'=7\,\&\,\omega\ge0\land d\ge0]\,\omega^2x^2+y^2\le c^2}}{\omega^2x^2+y^2\le c^2 \vdash [x'=y,y'=-\omega^2x-2d\omega y,d'=7\,\&\,\omega\ge0]\,\omega^2x^2+y^2\le c^2}$$

DC

$$\dfrac{\dfrac{\dfrac{*}{\omega\ge0\vdash 7\ge0}}{\omega\ge0\vdash [d':=7]\,d'\ge0}}{d\ge0\vdash [x'=y,y'=-\omega^2x-2d\omega y,d'=7\,\&\,\omega\ge0]\,d\ge0}$$

increasingly damped oscillator

# Differential Cuts for Differential Equations

$$\begin{array}{l}
\hline
\quad \omega\geq0\land d\geq0 \vdash [x':=y][y':=-\omega^2x-2d\omega y]\,2\omega^2xx'+2yy'\leq 0 \\
\hline
\omega^2x^2+y^2\leq c^2 \vdash [x'=y, y'=-\omega^2x-2d\omega y, d'=7\,\&\,\omega\geq0\land d\geq0]\,\omega^2x^2+y^2\leq c^2 \\
\hline
\omega^2x^2+y^2\leq c^2 \vdash [x'=y, y'=-\omega^2x-2d\omega y, d'=7\,\&\,\omega\geq0]\,\omega^2x^2+y^2\leq c^2
\end{array}$$

$$\begin{array}{l}
\qquad\quad * \\
\hline
\omega\geq0 \vdash 7\geq0 \\
\hline
\omega\geq0 \vdash [d':=7]\,d'\geq0 \\
\hline
d\geq0 \vdash [x'=y, y'=-\omega^2x-2d\omega y, d'=7\,\&\,\omega\geq0]\,d\geq0
\end{array}$$

increasingly damped oscillator

# Differential Cuts for Differential Equations

$$\begin{array}{c}
\hline
\omega\geq0\land d\geq0 \vdash 2\omega^2xy+2y(-\omega^2x-2d\omega y)\leq 0\\
\hline
\omega\geq0\land d\geq0 \vdash [x':=y][y':=-\omega^2x-2d\omega y]\,2\omega^2xx'+2yy'\leq 0\\
\hline
\omega^2x^2+y^2\leq c^2 \vdash [x'=y,y'=-\omega^2x-2d\omega y,d'=7\,\&\,\omega\geq0\land d\geq0]\,\omega^2x^2+y^2\leq c^2\\
\hline
\omega^2x^2+y^2\leq c^2 \vdash [x'=y,y'=-\omega^2x-2d\omega y,d'=7\,\&\,\omega\geq0]\,\omega^2x^2+y^2\leq c^2
\end{array}$$

$$\begin{array}{l}
\quad *\\
\hline
\omega\geq0 \vdash 7\geq0\\
\hline
\omega\geq0 \vdash [d':=7]\,d'\geq0\\
\hline
d\geq0 \vdash [x'=y,y'=-\omega^2x-2d\omega y,d'=7\,\&\,\omega\geq0]\,d\geq0
\end{array}$$

increasingly damped oscillator

# Differential Cuts for Differential Equations

$$\begin{array}{c}
* \\ \hline
\omega\geq0\land d\geq0 \vdash 2\omega^2xy+2y(-\omega^2x-2d\omega y)\leq 0 \\ \hline
\omega\geq0\land d\geq0 \vdash [x':=y][y':=-\omega^2x-2d\omega y]\,2\omega^2xx'+2yy'\leq 0 \\ \hline
\omega^2x^2+y^2\leq c^2 \vdash [x'=y,y'=-\omega^2x-2d\omega y,d'=7\,\&\,\omega\geq0\land d\geq0]\,\omega^2x^2+y^2\leq c^2 \\ \hline
\omega^2x^2+y^2\leq c^2 \vdash [x'=y,y'=-\omega^2x-2d\omega y,d'=7\,\&\,\omega\geq0]\,\omega^2x^2+y^2\leq c^2
\end{array}$$

$$\begin{array}{c}
* \\ \hline
\omega\geq0 \vdash 7\geq0 \\ \hline
\omega\geq0 \vdash [d':=7]\,d'\geq0 \\ \hline
d\geq0 \vdash [x'=y,y'=-\omega^2x-2d\omega y,d'=7\,\&\,\omega\geq0]\,d\geq0
\end{array}$$

increasingly damped oscillator

# Differential Cuts for Differential Equations

$$\dfrac{\dfrac{\dfrac{\dfrac{*}{\omega\geq0\land d\geq0 \vdash 2\omega^2xy+2y(-\omega^2x-2d\omega y)\leq 0}}{\omega\geq0\land d\geq0 \vdash [x':=y][y':=-\omega^2x-2d\omega y]\,2\omega^2xx'+2yy'\leq 0}}{\omega^2x^2+y^2\leq c^2 \vdash [x'=y,y'=-\omega^2x-2d\omega y, d'=7\,\&\,\omega\geq0\land d\geq0]\,\omega^2x^2+y^2\leq c^2}}{\omega^2x^2+y^2\leq c^2 \vdash [x'=y,y'=-\omega^2x-2d\omega y, d'=7\,\&\,\omega\geq0]\,\omega^2x^2+y^2\leq c^2}$$

init

$$\dfrac{\dfrac{\dfrac{*}{\omega\geq0 \vdash 7\geq0}}{\omega\geq0 \vdash [d':=7]\,d'\geq0}}{d\geq0 \vdash [x'=y,y'=-\omega^2x-2d\omega y, d'=7\,\&\,\omega\geq0]\,d\geq0}$$

Could repeatedly diffcut in formulas to help the proof

# Differentials

**Syntax** $e ::= x \mid x' \mid c \mid e+k \mid e\cdot k \mid (e)'$

**Semantics** $\omega[\![(e)']\!] =$

# Differentials

**Syntax** $e ::= x \mid x' \mid c \mid e+k \mid e \cdot k \mid (e)'$

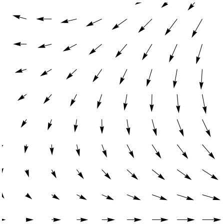
**Semantics**

$$\omega[\![(e)']\!] = \frac{\mathrm{d}\omega[\![e]\!]}{\mathrm{d}t}$$

# Differentials

**Syntax** $e ::= x \mid x' \mid c \mid e+k \mid e \cdot k \mid (e)'$

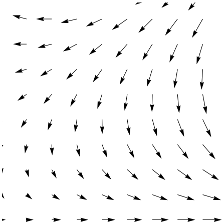
**Semantics** $\omega[\![(e)']\!] = \frac{\mathrm{d}\omega[\![e]\!]}{\mathrm{d}t}$ no time!



# Differential Forms

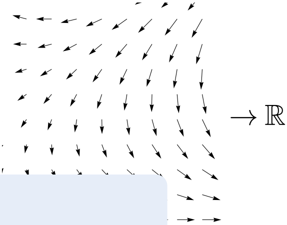
**Syntax** $e ::= x \mid x' \mid c \mid e+k \mid e\cdot k \mid (e)'$

**Semantics** $\omega[\![(e)']\!] = \sum_x \omega(x')\frac{\partial[\![e]\!]}{\partial x}(\omega)$



$\to \mathbb{R}$

# Differentials



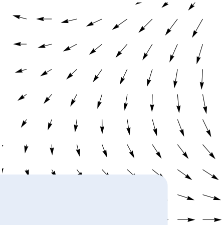
**Syntax** $e ::= x \mid x' \mid c \mid e+k \mid e \cdot k \mid (e)'$

**Semantics** $$\omega[\![(e)']\!] = \sum_x \omega(x') \frac{\partial [\![e]\!]}{\partial x}(\omega)$$

**Axioms**

$$\begin{aligned} (e+k)' &= (e)' + (k)' \\ (e \cdot k)' &= (e)' \cdot k + e \cdot (k)' \\ (c())' &= 0 && \text{for constants/numbers } c() \\ (x)' &= x' && \text{for variables } x \in \mathcal{V} \end{aligned}$$

# Differential Forms


$\to \mathbb{R}$

**Syntax**

$$e ::= x \mid x' \mid c \mid e+k \mid e\cdot k \mid (e)'$$

**Semantics**

$$\omega[\![(e)']\!] = \sum_x \omega(x')\frac{\partial[\![e]\!]}{\partial x}(\omega)$$

**Axioms**

$$(e+k)' = (e)' + (k)'$$

$$(e\cdot k)' = (e)'\cdot k + e\cdot (k)'$$

$$(c())' = 0 \qquad \text{for constants/numbers } c()$$

$$(x)' = x' \qquad \text{for variables } x \in \mathscr{V}$$

**ODE**

$$[\![x' = f(x)\,\&\,Q]\!] = \{(\varphi(0),\varphi(r)) : \varphi \models x' = f(x) \land Q$$
$$\text{for some } \varphi : [0,r] \to \mathscr{S}, \text{ some } r \in \mathbb{R}\}$$

$$\varphi(z)(x') = \frac{\mathrm{d}\varphi(t)(x)}{\mathrm{d}t}(z) \qquad \dots$$

# Differential Substitution Lemmas

**Lemma (Differential lemma)** (Differential value vs. Time-derivative)

*If* $\varphi \models x' = f(x) \land Q$ *for duration* $r>0$, *then for all* $0 \leq z \leq r$, $FV(e) \subseteq \{x\}$:

$$\varphi(z)[\![(e)']\!] = \frac{d\varphi(t)[\![e]\!]}{dt}(z)$$

**Lemma (Differential assignment)** (Effect on Differentials)

*If* $\varphi \models x' = f(x) \land Q$ *then* $\varphi \models P \leftrightarrow [x' := f(x)]P$

**Lemma (Derivations)** (Equations of Differentials)

$$(e+k)' = (e)' + (k)'$$

$$(e \cdot k)' = (e)' \cdot k + e \cdot (k)'$$

$$(c())' = 0 \qquad \textit{for constants/numbers } c()$$

$$(x)' = x' \qquad \textit{for variables } x \in \mathscr{V}$$

# Differential Substitution Lemmas

### Lemma (Differential lemma) (Differential value vs. Time-derivative)

*If* $\varphi \models x' = f(x) \land Q$ *for duration* $r>0$, *then for all* $0 \le z \le r$, $FV(e) \subseteq \{x\}$*:*

Syntactic

$$\varphi(z)[\![(e)']\!] = \frac{d\varphi(t)[\![e]\!]}{dt}(z)$$

Analytic

### Lemma (Differential assignment) (Effect on Differentials)

*If* $\varphi \models x' = f(x) \land Q$ *then* $\varphi \models P \leftrightarrow [x' := f(x)]P$

### Lemma (Derivations) (Equations of Differentials)

$$(e+k)' = (e)' + (k)'$$

$$(e \cdot k)' = (e)' \cdot k + e \cdot (k)'$$

$$(c())' = 0 \qquad \textit{for constants/numbers } c()$$

$$(x)' = x' \qquad \textit{for variables } x \in \mathscr{V}$$

# Differential Substitution Lemmas $\rightsquigarrow$ Proofs

**Lemma (Differential lemma)** (Differential value vs. Time-derivative)

*If* $\varphi \models x' = f(x) \land Q$ *for duration* $r>0$, *then for all* $0 \leq z \leq r$, $FV(e) \subseteq \{x\}$:

$$\varphi(z)[\![(e)']\!] = \frac{\mathrm{d}\varphi(t)[\![e]\!]}{\mathrm{d}t}(z)$$

**Lemma (Differential assignment)** (Effect on Differentials)

$$DE\ [x' = f(x)\,\&\,Q]P \leftrightarrow [x' = f(x)\,\&\,Q][x' := f(x)]P$$

**Lemma (Derivations)** (Equations of Differentials)

| | |
|---|---|
| $+'$ | $(e+k)' = (e)' + (k)'$ |
| $\cdot'$ | $(e \cdot k)' = (e)' \cdot k + e \cdot (k)'$ |
| $c'$ | $(c())' = 0$ |
| $x'$ | $(x)' = x'$ |

# Differential Substitution Lemmas $\rightsquigarrow$ Proofs

### Lemma (Differential lemma) (Differential value vs. Time-derivative)

*If* $\varphi \models x' = f(x) \land Q$ *for duration* $r>0$, *then for all* $0 \leq z \leq r$, $FV(e) \subseteq \{x\}$:

$$\varphi(z)[\![(e)']\!] = \frac{\mathrm{d}\varphi(t)[\![e]\!]}{\mathrm{d}t}(z)$$

### Lemma (Differential assignment) (Effect on Differentials)

*If* $\varphi \models x' = f(x) \land Q$ *then* $\varphi \models P \leftrightarrow [x' := f(x)]P$

### Axiomatics

DE $[x' = f(x) \,\&\, Q]P \leftrightarrow [x' = f(x) \,\&\, Q][x' := f(x)]P$

DI $\big([x' = f(x) \,\&\, Q]\, e \geq 0 \leftrightarrow [?Q]e \geq 0\big) \leftarrow [x' = f(x) \,\&\, Q]\, (e)' \geq 0$

# Differential Equation Axioms & Differential Axioms

DW $[x' = f(x) \,\&\, Q]Q$

DC $\big([x' = f(x) \,\&\, Q]P \leftrightarrow [x' = f(x) \,\&\, Q \land C]P\big) \leftarrow [x' = f(x) \,\&\, Q]C$

DE $[x' = f(x) \,\&\, Q]P \leftrightarrow [x' = f(x) \,\&\, Q][x' := f(x)]P$

DI $\big([x' = f(x) \,\&\, Q]P \leftrightarrow [?Q]P\big) \leftarrow [x' = f(x) \,\&\, Q](P)'$

DG $[x' = f(x) \,\&\, Q]P \leftrightarrow \exists y\, [x' = f(x), y' = a(x)y + b(x) \,\&\, Q]P$

DS $[x' = c() \,\&\, Q]P \leftrightarrow \forall t{\geq}0\, \big((\forall 0{\leq}s{\leq}t\, q(x{+}c()s)) \rightarrow [x := x{+}c()t]P\big)$

$+'$ $(e+k)' = (e)' + (k)'$

$\cdot'$ $(e\cdot k)' = (e)'\cdot k + e\cdot (k)'$

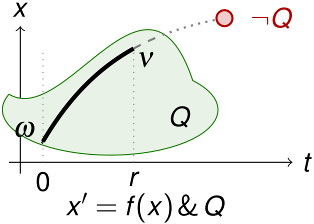
$\circ'$ $[y := g(x)][y' := 1]\big((f(g(x)))' = (f(y))' \cdot (g(x))'\big)$

JAR'17

# Differential Equation Axioms

## Axiom (Differential Weakening) (JAR'17)

DW $[x' = f(x) \,\&\, Q]Q$



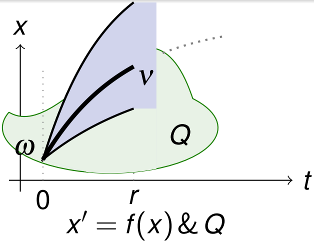
Differential equations cannot leave their evolution domains. Implies:

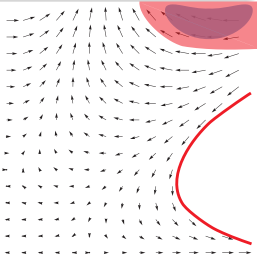
$$[x' = f(x) \,\&\, Q]P \leftrightarrow [x' = f(x) \,\&\, Q]\big(Q \to P\big)$$

# Differential Equation Axioms

**Axiom (Differential Cut)** (JAR'17)

DC $\big([x' = f(x) \,\&\, Q]P \leftrightarrow [x' = f(x) \,\&\, Q \land C]P\big)$
$\leftarrow [x' = f(x) \,\&\, Q]C$



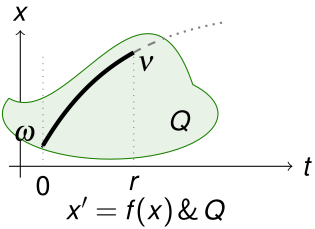


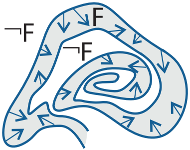
DC is a cut for differential equations.
DC is a differential modal modus ponens K.
Can't leave $C$, then might as well restrict state space to $C$.

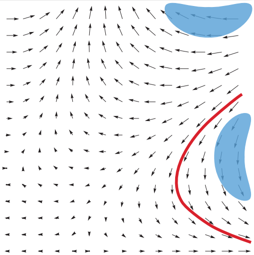
# Differential Equation Axioms

**Axiom (Differential Invariant)** (JAR'17)

DI $\big([x' = f(x)\,\&\,Q]P \leftrightarrow [?Q]P\big) \leftarrow [x' = f(x)\,\&\,Q](P)'$







Differential invariant: if $P$ true now and differential $(P)'$ true always

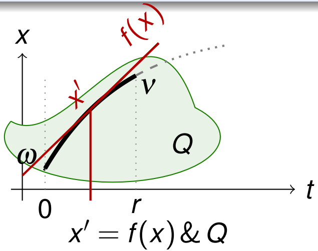
What's the differential of a formula???

What's the meaning of a differential term . . . in a state???

# Differential Equation Axioms

**Axiom (Differential Effect)** (JAR'17)

DE $[x' = f(x) \& Q]P \leftrightarrow [x' = f(x) \& Q][x' := f(x)]P$



Effect of differential equation on differential symbol $x'$

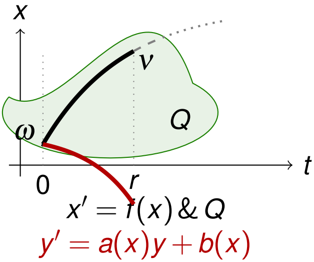
$[x' := f(x)]$ instantly mimics continuous effect $[x' = f(x)]$ on $x'$

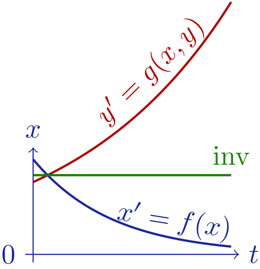
$[x' := f(x)]$ selects vector field $x' = f(x)$ for subsequent differentials

# Differential Equation Axioms

**Axiom (Differential Ghost)** (JAR'17)

DG $[x' = f(x) \,\&\, Q]P \leftrightarrow \exists y\, [x' = f(x), y' = a(x)y + b(x) \,\&\, Q]P$





Differential ghost/auxiliaries: extra differential equations that exist

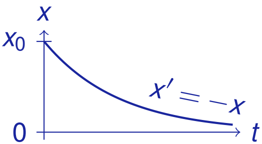
Can cause new invariants

"Dark matter" counterweight to balance conserved quantities

# Example: Differential Ghosts

**Example (▶ Differential ghost proof)**

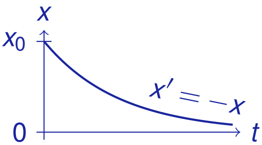
$$\text{DG}\;\frac{}{x > 0 \vdash [x' = -x]\, x > 0}$$



# Example: Differential Ghosts

## Example (▸ Differential ghost proof)

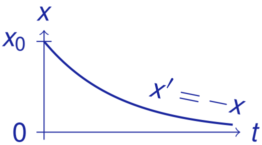
$$\text{DG}\;\dfrac{\text{MR}\;\dfrac{}{x > 0 \vdash \exists y\,[x' = -x, y' = \text{☁}]\,x > 0}}{x > 0 \vdash [x' = -x]\,x > 0}$$



# Example: Differential Ghosts

## Example (▸ Differential ghost proof)

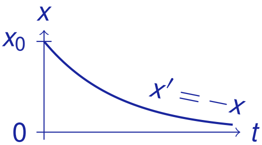
$$\text{DG}\;\dfrac{\text{MR}\;\dfrac{\mathbb{R}\;\dfrac{}{xy^2=1 \vdash x>0} \qquad \exists\text{R,cut}\;\dfrac{}{x>0 \vdash \exists y\,[x'=-x, y'=\text{☁}]\,xy^2=1}}{x>0 \vdash \exists y\,[x'=-x, y'=\text{☁}]\,x>0}}{x>0 \vdash [x'=-x]\,x>0}$$



# Example: Differential Ghosts

## Example (Differential ghost proof)

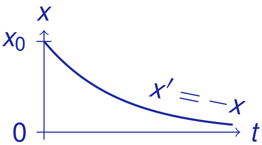
$$\text{DG}\;\dfrac{\text{MR}\;\dfrac{\mathbb{R}\;\dfrac{*}{xy^2{=}1 \vdash x{>}0} \qquad \exists\text{R,cut}\;\dfrac{}{x > 0 \vdash \exists y\,[x' = -x, y' = \text{☁}]\, xy^2 = 1}}{x > 0 \vdash \exists y\,[x' = -x, y' = \text{☁}]\, x > 0}}{x > 0 \vdash [x' = -x]\, x > 0}$$



# Example: Differential Ghosts

## Example (Differential ghost proof)

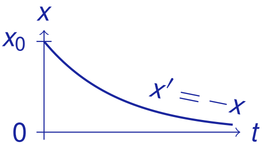
$$\text{DG}\;\dfrac{\text{MR}\;\dfrac{\mathbb{R}\;\dfrac{*}{xy^2{=}1 \vdash x{>}0} \qquad \exists\text{R,cut}\;\dfrac{\text{dI}\;\dfrac{}{xy^2{=}1 \vdash [x' = -x, y' = \text{☁}]\, xy^2 = 1}}{x > 0 \vdash \exists y\, [x' = -x, y' = \text{☁}]\, xy^2 = 1}}{x > 0 \vdash \exists y\, [x' = -x, y' = \text{☁}]\, x > 0}}{x > 0 \vdash [x' = -x]\, x > 0}$$



# Example: Differential Ghosts

## Example (Differential ghost proof)

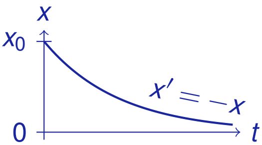
$$\text{DG}\ \cfrac{\text{MR}\ \cfrac{\mathbb{R}\ \cfrac{*}{xy^2{=}1 \vdash x{>}0} \qquad \exists\text{R,cut}\ \cfrac{\text{dI}\ \cfrac{[{:=}]\ \cfrac{}{\vdash [x'{:=}{-x}][y'{:=}\text{☁}]\,x'y^2 + x2yy' = 0}}{xy^2{=}1 \vdash [x' = -x, y' = \text{☁}]\,xy^2 = 1}}{x > 0 \vdash \exists y\,[x' = -x, y' = \text{☁}]\,xy^2 = 1}}{x > 0 \vdash \exists y\,[x' = -x, y' = \text{☁}]\,x > 0}}{x > 0 \vdash [x' = -x]\,x > 0}$$



# Example: Differential Ghosts

## Example (▸ Differential ghost proof)

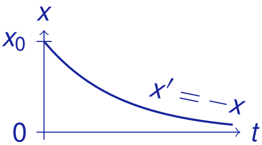
$$
\text{DG}\,\dfrac{\text{MR}\,\dfrac{\mathbb{R}\,\dfrac{*}{xy^2=1 \vdash x>0} \qquad \exists\text{R,cut}\,\dfrac{\text{dI}\,\dfrac{[:=]\,\dfrac{\mathbb{R}\,\dfrac{}{\vdash -xy^2+2xy\text{☁}=0}}{\vdash [x':=-x][y':=\text{☁}]x'y^2+x2yy'=0}}{xy^2=1 \vdash [x'=-x,y'=\text{☁}]\,xy^2=1}}{x>0 \vdash \exists y\,[x'=-x,y'=\text{☁}]\,xy^2=1}}{x>0 \vdash \exists y\,[x'=-x,y'=\text{☁}]\,x>0}}{x>0 \vdash [x'=-x]\,x>0}
$$



# Example: Differential Ghosts

## Example (Differential ghost proof)

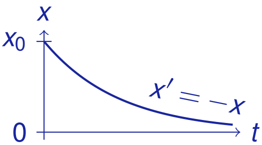
$$\text{DG}\;\dfrac{\text{MR}\;\dfrac{\mathbb{R}\,\dfrac{*}{xy^2{=}1 \vdash x{>}0} \qquad \exists\text{R,cut}\;\dfrac{\text{dI}\;\dfrac{[:=]\;\dfrac{\mathbb{R}\;\dfrac{*}{\vdash -xy^2+2xy\text{☁}=0}}{\vdash [x'{:=}{-x}][y'{:=}\text{☁}]x'y^2+x2yy'=0}}{xy^2{=}1 \vdash [x'=-x, y'=\text{☁}]\,xy^2=1}}{x>0 \vdash \exists y\,[x'=-x, y'=\text{☁}]\,xy^2=1}}{x>0 \vdash \exists y\,[x'=-x, y'=\text{☁}]\,x>0}}{x>0 \vdash [x'=-x]\,x>0}$$



# Example: Differential Ghosts

## Example (Differential ghost proof)

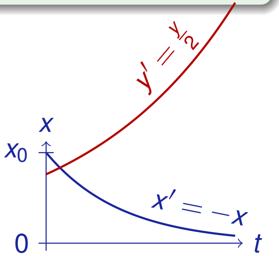
$$\text{DG}\,\dfrac{\text{MR}\,\dfrac{\mathbb{R}\,\dfrac{*}{xy^2{=}1 \vdash x{>}0} \qquad \exists\text{R,cut}\,\dfrac{\text{dI}\,\dfrac{[:=]\,\dfrac{\mathbb{R}\,\dfrac{*}{\vdash -xy^2+2xy\frac{y}{2} \quad =0}}{\vdash [x'{:=}{-x}][y'{:=}\frac{y}{2} \quad ]x'y^2+x2yy'=0}}{xy^2{=}1 \vdash [x'=-x,y'=\frac{y}{2} \quad ]xy^2=1}}{x>0 \vdash \exists y\,[x'=-x,y'=\frac{y}{2} \quad ]xy^2=1}}{x>0 \vdash \exists y\,[x'=-x,y'=\frac{y}{2} \quad ]x>0}}{x>0 \vdash [x'=-x]x>0}$$



# Example: Differential Ghosts

### Example (▸ Differential ghost proof)

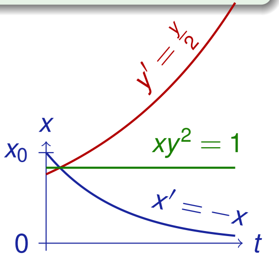
$$\dfrac{\dfrac{*}{xy^2{=}1 \vdash x{>}0}\,\mathbb{R} \qquad \dfrac{\dfrac{\dfrac{\dfrac{*}{\vdash -xy^2+2xy\frac{y}{2}=0}\,\mathbb{R}}{\vdash [x':=-x][y':=\frac{y}{2}]x'y^2+x2yy'=0}\,[:=]}{xy^2{=}1 \vdash [x'=-x,y'=\frac{y}{2}]\,xy^2=1}\,\text{dI}}{x>0 \vdash \exists y\,[x'=-x,y'=\frac{y}{2}]\,xy^2=1}\,\exists\text{R,cut}}{\dfrac{x>0 \vdash \exists y\,[x'=-x,y'=\frac{y}{2}]\,x>0}{x>0 \vdash [x'=-x]\,x>0}\,\text{DG}}\,\text{MR}$$



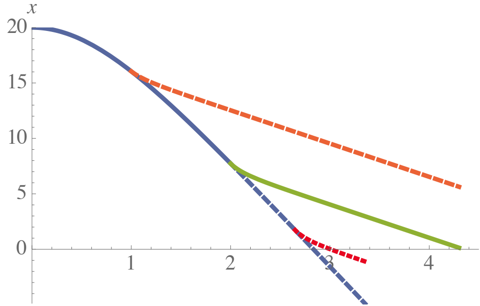
# Example: Differential Ghosts

## Example (Differential ghost proof)

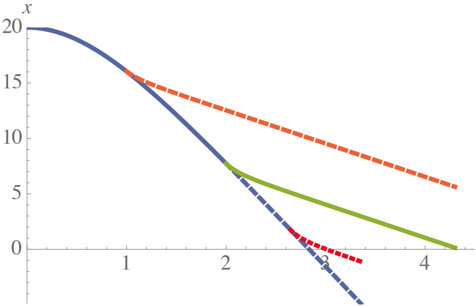
$$\text{DG}\;\dfrac{\text{MR}\;\dfrac{\mathbb{R}\;\dfrac{*}{xy^2{=}1 \vdash x{>}0} \qquad \exists\text{R,cut}\;\dfrac{\text{dI}\;\dfrac{[:=]\;\dfrac{\mathbb{R}\;\dfrac{*}{\vdash -xy^2+2xy\frac{y}{2} = 0}}{\vdash [x'{:=}{-x}][y'{:=}\frac{y}{2}]x'y^2+x2yy'=0}}{xy^2{=}1 \vdash [x'=-x,y'=\frac{y}{2}]\,xy^2=1}}{x>0 \vdash \exists y\,[x'=-x,y'=\frac{y}{2}]\,xy^2=1}}{x>0 \vdash \exists y\,[x'=-x,y'=\frac{y}{2}]\,x>0}}{x>0 \vdash [x'=-x]\,x>0}$$



# Ex: Parachute Open or Keep Closed



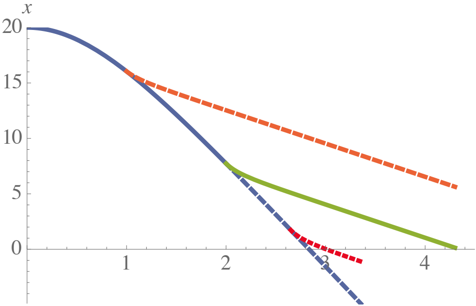
# Ex: Parachute Open or Keep Closed



**Example (Parachute)**

$$\big((?(Q \wedge r = a) \cup r := p); t := 0;$$
$$\{x' = v, v' = -g + rv^2, t' = 1 \,\&\, t \leq T \wedge x \geq 0 \wedge v < 0\}\big)^*$$

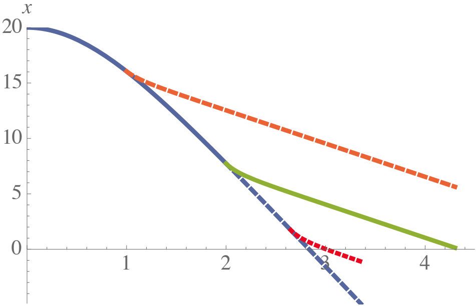
# Ex: Parachute Open or Keep Closed



**Example (▸ Parachute)**

$$\to\Big[\Big(\big(?(Q\land r=a)\cup r:=p\big);t:=0;$$
$$\{x'=v,v'=-g+rv^2,t'=1\,\&\,t\le T\land x\ge 0\land v<0\}\Big)^*\Big]$$
$$(x=0\to v\ge m)$$

# Ex: Parachute Open or Keep Closed



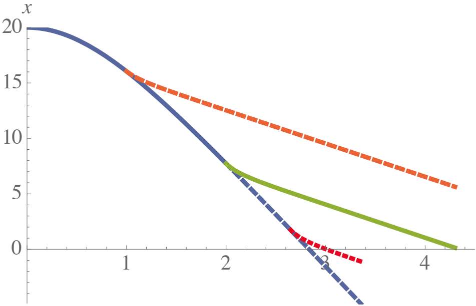
**Example (▸ Parachute)**

$$\rightarrow \Big[\Big(\big(?(Q \land r = a) \cup r := p\big); t := 0;$$
$$\{x' = v, v' = -g + rv^2, t' = 1 \,\&\, t \leq T \land x \geq 0 \land v < 0\}\Big)^*\Big]$$
$$(x = 0 \rightarrow v \geq m)$$

# Ex: Parachute Open or Keep Closed

$$Q \equiv v - gT > -\sqrt{g/p}$$

Conservatively bounded next velocity above parachute's limit velocity.



## Example (▸ Parachute)

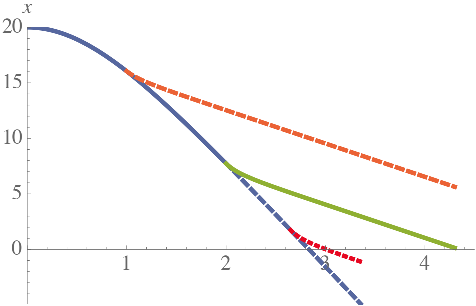
$$m < -\sqrt{g/p} \rightarrow \Big[\Big(\big(?(Q \land r = a) \cup r := p\big); t := 0;$$
$$\{x' = v, v' = -g + rv^2, t' = 1 \,\&\, t \le T \land x \ge 0 \land v < 0\}\Big)^*\Big]$$
$$(x = 0 \rightarrow v \ge m)$$

# Ex: Parachute Open or Keep Closed

$$Q \equiv v - gT > -\sqrt{g/p}$$

Conservatively bounded next velocity above parachute's limit velocity.
Limit by differential ghost:

$$y' = -\frac{p}{2}(v - \sqrt{g/p}) \quad y^2\underbrace{(v + \sqrt{g/p})}_{>0} = 1$$



## Example (▶ Parachute)

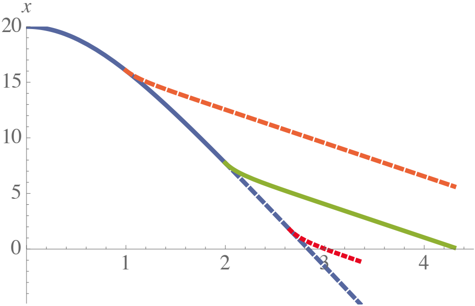
$$m < -\sqrt{g/p} \rightarrow \Big[\Big(\big(?(Q \land r = a) \cup r := p\big); t := 0;$$
$$\{x' = v, v' = -g + rv^2, t' = 1 \,\&\, t \le T \land x \ge 0 \land v < 0\}\Big)^*\Big]$$
$$(x = 0 \rightarrow v \ge m)$$

# Ex: Parachute Open or Keep Closed

$$Q \equiv v - gT > -\sqrt{g/p}$$

Conservatively bounded next velocity above parachute's limit velocity. Limit by differential ghost:

$$y' = -\frac{p}{2}(v - \sqrt{g/p}) \quad y^2(\underbrace{v + \sqrt{g/p}}_{>0}) = 1$$



$v \geq \text{old}(v) - gt$ if closed

## Example ( ▸ Parachute)

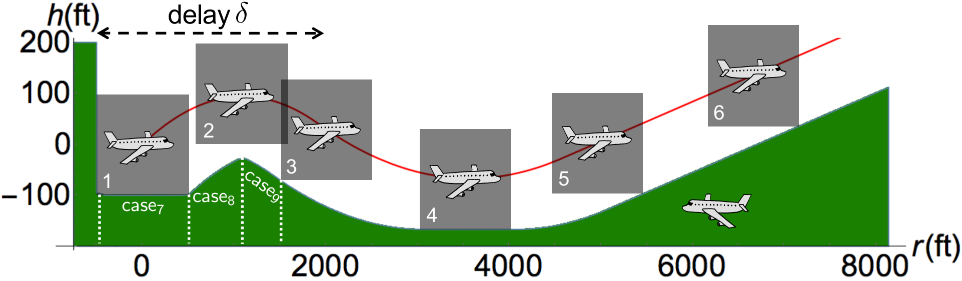
$$m < -\sqrt{g/p} \to \Big[\Big(\big(?(Q \land r = a) \cup r := p\big); t := 0; \{x' = v, v' = -g + rv^2, t' = 1 \,\&\, t \leq T \land x \geq 0 \land v < 0\}\Big)^*\Big] (x = 0 \to v \geq m)$$

# Outline (CPS Application Highlights)

1. CPS are Multi-Dynamical Systems
   - Hybrid Systems / Games / Stochastic / Distributed Hybrid Systems
2. Differential Dynamic Logic
   - Syntax
   - Semantics
   - Example: Car Control Design
3. Dynamic Axioms for Dynamical Systems
   - Axiomatics
   - Example: Safe Car Control
   - Soundness and Completeness
4. Differential Invariants for Differential Equations
   - Differential Axioms
   - Example: Differential Ghosts
5. **Applications**
6. Summary

# Airborne Collision Avoidance System ACAS X: Verify

- Developed by the FAA to replace current TCAS in aircraft
- Approximately optimizes Markov Decision Process on a grid
- Advisory from lookup tables with numerous 5D interpolation regions

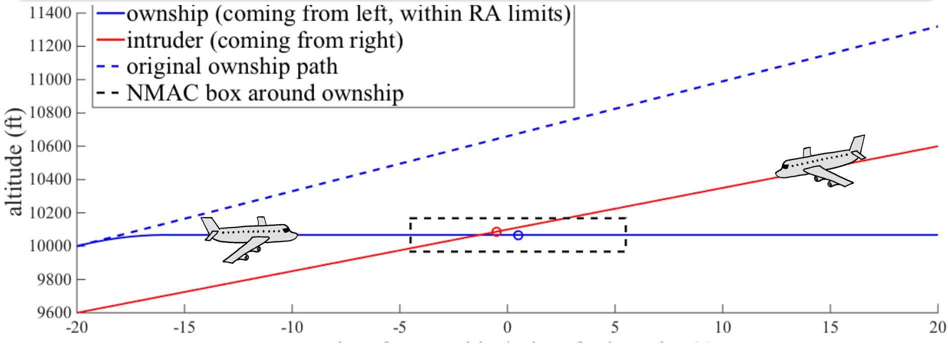


1. Identified safe region for each advisory symbolically
2. Proved safety for hybrid systems flight model in KeYmaera X

STTT'17

# Airborne Collision Avoidance System ACAS X: Compare

ACAS X table comparison shows safe advisory in 97.7% of the 648,591,384,375 states compared (15,160,434,734 counterexamples).

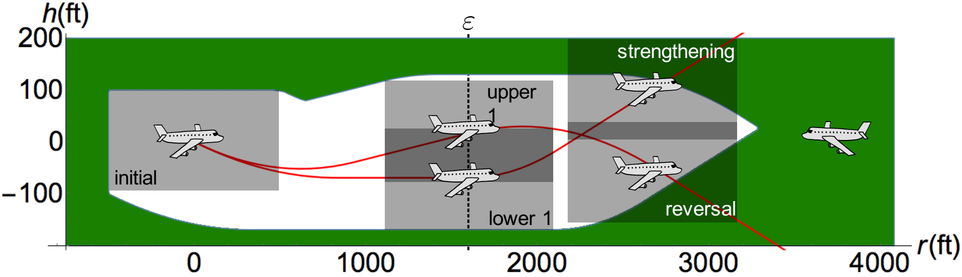


ACAS X issues DNC advisory, which induces collision unless corrected

STTT'17

# Airborne Collision Avoidance System ACAS X: Refine

- Conservative, so too many counterexamples
- Settle for: safe for a little while, with safe future advisory possibility
- Safeable advisory: a subsequent advisory can safely avoid collision

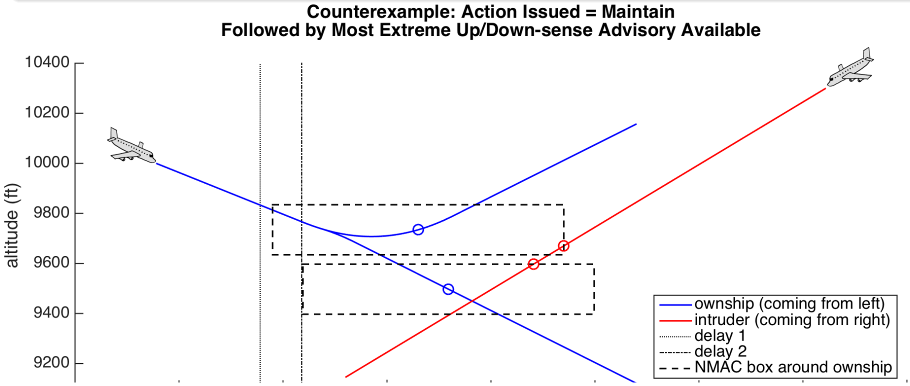


1. Identified safeable region for each advisory symbolically
2. Proved safety for hybrid systems flight model in KeYmaera X

STTT'17

# Airborne Collision Avoidance System ACAS X: Compare

ACAS X table comparison shows safeable advisory in more of the 648,591,384,375 states compared (≈899 $10^6$ counterexamples).

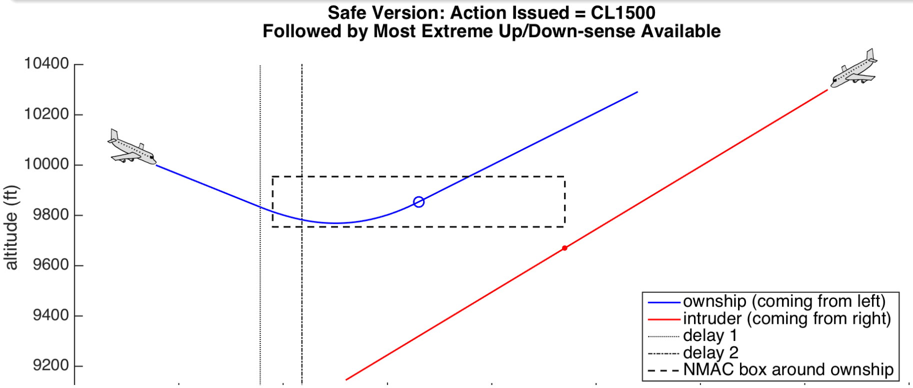


ACAS X issues Maintain advisory instead of CL1500

STTT'17

# Airborne Collision Avoidance System ACAS X: Compare

ACAS X table comparison shows safeable advisory in more of the 648,591,384,375 states compared ($\approx$899 $10^6$ counterexamples).

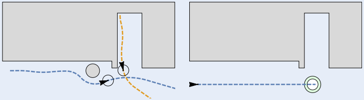


ACAS X issues Maintain advisory instead of CL1500

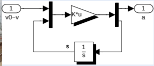
STTT'17

# Application Highlights

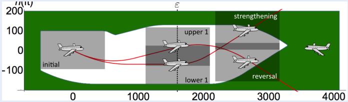
## Obstacle Avoidance + Ground Navigation



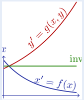
## Train Control Brakes



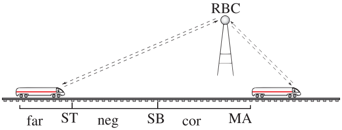
## Airborne Collision Avoidance (ACAS X)

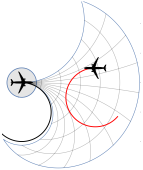


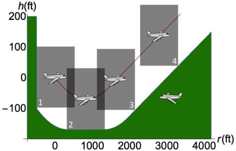
## Ship Cooling

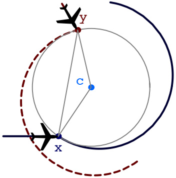


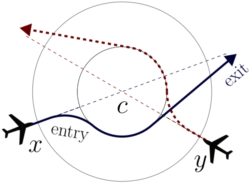
# Verified CPS Applications: Trains & Airplanes

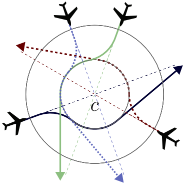


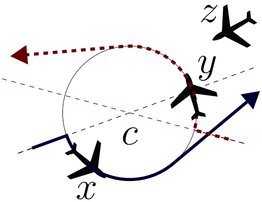


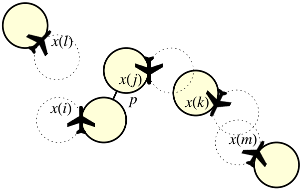


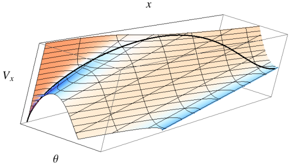






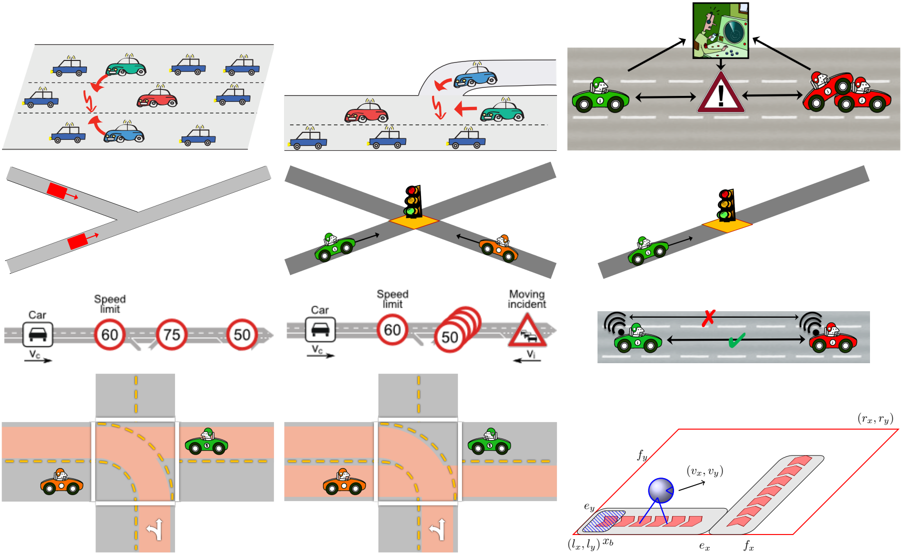






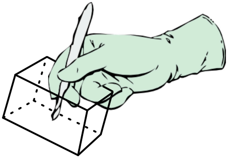
EM’09,JAIS’14,TACAS’15,EMSOFT’15,FM’09,HSCC’11,HSCC’13,TACAS’14, RSSRail’17

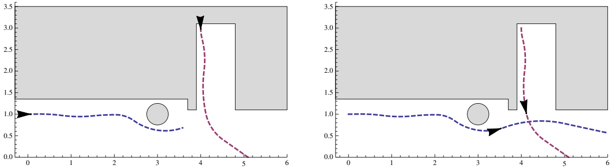
# Verified CPS Applications: Cars

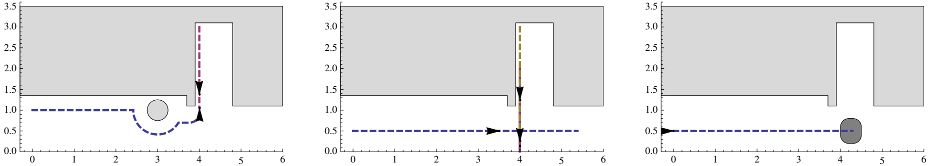


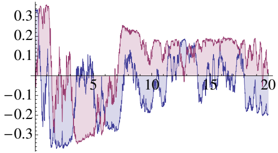
FM’11,LMCS’12,ICCPS’12,ITSC’11,ITSC’13,IJCAR’12

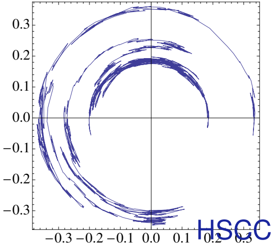
# Verified CPS Applications: Robots

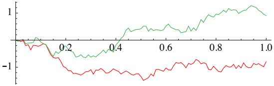






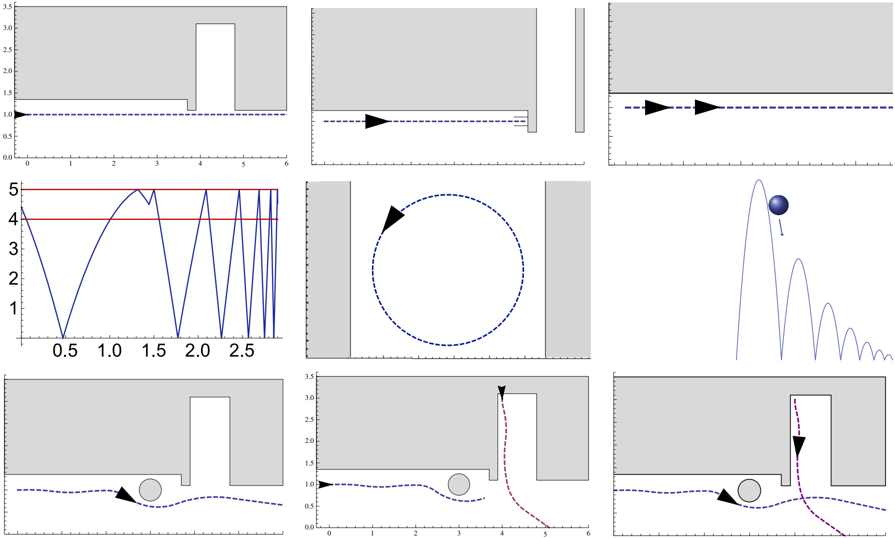






HSCC'13,RSS'13,CADE'12, IJRR'17

# Verified CPS Applications: lfcps.org/course/

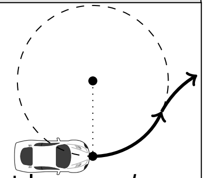


undergrads in *Foundations of Cyber-Physical Systems* course

# KeYmaera X aXiomatic Tactical Theorem Prover for CPS

Proof search →

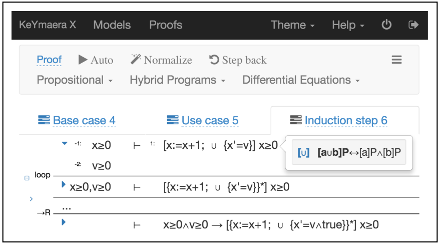
**Model**



ctrl: $a := -b$;

plant: $x'' = a$

## KeYmaera X



-1: $x \geq 0$ ⊢ 1: $[x:=x+1; \cup \{x'=v\}]\, x \geq 0$

-2: $v \geq 0$

[∪] $[a \cup b]P \leftrightarrow [a]P \wedge [b]P$

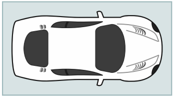
loop $x \geq 0, v \geq 0 \vdash [\{x:=x+1; \cup \{x'=v\}\}^*]\, x \geq 0$

→R ...

$\vdash x \geq 0 \wedge v \geq 0 \rightarrow [\{x:=x+1; \cup \{x'=v \wedge true\}\}^*]\, x \geq 0$

**generates proofs**

ModelPlex proof →



Model Safety

Compliance Monitor

### Trustworthy

Uniform substitution

Sound & complete

Small core: 1700 LOC

### Flexible

Proof automation

Interactive UI

Programmable

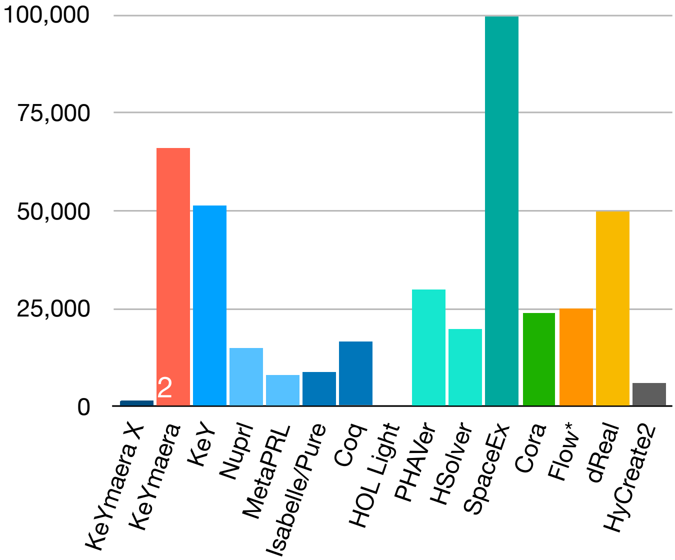
### Customizable

Scala+Java API

Command line

REST API

# KeYmaera X Small Kernel for Soundness 1 700 LOC



Disclaimer: Self-reported estimates of the soundness-critical lines of code + rules

# Outline (Dynamic Logic for Dynamical Systems)

1. CPS are Multi-Dynamical Systems
   - Hybrid Systems / Games / Stochastic / Distributed Hybrid Systems
2. Differential Dynamic Logic
   - Syntax
   - Semantics
   - Example: Car Control Design
3. Dynamic Axioms for Dynamical Systems
   - Axiomatics
   - Example: Safe Car Control
   - Soundness and Completeness
4. Differential Invariants for Differential Equations
   - Differential Axioms
   - Example: Differential Ghosts
5. Applications
6. **Summary**

# Acknowledgments

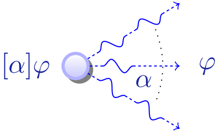
Logical Systems Lab at Carnegie Mellon University
Yong Kiam Tan, Brandon Bohrer, Nathan Fulton, Sarah Loos
Stefan Mitsch, Khalil Ghorbal, Jean-Baptiste Jeannin, Andrew Sogokon

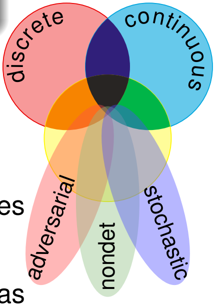
# Dynamic Logic for Dynamical Systems

Logical foundations make a big difference for CPS, and vice versa

**differential dynamic logic**

$\mathsf{dL} = \mathsf{DL} + \mathsf{HP}$





- Strong analytic foundations
- Practical reasoning advances
- Significant applications
- Catalyze many science areas

1. Multi-dynamical systems
2. Combine simple dynamics
3. Tame complexity
4. Complete axiomatization

Numerous wonders remain to be discovered

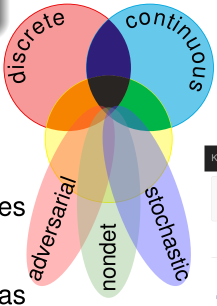
# Dynamic Logic for Dynamical Systems

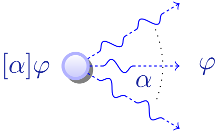
Logical foundations make a big difference for CPS, and vice versa

**differential dynamic logic**

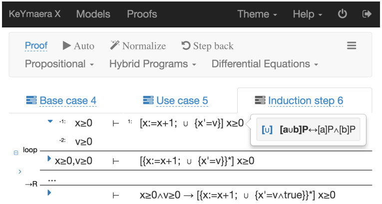
$$\mathsf{dL} = \mathsf{DL} + \mathsf{HP}$$

- Strong analytic foundations
- Practical reasoning advances
- Significant applications
- Catalyze many science areas





## KeYmaera X



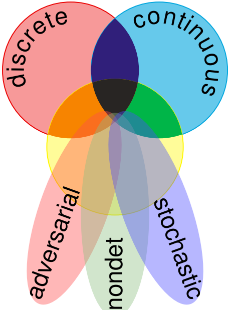
```
-1: x≥0   ⊢ 1: [x:=x+1; ∪ {x'=v}] x≥0
-2: v≥0
x≥0,v≥0   ⊢ [{x:=x+1; ∪ {x'=v}}*] x≥0
...
          ⊢ x≥0∧v≥0 → [{x:=x+1; ∪ {x'=v∧true}}*] x≥0
```

Numerous wonders remain to be discovered

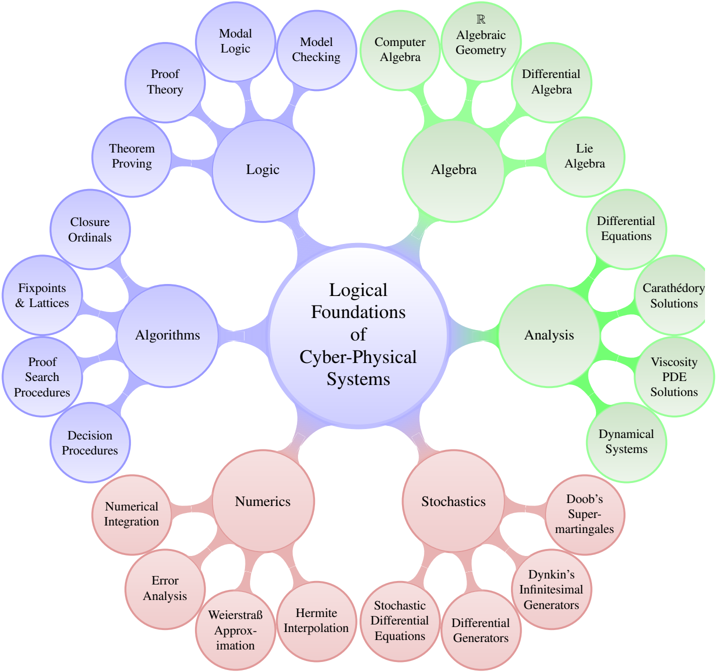
# Future CPS Challenges

Numerous wonders remain to be discovered

- Scalable continuous stochastics CADE'11
- Concurrent CPS
- Real arithmetic: Scalable and verified CADE'09
- Verified CPS implementations, ModelPlex FMSD'16
- Correct CPS execution
- CPS-conducive tactic languages+libraries ITP'17
- Tactics exploiting CPS structure/linearity/...
- Invariant generation FMSD'09 TACAS'14
- Tactics & proofs for reachable set computations
- Parallel proof search & disprovers
- Correct model transformation FM'14
- Inspiring applications



CPSs deserve proofs as safety evidence!



Logical Foundations of Cyber-Physical Systems

Logic
- Modal Logic
- Model Checking
- Proof Theory
- Theorem Proving

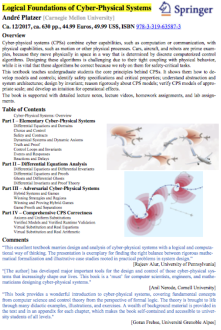
Algebra
- Computer Algebra
- ℝ Algebraic Geometry
- Differential Algebra
- Lie Algebra

Analysis
- Differential Equations
- Carathéodory Solutions
- Viscosity PDE Solutions
- Dynamical Systems

Stochastics
- Doob's Super-martingales
- Dynkin's Infinitesimal Generators
- Differential Generators
- Stochastic Differential Equations

Numerics
- Numerical Integration
- Error Analysis
- Weierstraß Approx-imation
- Hermite Interpolation

Algorithms
- Closure Ordinals
- Fixpoints & Lattices
- Proof Search Procedures
- Decision Procedures



**Logical Foundations of Cyber-Physical Systems** Springer

**André Platzer** [Carnegie Mellon University]

**Ca. 12/2017, ca. 630 pp., 44.99 Euros, 49.99 US$, ISBN 978-3-319-63587-3**

**Overview**

Cyber-physical systems (CPSs) combine cyber capabilities, such as computation or communication, with physical capabilities, such as motion or other physical processes. Cars, aircraft, and robots are prime examples, because they move physically in space in a way that is determined by discrete computerized control algorithms. Designing these algorithms is challenging due to their tight coupling with physical behavior, while it is vital that these algorithms be correct because we rely on them for safety-critical tasks.

This textbook teaches undergraduate students the core principles behind CPSs. It shows them how to develop models and controls; identify safety specifications and critical properties; understand abstraction and system architectures; design by invariant; reason rigorously about CPS models; verify CPS models of appropriate scale; and develop an intuition for operational effects.

The book is supported with detailed lecture notes, lecture videos, homework assignments, and lab assignments.

**Table of Contents**

Cyber-Physical Systems: Overview
**Part I – Elementary Cyber-Physical Systems**
Differential Equations and Domains
Choice and Control
Safety and Contracts
Dynamical Systems and Dynamic Axioms
Truth and Proof
Control Loops and Invariants
Events and Responses
Reactions and Delays
**Part II – Differential Equations Analysis**
Differential Equations and Differential Invariants
Differential Equations and Proofs
Ghosts and Differential Ghosts
Differential Invariants and Proof Theory
**Part III – Adversarial Cyber-Physical Systems**
Hybrid Systems and Games
Winning Strategies and Regions
Winning and Proving Hybrid Games
Game Proofs and Separations
**Part IV – Comprehensive CPS Correctness**
Axioms and Uniform Substitutions
Verified Models and Verified Runtime Validation
Virtual Substitution and Real Equations
Virtual Substitution and Real Arithmetic

**Comments**

"This excellent textbook marries design and analysis of cyber-physical systems with a logical and computational way of thinking. The presentation is exemplary for finding the right balance between rigorous mathematical formalization and illustrative case studies rooted in practical problems in system design."

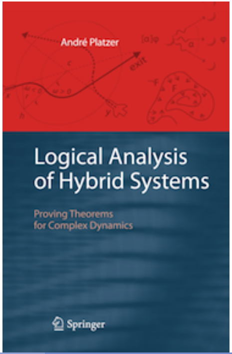
[Rajeev Alur, University of Pennsylvania]

"[The author] has developed major important tools for the design and control of those cyber-physical systems that increasingly shape our lives. This book is a 'must' for computer scientists, engineers, and mathematicians designing cyber-physical systems."

[Anil Nerode, Cornell University]

"This book provides a wonderful introduction to cyber-physical systems, covering fundamental concepts from computer science and control theory from the perspective of formal logic. The theory is brought to life through many didactic examples, illustrations, and exercises. A wealth of background material is provided in the text and in an appendix for each chapter, which makes the book self-contained and accessible to university students of all levels."

[Goran Frehse, Université Grenoble Alpes]



André Platzer

Logical Analysis of Hybrid Systems

Proving Theorems for Complex Dynamics

Springer

# Outline

7 Differential Invariant Soundness Proof

- Differential Radical Invariants

# Differential Substitution Lemmas

**Lemma (Differential lemma)** (Differential value vs. Time-derivative)

*If* $\varphi \models x' = f(x) \land Q$ *for duration* $r>0$*, then for all* $0\leq z\leq r$, $FV(e) \subseteq \{x\}$:

Syntactic $$\varphi(z)[\![(e)']\!] = \frac{\mathrm{d}\varphi(t)[\![e]\!]}{\mathrm{d}t}(z)$$ Analytic

**Lemma (Differential assignment)** (Effect on Differentials)

*If* $\varphi \models x' = f(x) \land Q$ *then* $\varphi \models P \leftrightarrow [x' := f(x)]P$

**Lemma (Derivations)** (Equations of Differentials)

$$\begin{aligned}
(e+k)' &= (e)' + (k)' && \\
(e\cdot k)' &= (e)'\cdot k + e\cdot (k)' && \\
(c())' &= 0 && \textit{for constants/numbers } c() \\
(x)' &= x' && \textit{for variables } x \in \mathscr{V}
\end{aligned}$$

# Soundness Proof

**Lemma (Differential lemma)** (Differential value vs. Time-derivative)

*If* $\varphi \models x' = f(x) \land Q$ *for duration* $r>0$*, then for all* $0 \le z \le r$*,* $FV(e) \subseteq \{x\}$*:*

$$\varphi(z)[\![(e)']\!] = \frac{\mathrm{d}\varphi(t)[\![e]\!]}{\mathrm{d}t}(z)$$

**Semantics**

$$\omega[\![(e)']\!] = \sum_x \omega(x') \frac{\partial [\![e]\!]}{\partial x}(\omega)$$

**Definition (Hybrid program semantics)** $([\![\cdot]\!] : \mathrm{HP} \to \wp(\mathscr{S} \times \mathscr{S}))$

$$[\![x' = f(x) \,\&\, Q]\!] = \{(\varphi(0), \varphi(r)) : \varphi(z) \models x' = f(x) \land Q \text{ for all } 0 \le z \le r$$
$$\text{for a } \varphi : [0, r] \to \mathscr{S} \text{ where } \varphi(z)(x') \overset{\text{def}}{=} \frac{\mathrm{d}\varphi(t)(x)}{\mathrm{d}t}(z)\}$$

# Soundness Proof

**Lemma (Differential lemma)** (Differential value vs. Time-derivative)

*If* $\varphi \models x' = f(x) \land Q$ *for duration* $r>0$*, then for all* $0\leq z\leq r$*,* $FV(e) \subseteq \{x\}$*:*

$$\varphi(z)[\![(e)']\!] = \frac{\mathrm{d}\varphi(t)[\![e]\!]}{\mathrm{d}t}(z)$$

$$\frac{\mathrm{d}\varphi(t)[\![e]\!]}{\mathrm{d}t}(z)$$

Semantics

$$\omega[\![(e)']\!] = \sum_x \omega(x')\frac{\partial [\![e]\!]}{\partial x}(\omega)$$

**Definition (Hybrid program semantics)** $([\![\cdot]\!] : \mathrm{HP} \to \wp(\mathscr{S} \times \mathscr{S}))$

$$[\![x' = f(x) \,\&\, Q]\!] = \{(\varphi(0), \varphi(r)) : \varphi(z) \models x' = f(x) \land Q \text{ for all } 0\leq z\leq r$$
$$\text{for a } \varphi : [0,r] \to \mathscr{S} \text{ where } \varphi(z)(x') \overset{\text{def}}{=} \frac{\mathrm{d}\varphi(t)(x)}{\mathrm{d}t}(z)\}$$

# Soundness Proof

**Lemma (Differential lemma)** (Differential value vs. Time-derivative)

*If* $\varphi \models x' = f(x) \land Q$ *for duration* $r>0$*, then for all* $0 \le z \le r$, $FV(e) \subseteq \{x\}$*:*

$$\varphi(z)[\![(e)']\!] = \frac{d\varphi(t)[\![e]\!]}{dt}(z)$$

$$\frac{d\varphi(t)[\![e]\!]}{dt}(z) \overset{\text{chain}}{=} \sum_x \frac{\partial [\![e]\!]}{\partial x}(\varphi(z)) \frac{d\varphi(t)(x)}{dt}(z)$$

Semantics

$$\omega[\![(e)']\!] = \sum_x \omega(x') \frac{\partial [\![e]\!]}{\partial x}(\omega)$$

**Definition (Hybrid program semantics)** ($[\![\cdot]\!] : \text{HP} \to \wp(\mathscr{S} \times \mathscr{S})$)

$$[\![x' = f(x) \,\&\, Q]\!] = \{(\varphi(0), \varphi(r)) : \varphi(z) \models x' = f(x) \land Q \text{ for all } 0 \le z \le r$$

$$\text{for a } \varphi : [0, r] \to \mathscr{S} \text{ where } \varphi(z)(x') \overset{\text{def}}{=} \frac{d\varphi(t)(x)}{dt}(z)\}$$

# Soundness Proof

**Lemma (Differential lemma)** (Differential value vs. Time-derivative)

*If* $\varphi \models x' = f(x) \land Q$ *for duration* $r>0$*, then for all* $0\le z\le r$, $FV(e) \subseteq \{x\}$:

$$\varphi(z)[\![(e)']\!] = \frac{d\varphi(t)[\![e]\!]}{dt}(z)$$

$$\frac{d\varphi(t)[\![e]\!]}{dt}(z) \overset{\text{chain}}{=} \sum_x \frac{\partial [\![e]\!]}{\partial x}(\varphi(z)) \frac{d\varphi(t)(x)}{dt}(z)$$

**Semantics**

$$\omega[\![(e)']\!] = \sum_x \omega(x') \frac{\partial [\![e]\!]}{\partial x}(\omega)$$

**Definition (Hybrid program semantics)** ($[\![\cdot]\!] : \mathrm{HP} \to \wp(\mathcal{S} \times \mathcal{S})$)

$$[\![x' = f(x) \,\&\, Q]\!] = \{(\varphi(0),\varphi(r)) : \varphi(z) \models x' = f(x) \land Q \text{ for all } 0\le z\le r$$
$$\text{for a } \varphi : [0,r] \to \mathcal{S} \text{ where } \varphi(z)(x') \overset{\text{def}}{=} \frac{d\varphi(t)(x)}{dt}(z)\}$$

# Soundness Proof

**Lemma (Differential lemma)** (Differential value vs. Time-derivative)

*If* $\varphi \models x' = f(x) \land Q$ *for duration* $r>0$*, then for all* $0\le z\le r$, $FV(e) \subseteq \{x\}$:

$$\varphi(z)[\![(e)']\!] = \frac{d\varphi(t)[\![e]\!]}{dt}(z)$$

$$\frac{d\varphi(t)[\![e]\!]}{dt}(z) \overset{\text{chain}}{=} \sum_x \frac{\partial[\![e]\!]}{\partial x}(\varphi(z))\frac{d\varphi(t)(x)}{dt}(z) = \sum_x \frac{\partial[\![e]\!]}{\partial x}(\varphi(z))\varphi(z)(x')$$

Semantics

$$\omega[\![(e)']\!] = \sum_x \omega(x')\frac{\partial[\![e]\!]}{\partial x}(\omega)$$

**Definition (Hybrid program semantics)** $([\![\cdot]\!] : \mathrm{HP} \to \wp(\mathscr{S}\times\mathscr{S}))$

$[\![x' = f(x) \,\&\, Q]\!] = \{(\varphi(0),\varphi(r)) : \varphi(z) \models x' = f(x) \land Q$ for all $0\le z\le r$
for a $\varphi : [0,r] \to \mathscr{S}$ where $\varphi(z)(x') \overset{\text{def}}{=} \frac{d\varphi(t)(x)}{dt}(z)\}$

# Soundness Proof

**Lemma (Differential lemma)** (Differential value vs. Time-derivative)

*If* $\varphi \models x' = f(x) \land Q$ *for duration* $r>0$*, then for all* $0 \le z \le r$*,* $FV(e) \subseteq \{x\}$*:*

$$\varphi(z)[\![(e)']\!] = \frac{\mathrm{d}\varphi(t)[\![e]\!]}{\mathrm{d}t}(z)$$

$$\frac{\mathrm{d}\varphi(t)[\![e]\!]}{\mathrm{d}t}(z) \overset{\text{chain}}{=} \sum_x \frac{\partial [\![e]\!]}{\partial x}(\varphi(z)) \frac{\mathrm{d}\varphi(t)(x)}{\mathrm{d}t}(z) = \sum_x \frac{\partial [\![e]\!]}{\partial x}(\varphi(z))\varphi(z)(x')$$

**Semantics**

$$\varphi(z)[\![(e)']\!] = \sum_x \varphi(z)(x') \frac{\partial [\![e]\!]}{\partial x}(\varphi(z))$$

**Definition (Hybrid program semantics)** ($[\![\cdot]\!] : \mathrm{HP} \to \wp(\mathscr{S} \times \mathscr{S})$)

$$[\![x' = f(x) \,\&\, Q]\!] = \{(\varphi(0), \varphi(r)) : \varphi(z) \models x' = f(x) \land Q \text{ for all } 0 \le z \le r$$
$$\text{for a } \varphi : [0,r] \to \mathscr{S} \text{ where } \varphi(z)(x') \overset{\text{def}}{=} \frac{\mathrm{d}\varphi(t)(x)}{\mathrm{d}t}(z)\}$$

# Differential Radical Invariants

## Theorem (Differential radical invariant characterization)

$$\frac{h = 0 \rightarrow \bigwedge_{i=1}^{N-1} h_p^{(i)} = 0}{h = 0 \rightarrow [x' = p]h = 0}$$

*characterizes **all** algebraic invariants, where* $N = ord \sqrt[\prime]{(h)}$*, i.e.*

$$h_p^{(N)} = \sum_{i=0}^{N-1} g_i h_p^{(i)} \quad (g_i \in \mathbb{R}[x]) \quad h_p^{(i+1)} = [x' {:=} p](h_p^{(i)})'$$

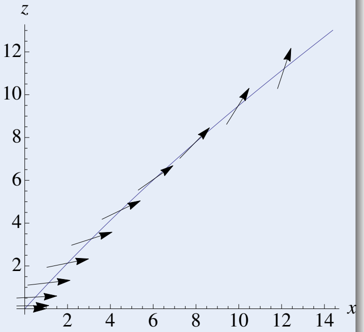
## Corollary (Algebraic Invariants Decidable)

*Algebraic invariants of algebraic differential equations are decidable.*

# Example: Longitudinal Dynamics of an Airplane

## Study (6th Order Longitudinal Flight Equations)

| | |
|---|---|
| $u' = \frac{X}{m} - g\sin(\theta) - qw$ | axial velocity |
| $w' = \frac{Z}{m} + g\cos(\theta) + qu$ | vertical velocity |
| $x' = \cos(\theta)u + \sin(\theta)w$ | range |
| $z' = -\sin(\theta)u + \cos(\theta)w$ | altitude |
| $\theta' = q$ | pitch angle |
| $q' = \frac{M}{I_{yy}}$ | pitch rate |



$X$ : thrust along $u$
$Z$ : thrust along $w$
$M$ : thrust moment for $w$
$g$ : gravity
$m$ : mass
$I_{yy}$ : inertia second diagonal

with Khalil Ghorbal TACAS'14

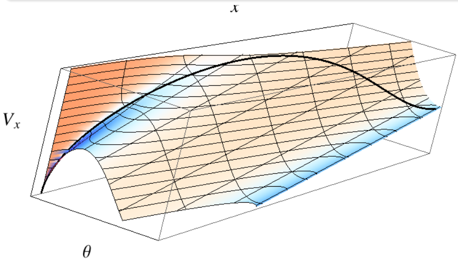
# Case Study: Longitudinal Dynamics of an Airplane

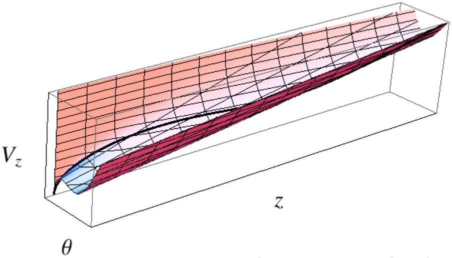
### Result (DRI Automatically Generates Invariant Functions)

$$\frac{Mz}{I_{yy}} + g\theta + \left(\frac{X}{m} - qw\right)\cos(\theta) + \left(\frac{Z}{m} + qu\right)\sin(\theta)$$

$$\frac{Mx}{I_{yy}} - \left(\frac{Z}{m} + qu\right)\cos(\theta) + \left(\frac{X}{m} - qw\right)\sin(\theta)$$

$$-q^2 + \frac{2M\theta}{I_{yy}}$$





with Khalil Ghorbal TACAS'14

André Platzer.
Logic & proofs for cyber-physical systems.
In Nicola Olivetti and Ashish Tiwari, editors, *IJCAR*, volume 9706 of *LNCS*, pages 15–21, Cham, 2016. Springer.
doi:10.1007/978-3-319-40229-1_3.

André Platzer.
Logics of dynamical systems.
In LICS [29], pages 13–24.
doi:10.1109/LICS.2012.13.

André Platzer.
*Logical Foundations of Cyber-Physical Systems*.
Springer, Cham, 2018.
URL: http://www.springer.com/978-3-319-63587-3,
doi:10.1007/978-3-319-63588-0.

André Platzer.
Differential dynamic logic for hybrid systems.
*J. Autom. Reas.*, 41(2):143–189, 2008.
doi:10.1007/s10817-008-9103-8.

📄 André Platzer.
A complete uniform substitution calculus for differential dynamic logic.
*J. Autom. Reas.*, 59(2):219–265, 2017.
`doi:10.1007/s10817-016-9385-1`.

📄 André Platzer.
Differential game logic.
*ACM Trans. Comput. Log.*, 17(1):1:1–1:51, 2015.
`doi:10.1145/2817824`.

📄 André Platzer.
Differential hybrid games.
*ACM Trans. Comput. Log.*, 18(3):19:1–19:44, 2017.
`doi:10.1145/3091123`.

📄 André Platzer.
The complete proof theory of hybrid systems.
In LICS [29], pages 541–550.
`doi:10.1109/LICS.2012.64`.

📄 André Platzer.

A complete axiomatization of quantified differential dynamic logic for distributed hybrid systems.
*Log. Meth. Comput. Sci.*, 8(4:17):1–44, 2012.
Special issue for selected papers from CSL'10.
`doi:10.2168/LMCS-8(4:17)2012`.

André Platzer.
Stochastic differential dynamic logic for stochastic hybrid programs.
In Nikolaj Bjørner and Viorica Sofronie-Stokkermans, editors, *CADE*, volume 6803 of *LNCS*, pages 446–460, Berlin, 2011. Springer.
`doi:10.1007/978-3-642-22438-6_34`.

André Platzer.
A uniform substitution calculus for differential dynamic logic.
In Felty and Middeldorp [30], pages 467–481.
`doi:10.1007/978-3-319-21401-6_32`.

Nathan Fulton, Stefan Mitsch, Jan-David Quesel, Marcus Völp, and André Platzer.
KeYmaera X: An axiomatic tactical theorem prover for hybrid systems.
In Felty and Middeldorp [30], pages 527–538.

doi:10.1007/978-3-319-21401-6_36.

- Stefan Mitsch and André Platzer.
  ModelPlex: Verified runtime validation of verified cyber-physical system models.
  *Form. Methods Syst. Des.*, 49(1-2):33–74, 2016.
  Special issue of selected papers from RV'14.
  doi:10.1007/s10703-016-0241-z.

- Stefan Mitsch, Khalil Ghorbal, David Vogelbacher, and André Platzer.
  Formal verification of obstacle avoidance and navigation of ground robots.
  *I. J. Robotics Res.*, 36(12):1312–1340, 2017.
  doi:10.1177/0278364917733549.

- André Platzer and Jan-David Quesel.
  European Train Control System: A case study in formal verification.
  In Karin Breitman and Ana Cavalcanti, editors, *ICFEM*, volume 5885 of *LNCS*, pages 246–265, Berlin, 2009. Springer.
  doi:10.1007/978-3-642-10373-5_13.

📄 Stefan Mitsch, Marco Gario, Christof J. Budnik, Michael Golm, and André Platzer.
Formal verification of train control with air pressure brakes.
In Alessandro Fantechi, Thierry Lecomte, and Alexander Romanovsky, editors, *RSSRail*, volume 10598 of *LNCS*, pages 173–191. Springer, 2017.
`doi:10.1007/978-3-319-68499-4_12`.

📄 Jean-Baptiste Jeannin, Khalil Ghorbal, Yanni Kouskoulas, Aurora Schmidt, Ryan Gardner, Stefan Mitsch, and André Platzer.
A formally verified hybrid system for safe advisories in the next-generation airborne collision avoidance system.
*STTT*, 19(6):717–741, 2017.
`doi:10.1007/s10009-016-0434-1`.

📄 André Platzer.
Differential-algebraic dynamic logic for differential-algebraic programs.
*J. Log. Comput.*, 20(1):309–352, 2010.
`doi:10.1093/logcom/exn070`.

📄 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.
`doi:10.1007/s10703-009-0079-8`.

André Platzer.
The structure of differential invariants and differential cut elimination.
*Log. Meth. Comput. Sci.*, 8(4:16):1–38, 2012.
`doi:10.2168/LMCS-8(4:16)2012`.

André Platzer.
A differential operator approach to equational differential invariants.
In Lennart Beringer and Amy Felty, editors, *ITP*, volume 7406 of *LNCS*, pages 28–48, Berlin, 2012. Springer.
`doi:10.1007/978-3-642-32347-8_3`.

André Platzer and Yong Kiam Tan.
Differential equation axiomatization: The impressive power of differential ghosts.
In Anuj Dawar and Erich Grädel, editors, *LICS*, pages 819–828, New York, 2018. ACM.

doi:10.1145/3209108.3209147.

André Platzer, Jan-David Quesel, and Philipp Rümmer.
Real world verification.
In Renate A. Schmidt, editor, *CADE*, volume 5663 of *LNCS*, pages 485–501, Berlin, 2009. Springer.
doi:10.1007/978-3-642-02959-2_35.

Nathan Fulton, Stefan Mitsch, Brandon Bohrer, and André Platzer.
Bellerophon: Tactical theorem proving for hybrid systems.
In Mauricio Ayala-Rincón and César A. Muñoz, editors, *ITP*, volume 10499 of *LNCS*, pages 207–224. Springer, 2017.
doi:10.1007/978-3-319-66107-0_14.

André Platzer.
*Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics*.
Springer, Heidelberg, 2010.
URL: http://www.springer.com/978-3-642-14508-7, doi:10.1007/978-3-642-14509-4.

Khalil Ghorbal and André Platzer.

Characterizing algebraic invariants by differential radical invariants.
In Erika Ábrahám and Klaus Havelund, editors, *TACAS*, volume 8413 of *LNCS*, pages 279–294, Berlin, 2014. Springer.
`doi:10.1007/978-3-642-54862-8_19`.

Thomas A. Henzinger.
The theory of hybrid automata.
In *LICS*, pages 278–292, Los Alamitos, 1996. IEEE Computer Society.
`doi:10.1109/LICS.1996.561342`.

Jennifer M. Davoren and Anil Nerode.
Logics for hybrid systems.
*IEEE*, 88(7):985–1010, 2000.
`doi:10.1109/5.871305`.

*Logic in Computer Science (LICS), 2012 27th Annual IEEE Symposium on*, Los Alamitos, 2012. IEEE.

Amy Felty and Aart Middeldorp, editors.
*International Conference on Automated Deduction, CADE'15, Berlin, Germany, Proceedings*, volume 9195 of *LNCS*, Berlin, 2015. Springer.
`doi:10.1007/978-3-319-21401-6`.