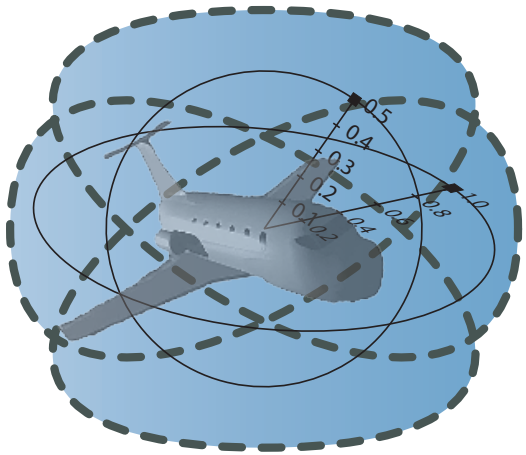
Foundations of Cyber-Physical Systems

André Platzer

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



Outline

Outline

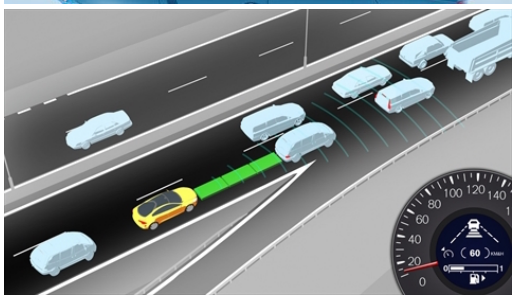
CPSs Promise Transformative Impact!

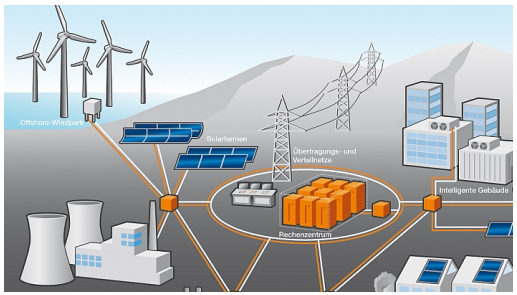
Prospects: Safe & Efficient

Driver assistance
Autonomous cars

Pilot decision support
Autopilots / UAVs

Train protection
Robots help people





Prerequisite: CPS need to be safe

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

Can you trust a computer to control physics?

Can you trust a computer to control physics?

Rationale

1. Safety guarantees require analytic foundations.
2. Foundations revolutionized digital computer science & our society.
3. Need even stronger foundations when software reaches out into our physical world.

Cyber-physical Systems

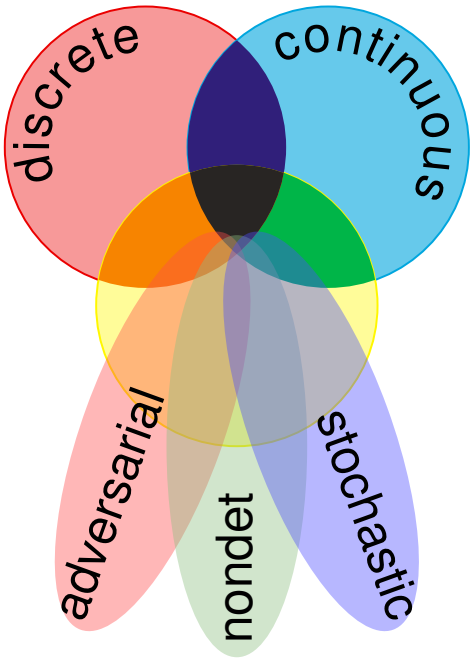
CPS combine cyber capabilities with physical capabilities to solve problems that neither part could solve alone.

How can we provide people with cyber-physical systems they can bet their lives on?
— Jeannette Wing

CPSs are Multi-Dynamical Systems

CPS Dynamics

CPS are characterized by multiple facets of dynamical systems.



CPS Compositions

CPS combine multiple simple dynamical effects.

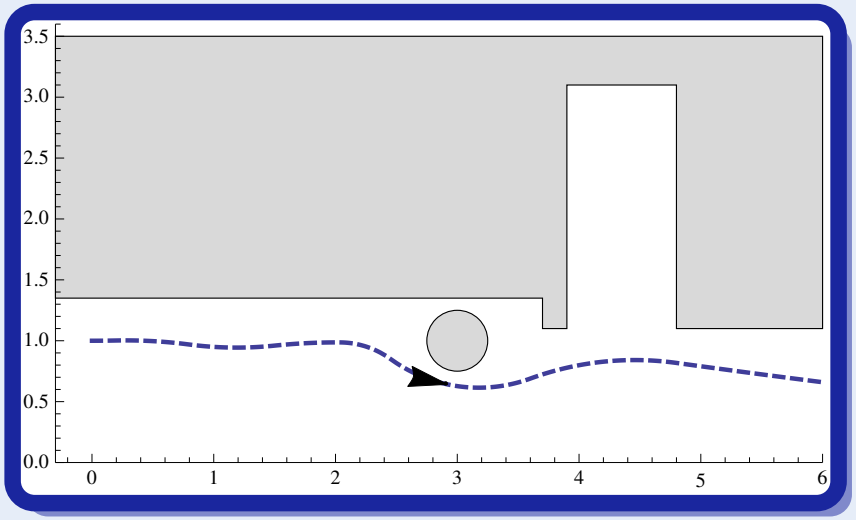
Tame Parts

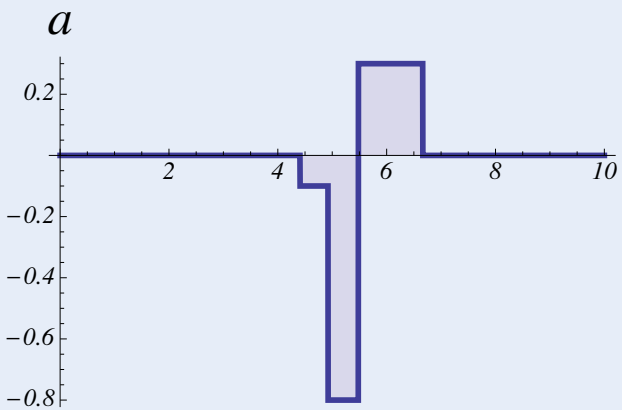
Exploiting compositionality tames CPS complexity.

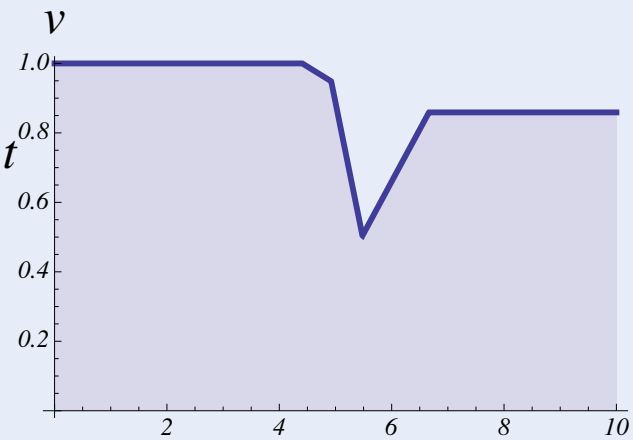
Challenge (Hybrid Systems)

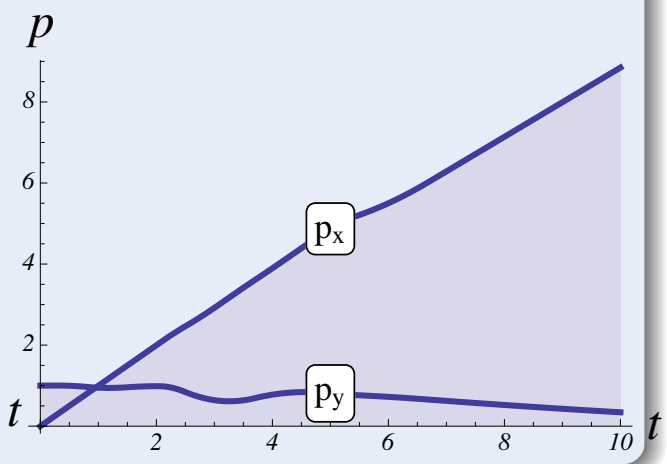
Fixed rule describing state evolution with both

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





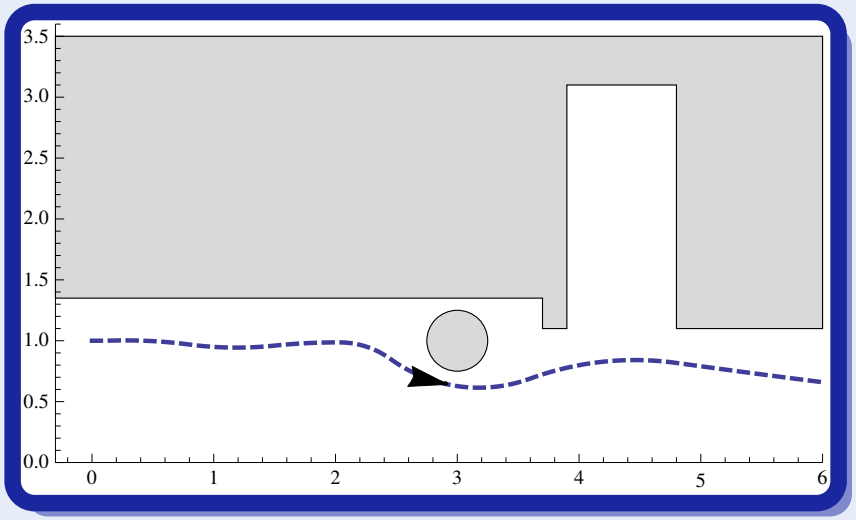


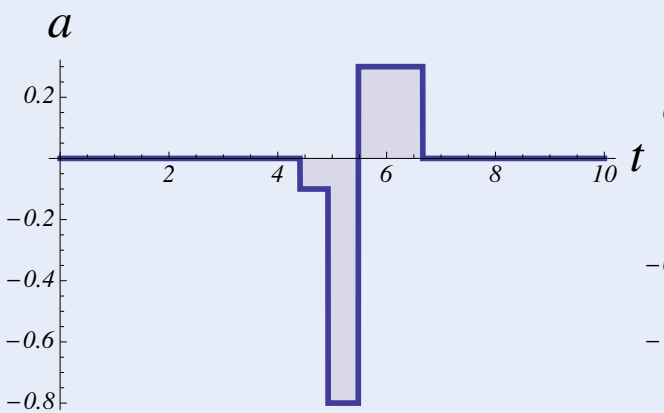


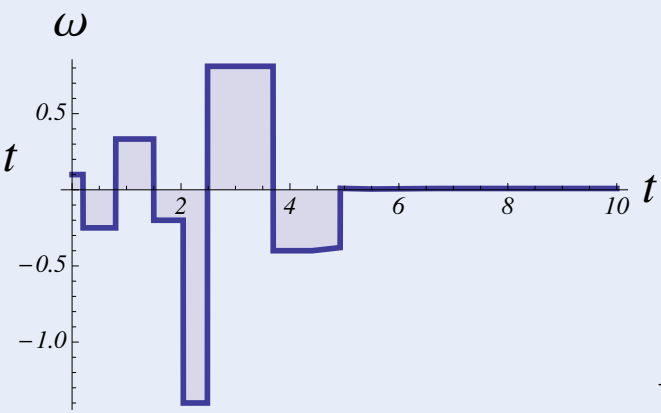
Challenge (Hybrid Systems)

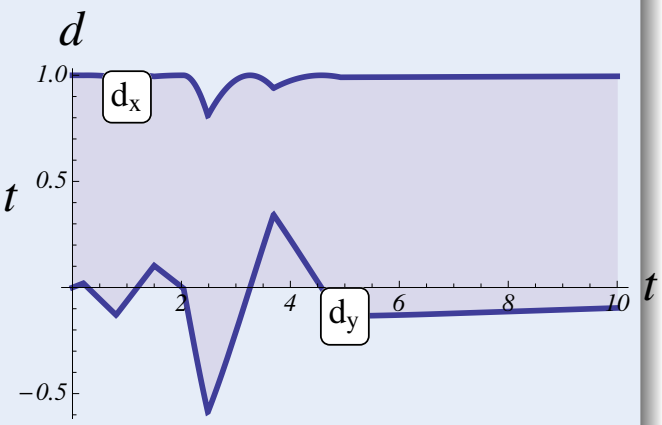
Fixed rule describing state evolution with both

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





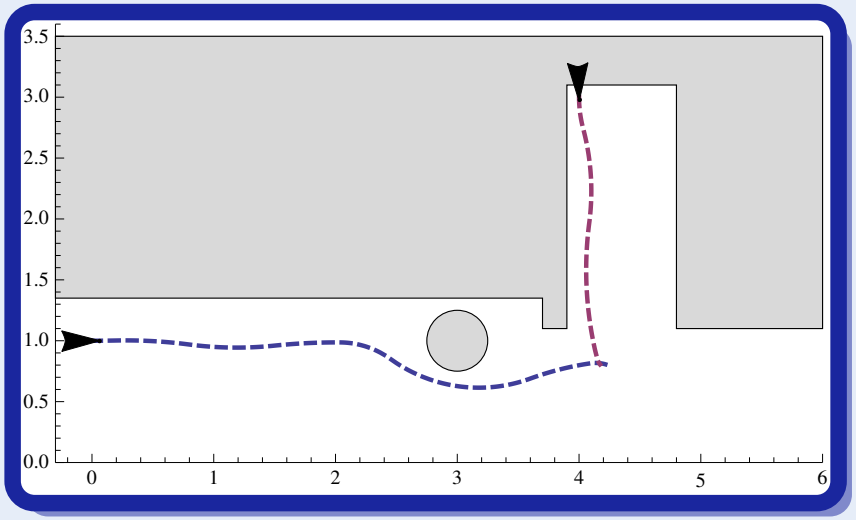


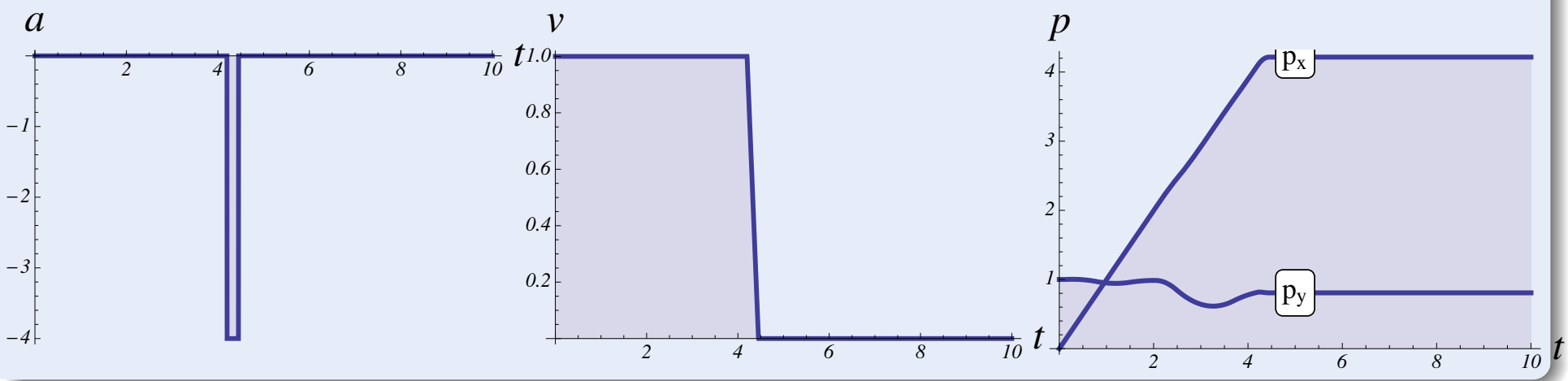


Challenge (Hybrid Systems)

Fixed rule describing state evolution with both

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

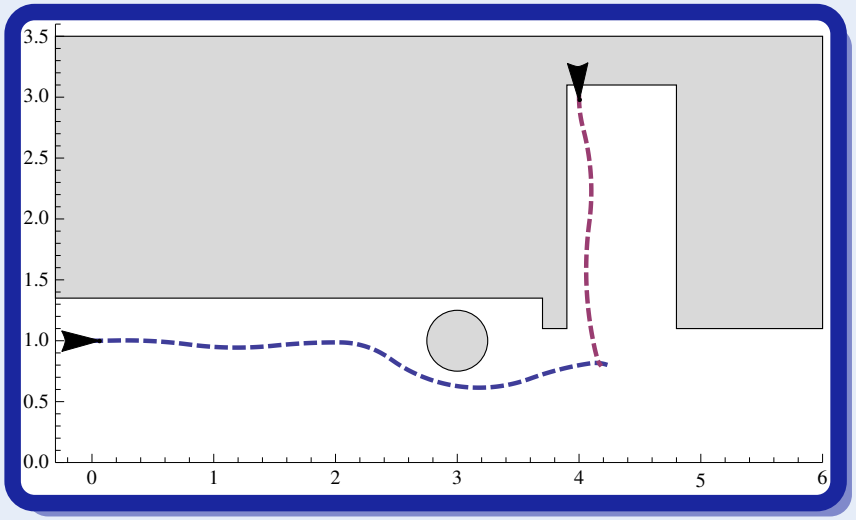


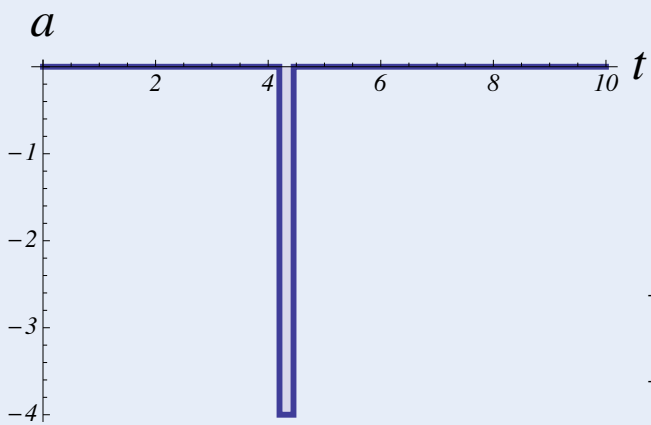


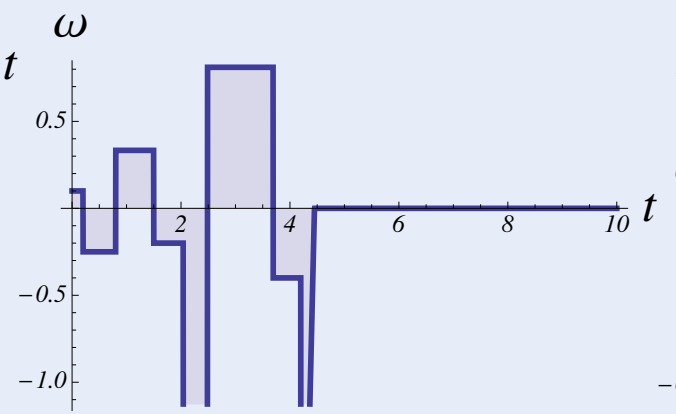
Challenge (Hybrid Systems)

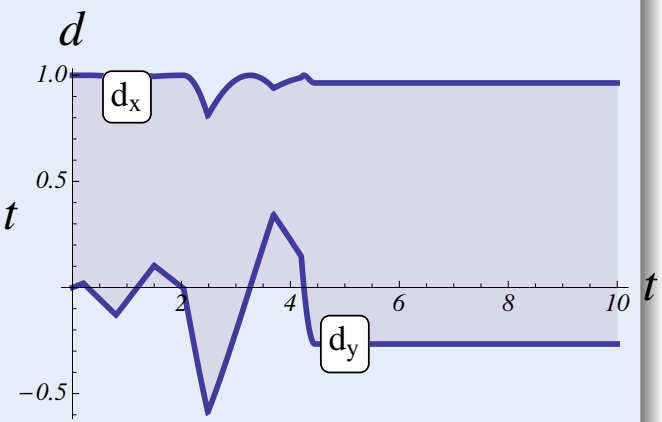
Fixed rule describing state evolution with both

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





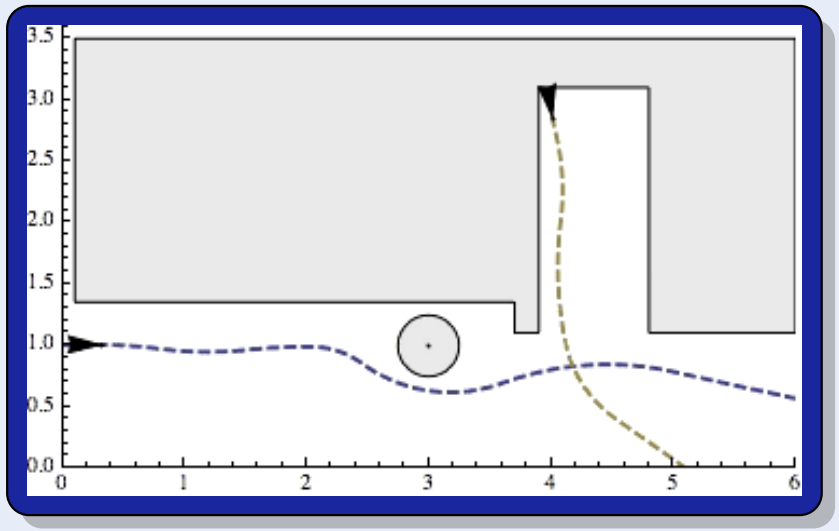


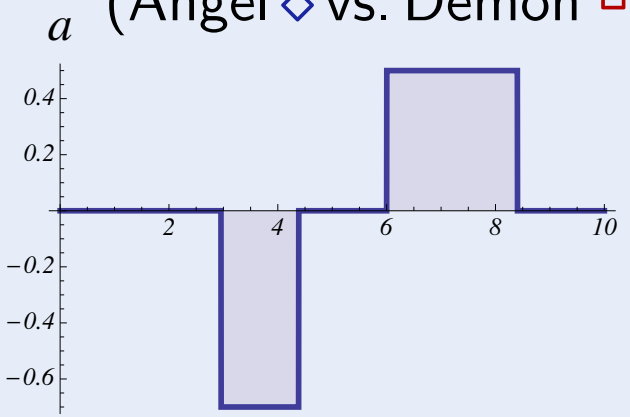


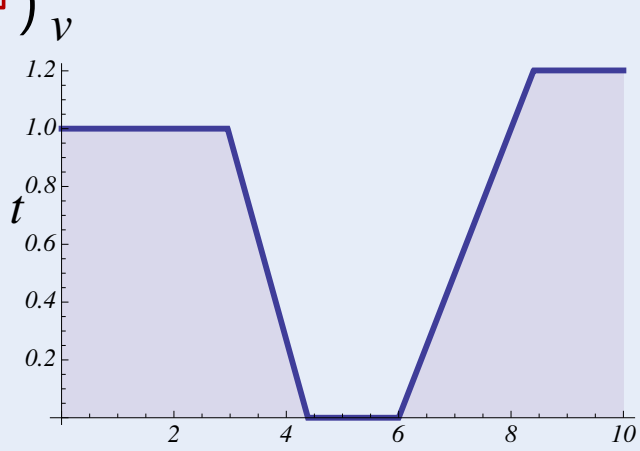
Challenge (Hybrid Games)

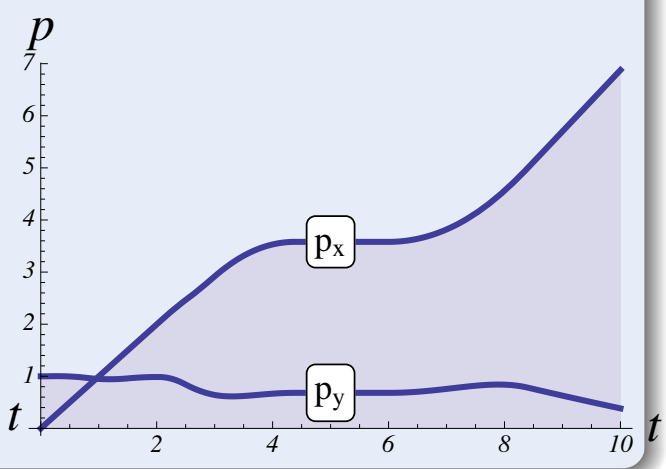
Game rules describing play choices with

- Discrete dynamics (control decisions)
- Continuous dynamics (differential equations)
- Adversarial dynamics (Angel ◇ vs. Demon □)





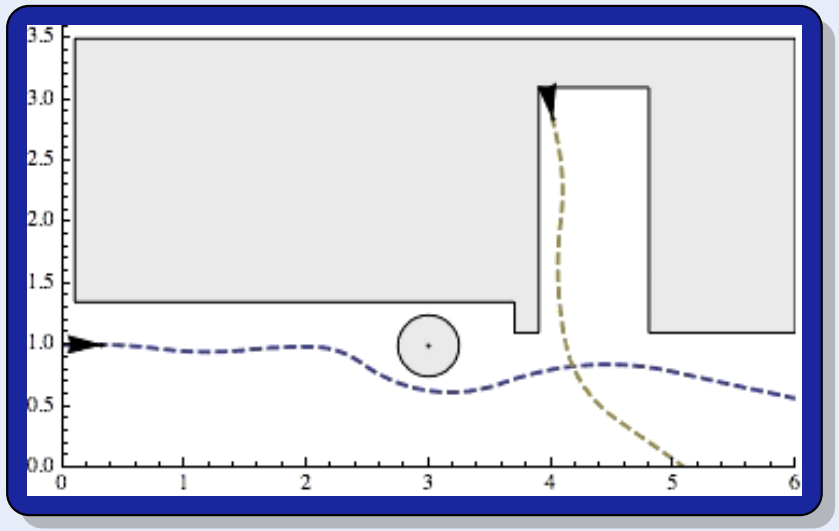


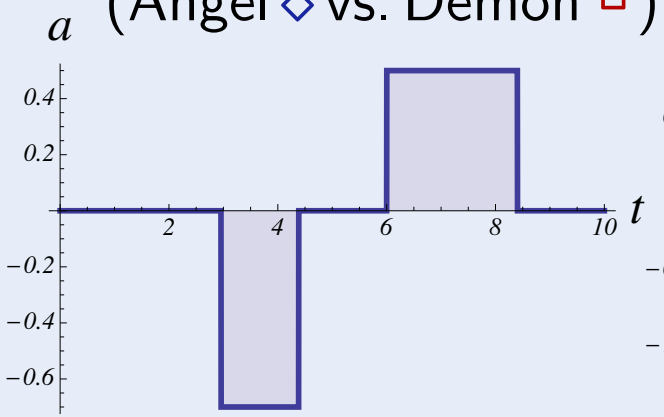


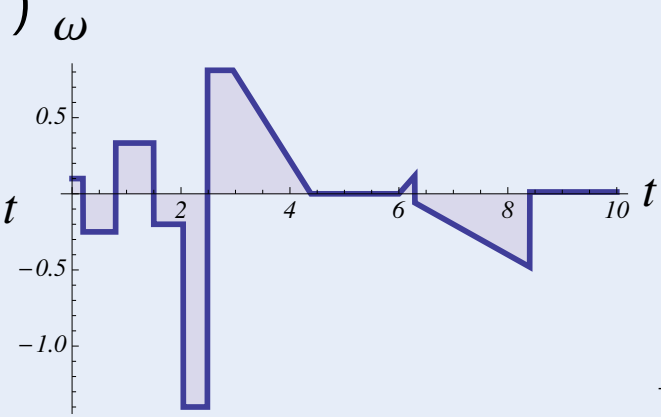
Challenge (Hybrid Games)

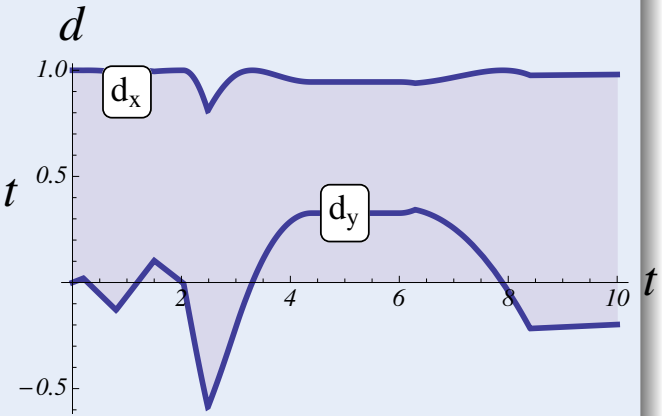
Game rules describing play choices with

- Discrete dynamics (control decisions)
- Continuous dynamics (differential equations)
- Adversarial dynamics (Angel ◇ vs. Demon □)





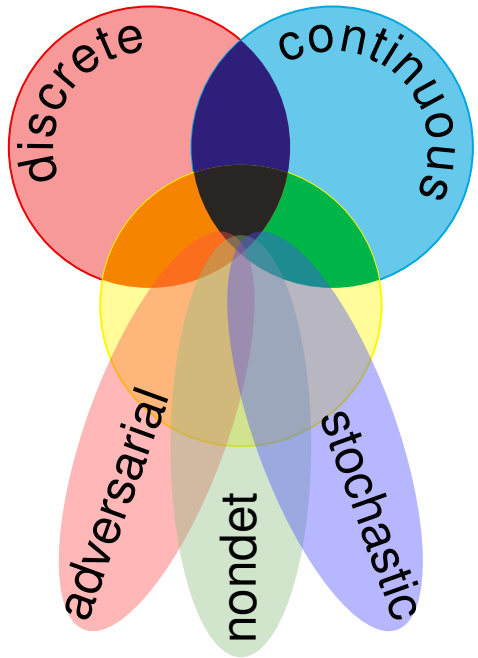




CPSs are Multi-Dynamical Systems

hybrid systems

HS = discrete + ODE

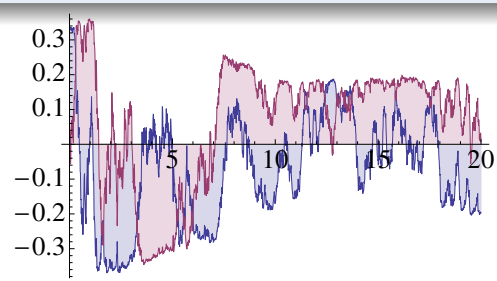


hybrid games

HG = HS + adversary

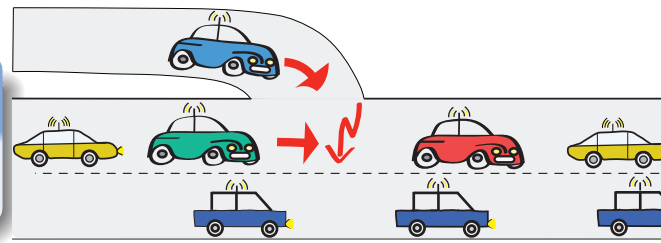
stochastic hybrid sys.

SHS = HS + stochastics



distributed hybrid sys.

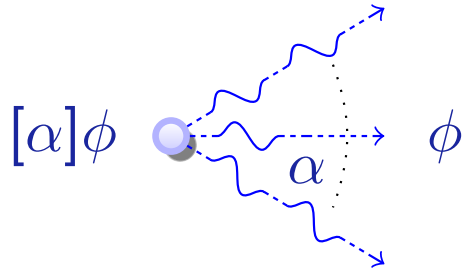
DHS = HS + distributed

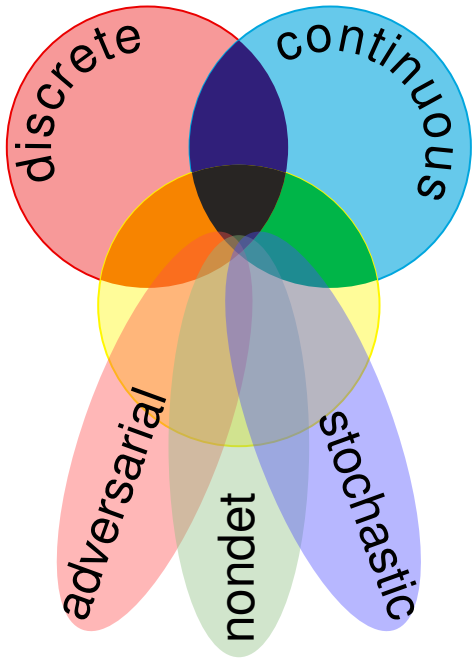


Dynamic Logics for Dynamical Systems

differential dynamic logic

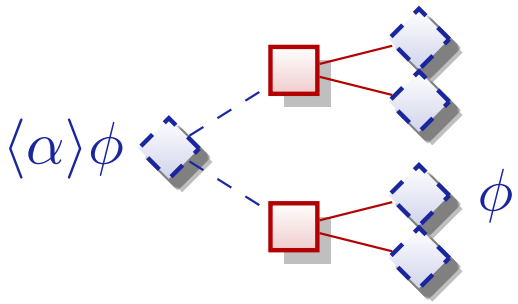
$$\mathsf{d}\mathcal{L} = \mathsf{DL} + \mathsf{HP}$$





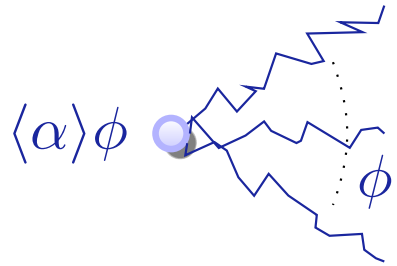
differential game logic

$$\mathsf{dG}\mathcal{L} = \mathsf{GL} + \mathsf{HG}$$



stochastic differential DL

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



quantified differential DL

$$\mathsf{Qd}\mathcal{L} = \mathsf{FOL} + \mathsf{DL} + \mathsf{QHP}$$

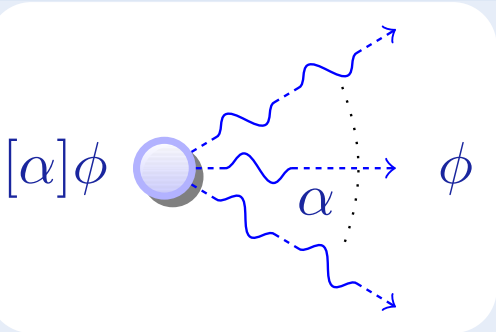
JAR'08,CADE'11,LMCS'12,LICS'12

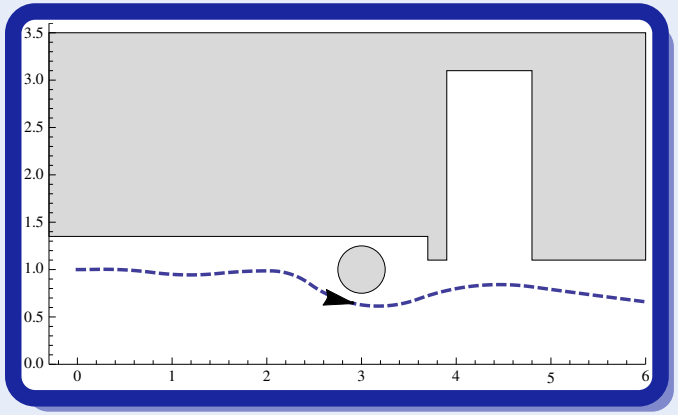
LICS'12,CADE'15,TOCL'15

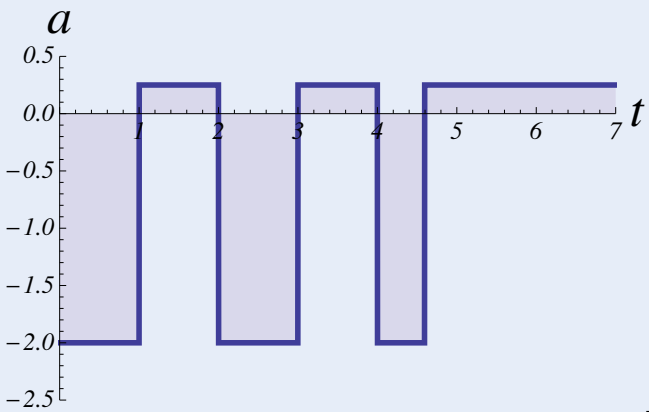
Outline

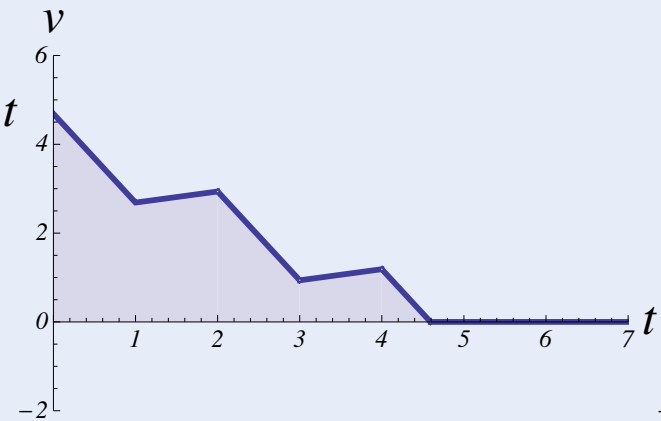
Outline

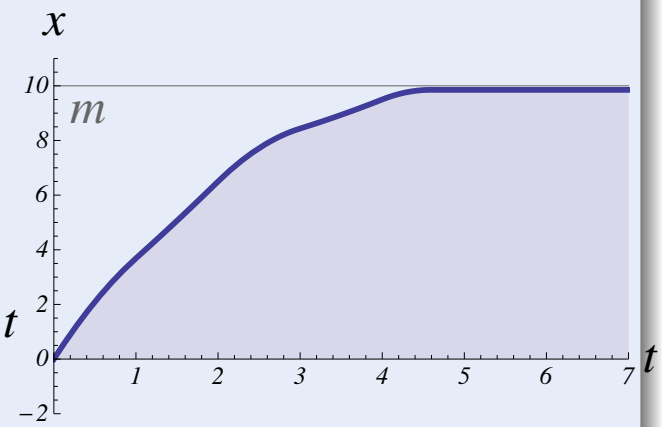
Concept (Differential Dynamic Logic) (JAR'08,LICS'12)



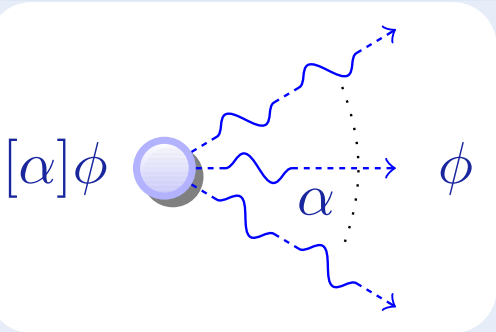


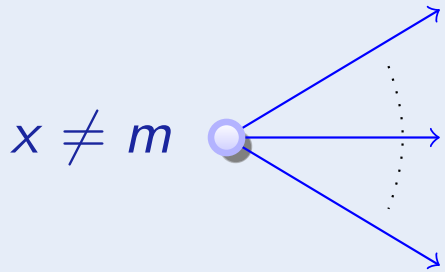


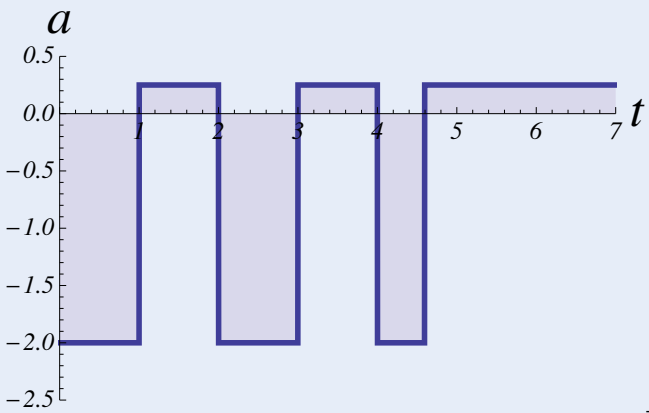


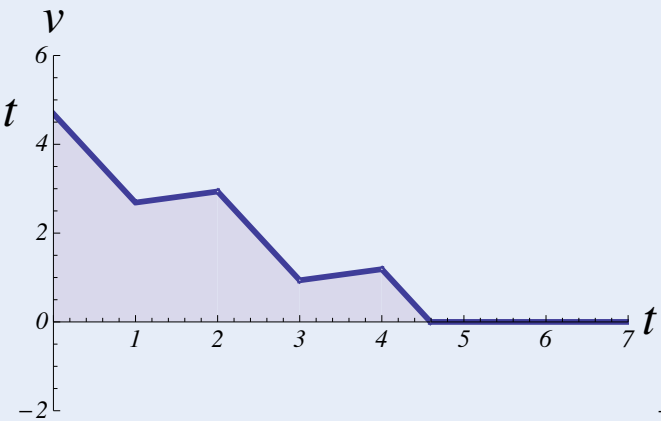


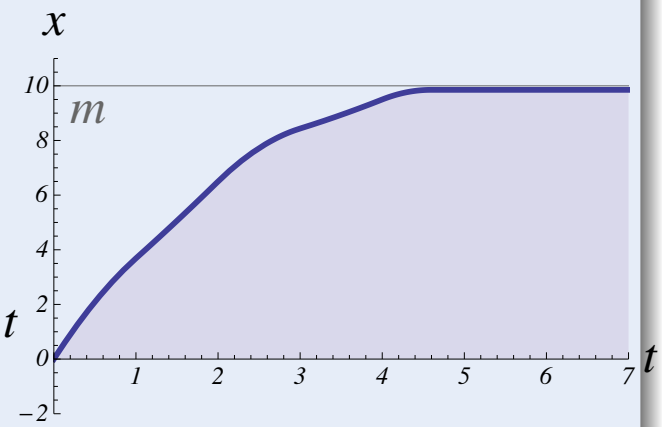
Concept (Differential Dynamic Logic) (JAR'08,LICS'12)



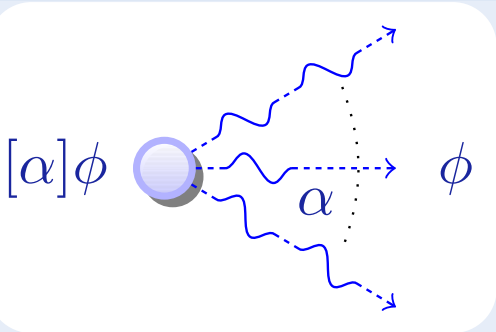


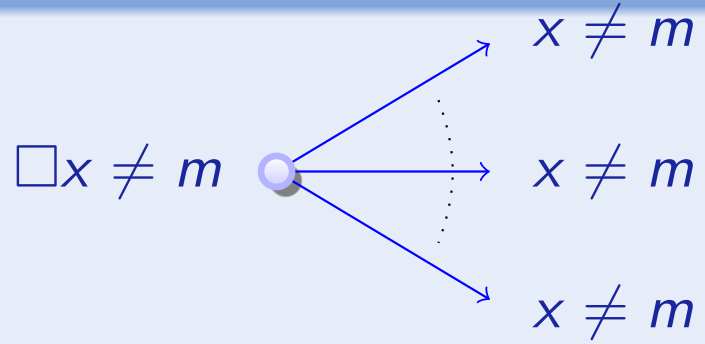


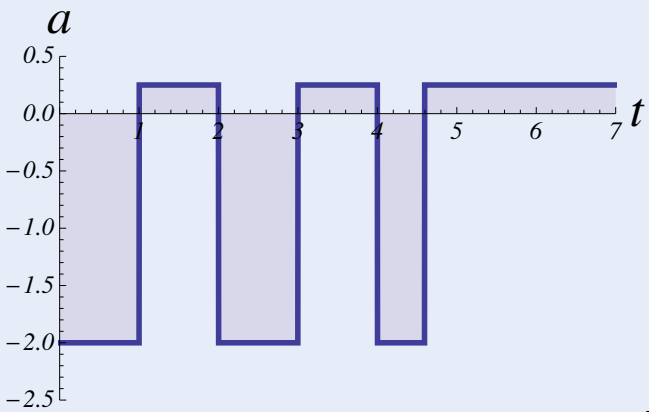


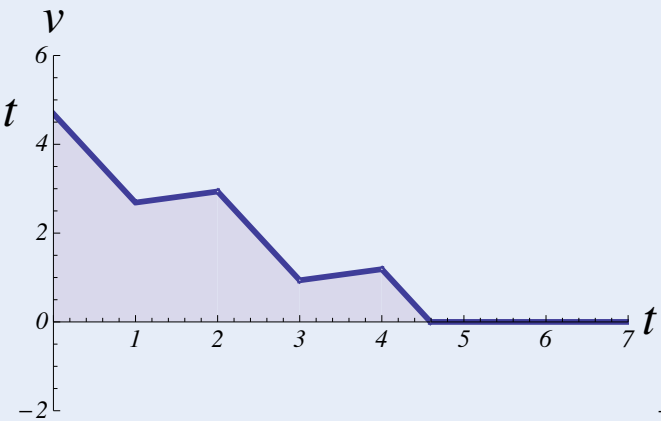


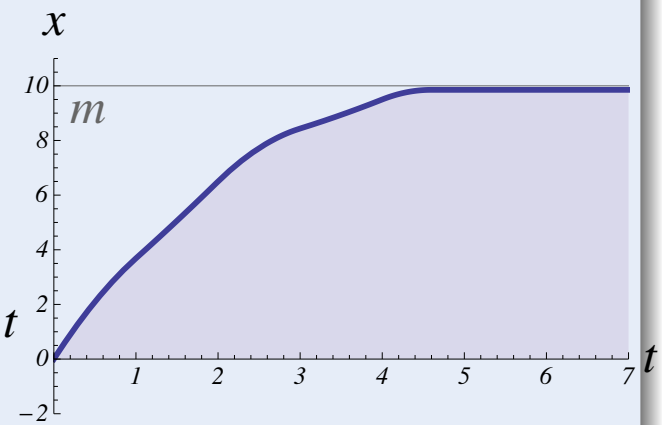
Concept (Differential Dynamic Logic) (JAR'08,LICS'12)



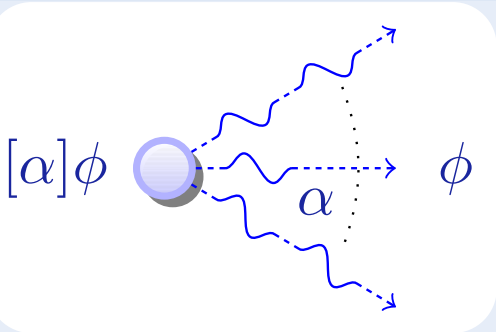


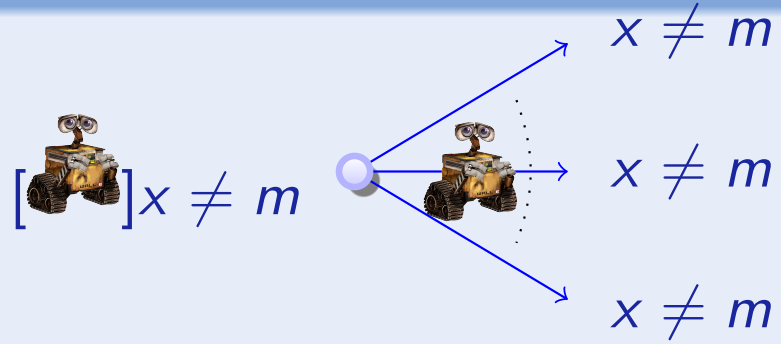


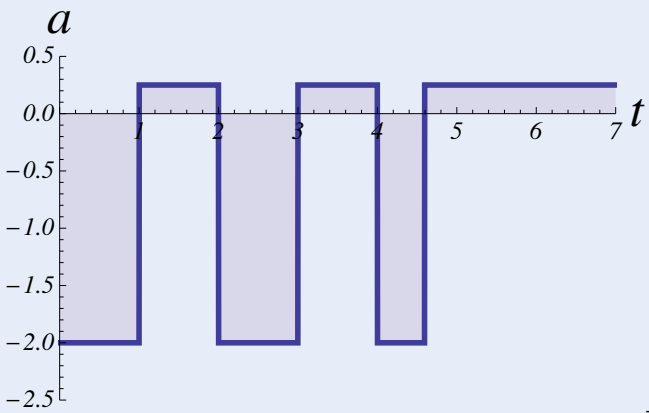


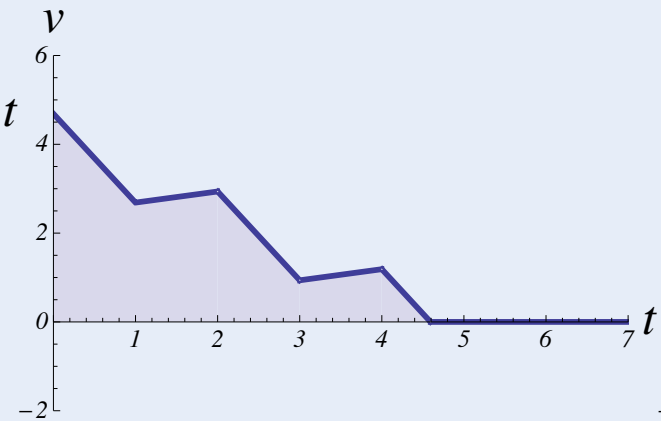


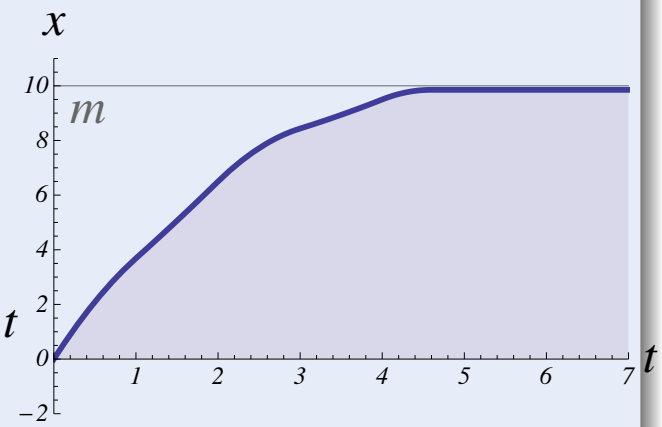
Concept (Differential Dynamic Logic) (JAR'08,LICS'12)



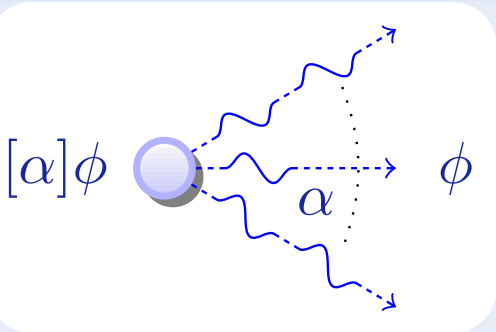


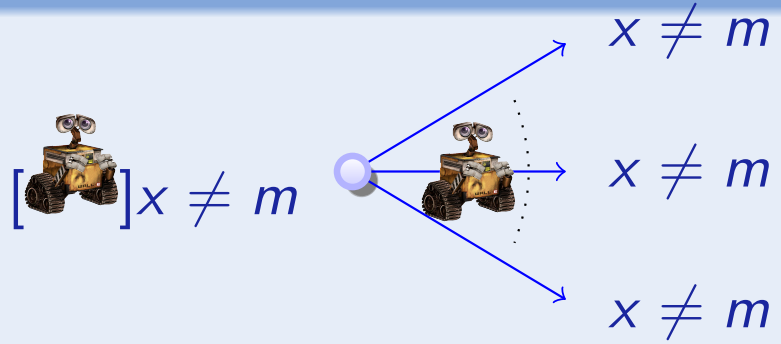


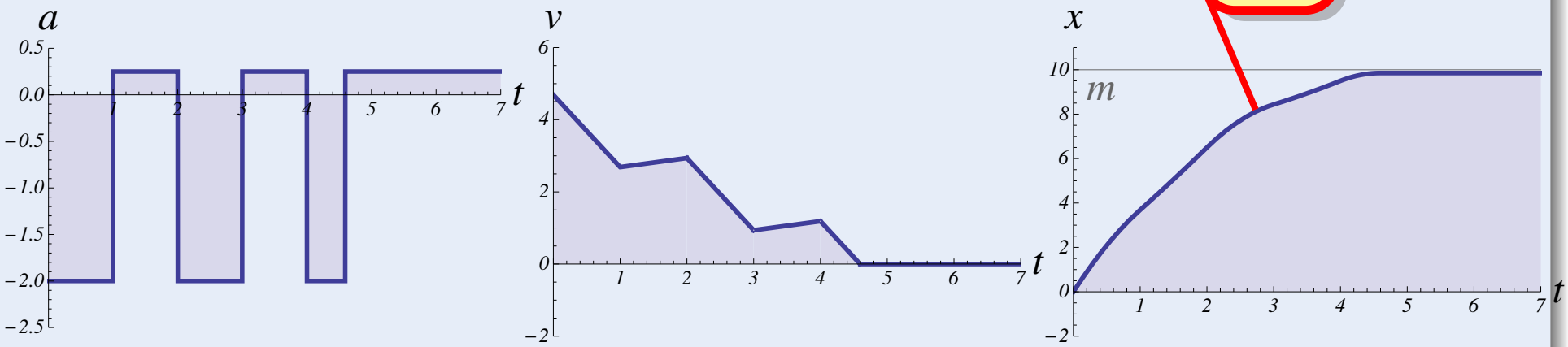




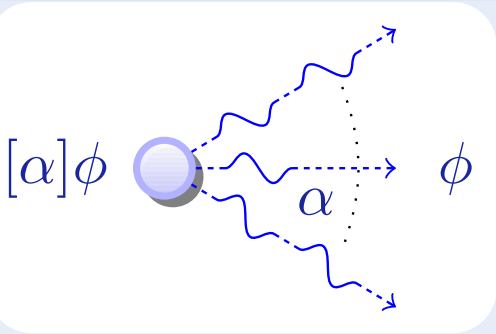
Concept (Differential Dynamic Logic) (JAR'08,LICS'12)

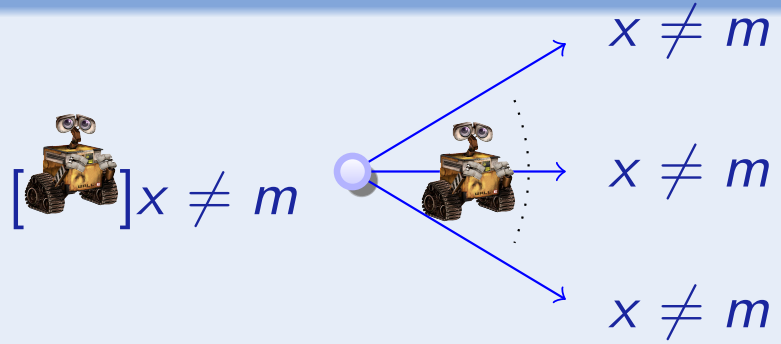


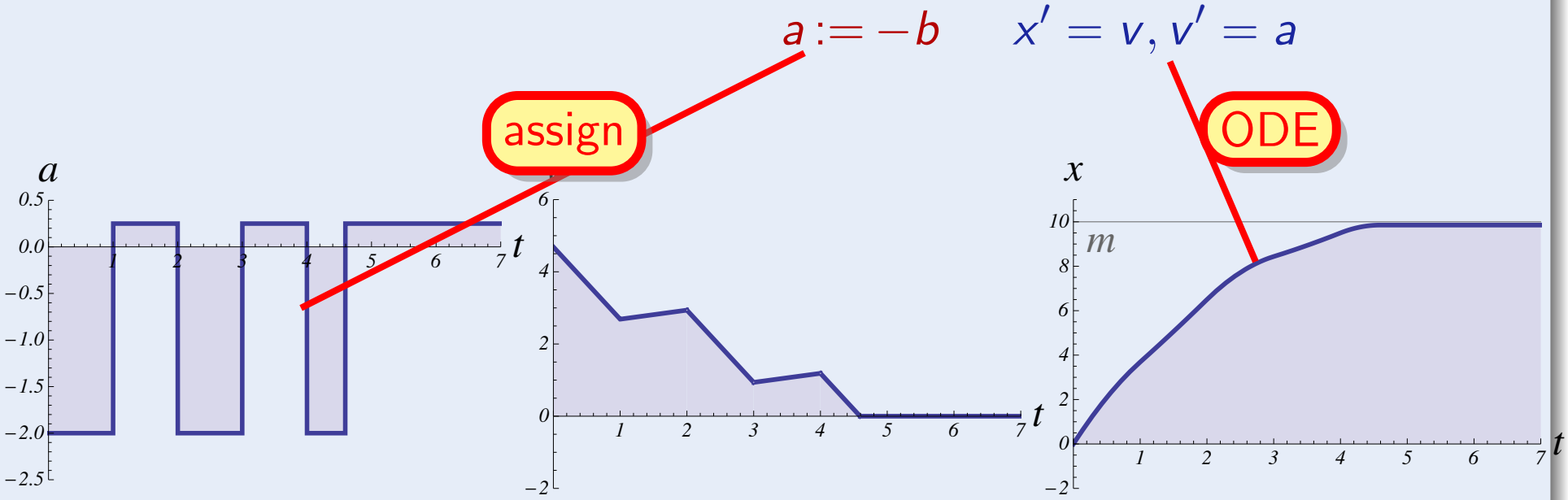




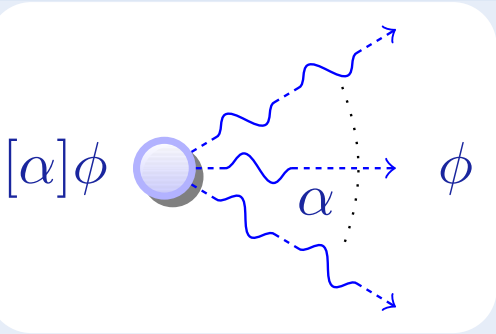
Concept (Differential Dynamic Logic) (JAR'08,LICS'12)

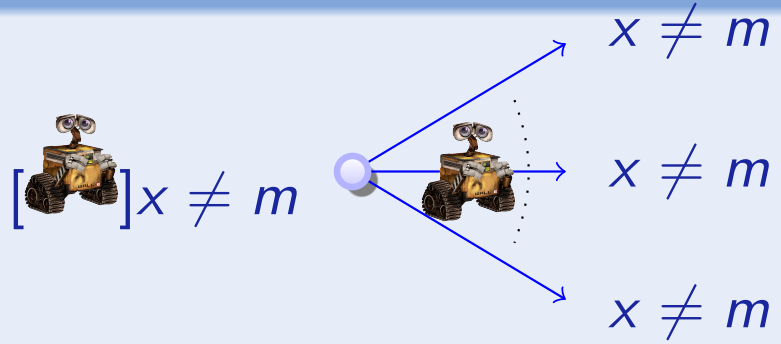






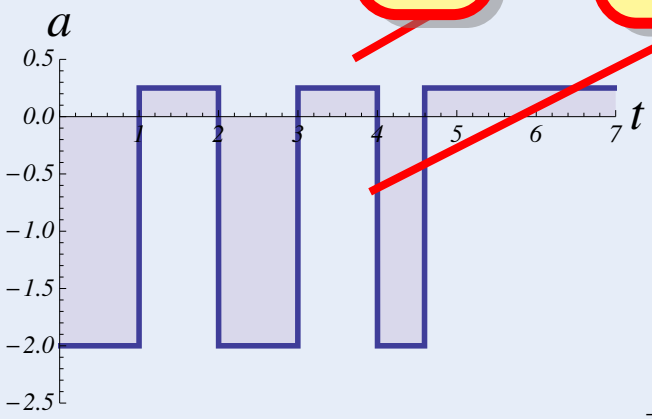
Concept (Differential Dynamic Logic) (JAR'08,LICS'12)

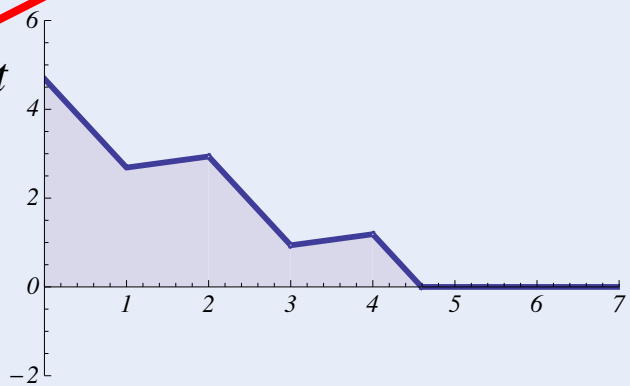


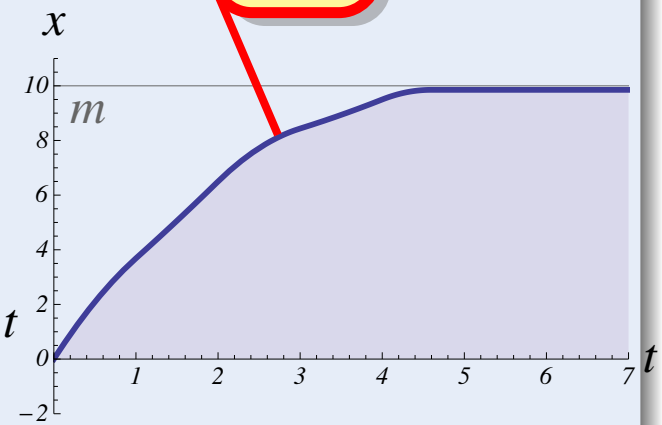


$(\texttt{if}(\mathrm{SB}(x,m))\ a := -b) \quad x' = v, v' = a$

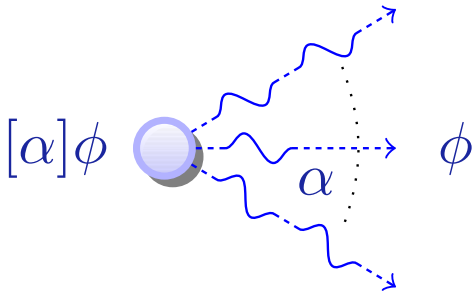
test assign ODE







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



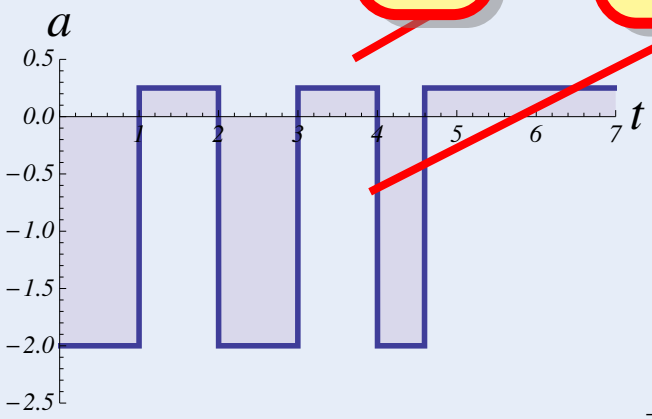
seq. compose

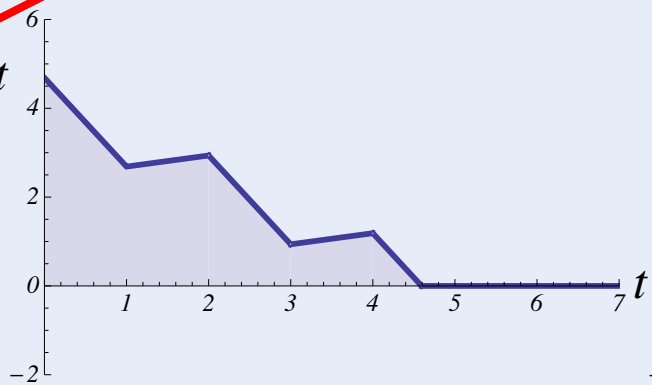
$$(\texttt{if}(\mathrm{SB}(x,m))\ a := -b)\ ;\ x' = v, v' = a$$

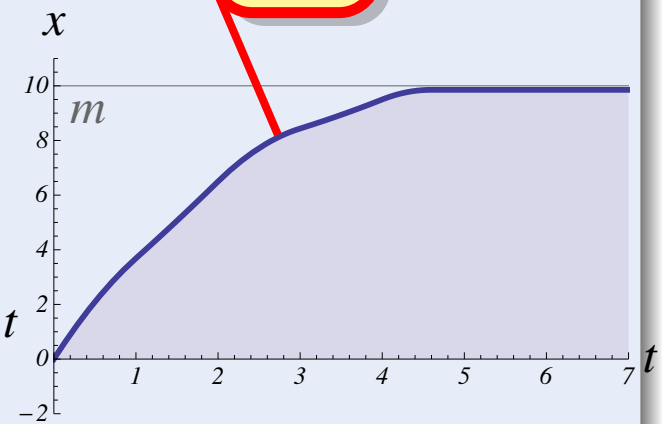
test

assign

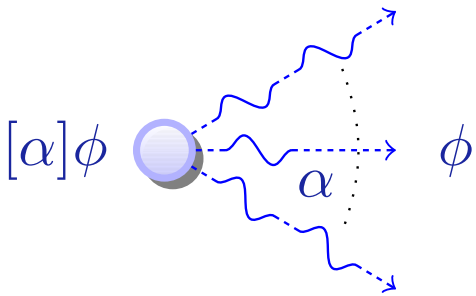
ODE







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



seq. compose

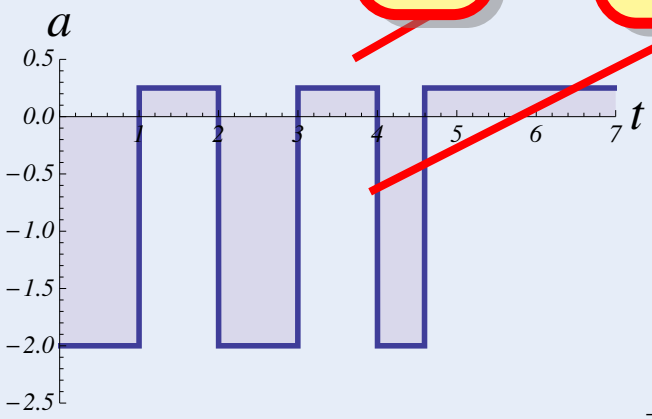
nondet. repeat

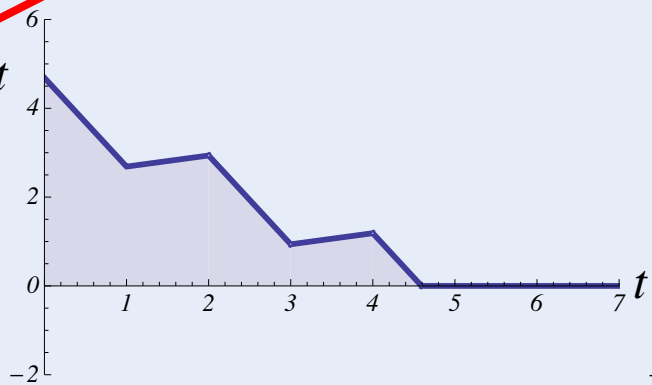
$$\big((\texttt{if}(\mathrm{SB}(x,m))\ a := -b)\ ;\ x' = v, v' = a\big)^*$$

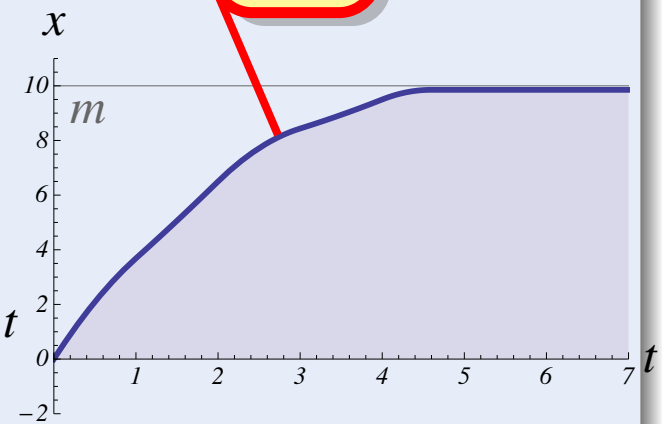
test

assign

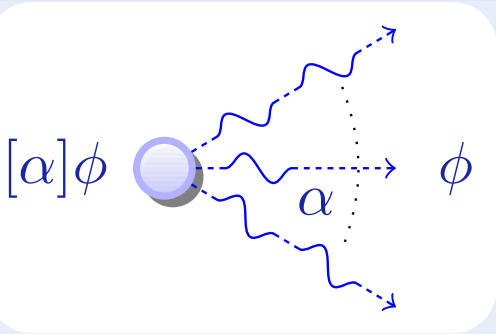
ODE

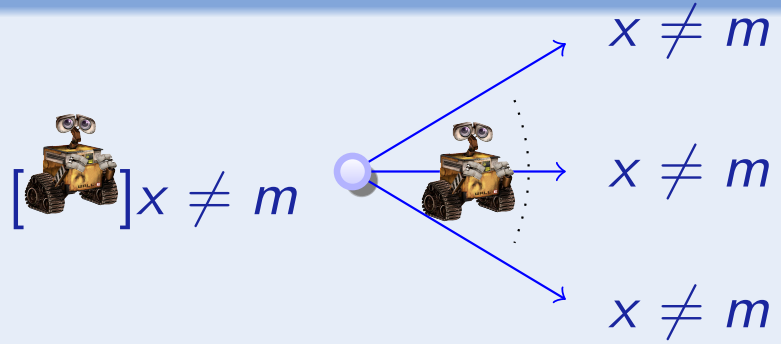






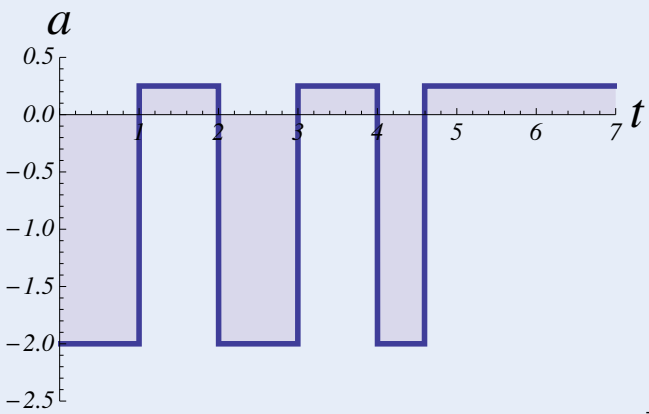
Concept (Differential Dynamic Logic) (JAR'08,LICS'12)

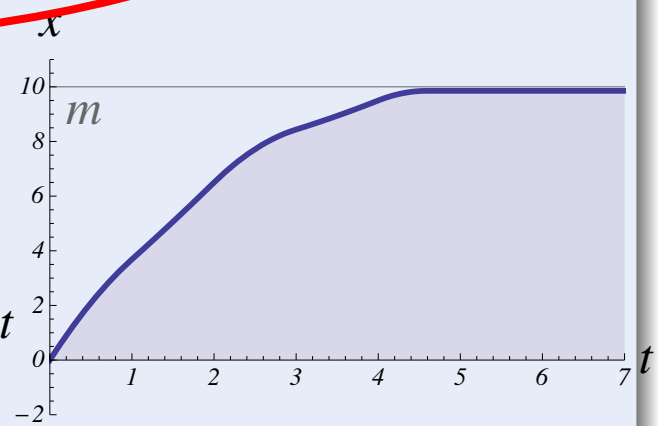




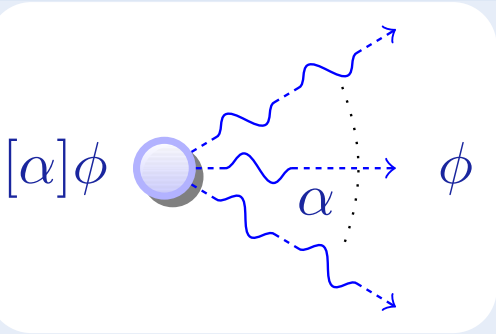
$$\Big[\big((\texttt{if}(\mathrm{SB}(x,m))\ a := -b)\ ;\ x' = v, v' = a\big)^*\Big] \underbrace{x \neq m}_{\text{post}}$$

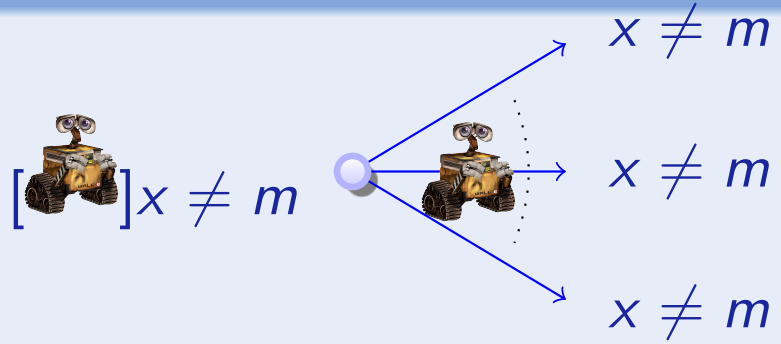
all runs



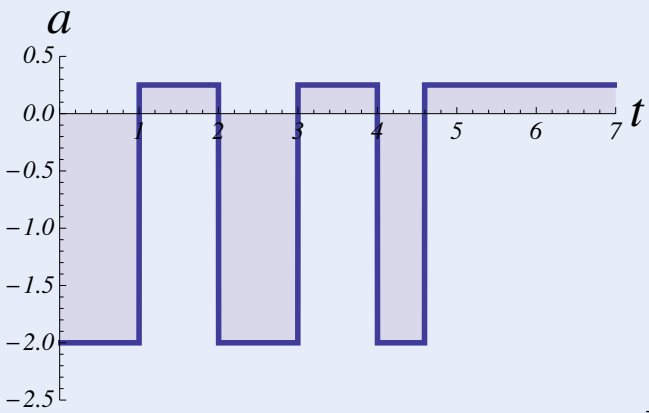


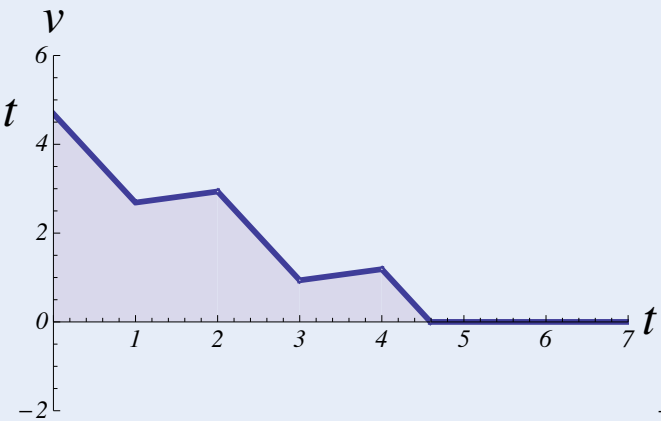
Concept (Differential Dynamic Logic) (JAR'08,LICS'12)

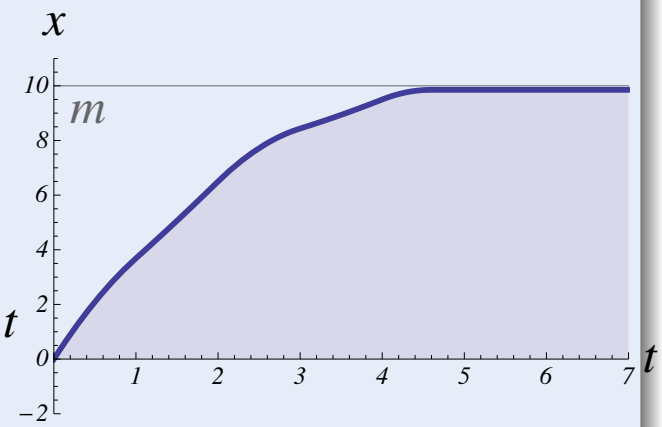




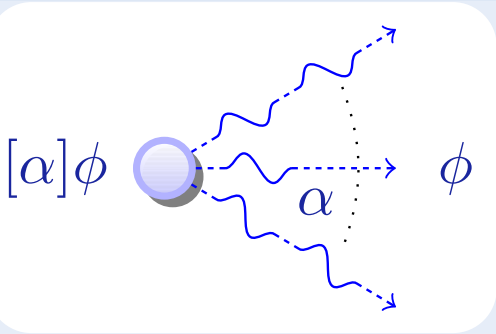
$$\underbrace{x \neq m \wedge b > 0}_{\text{init}} \rightarrow \big[\big((\texttt{if}(\mathrm{SB}(x,m))\ a := -b)\ ;\ x' = v, v' = a\big)^*\big]\underbrace{x \neq m}_{\text{post}}$$

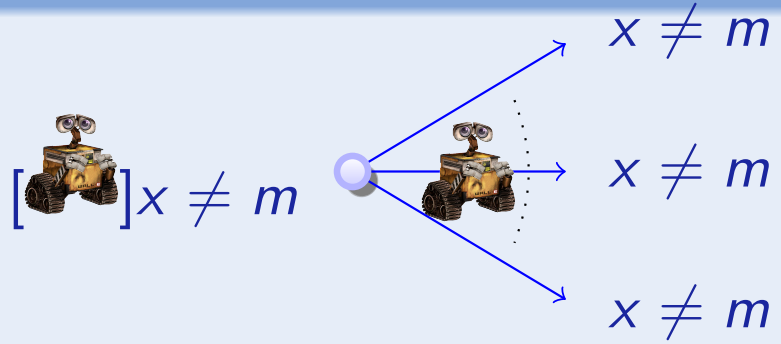






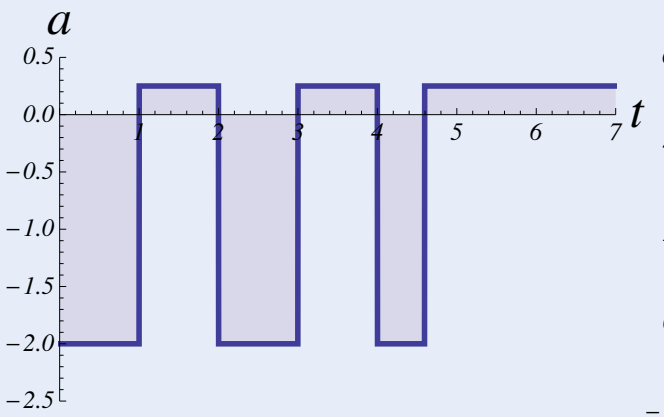
Concept (Differential Dynamic Logic) (JAR'08,LICS'12)

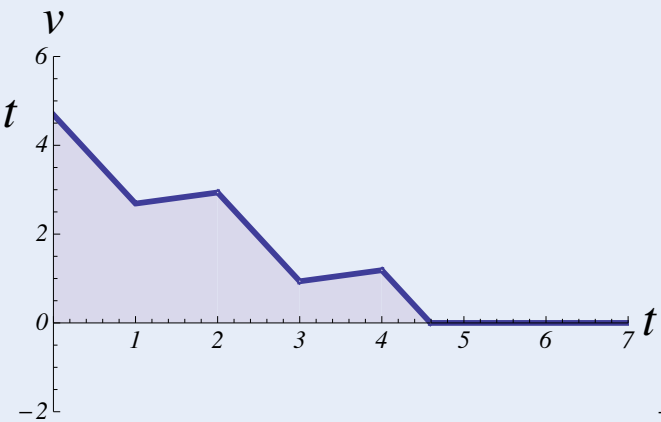


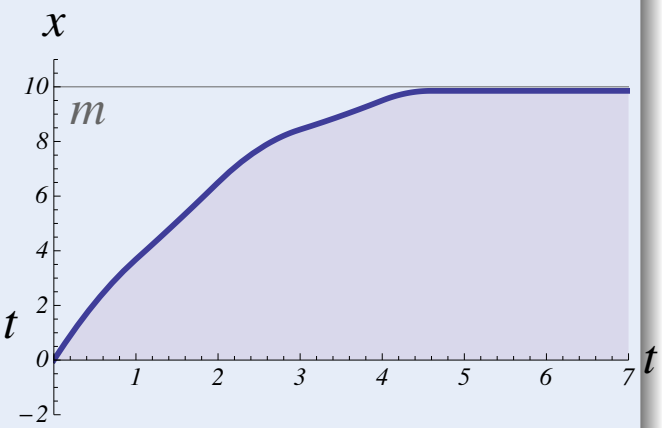


nondet. choice

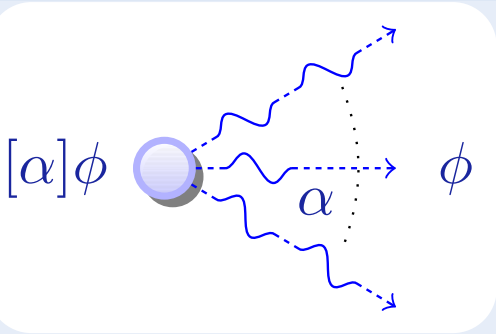
$$\underbrace{x \neq m \wedge b > 0}_{\text{init}} \rightarrow \left[\left((?\neg \mathrm{SB}(x,m) \cup a := -b)\ ;\ x' = v, v' = a\right)^*\right] \underbrace{x \neq m}_{\text{post}}$$

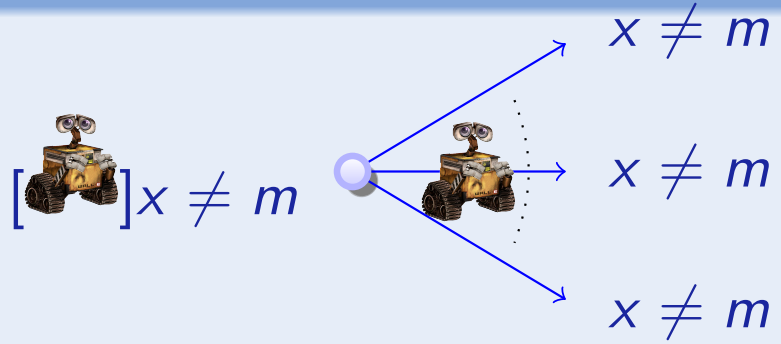






Concept (Differential Dynamic Logic) (JAR'08,LICS'12)

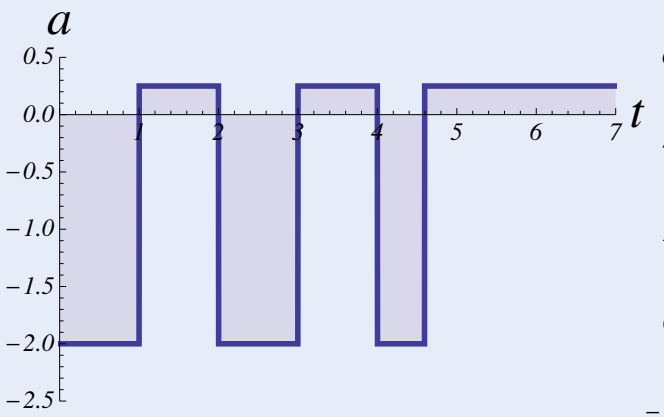


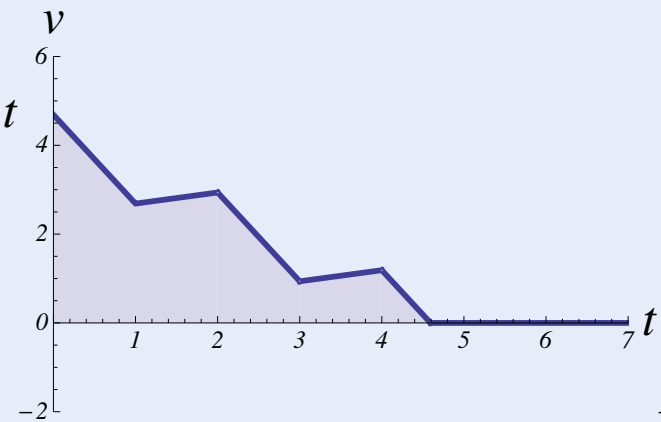


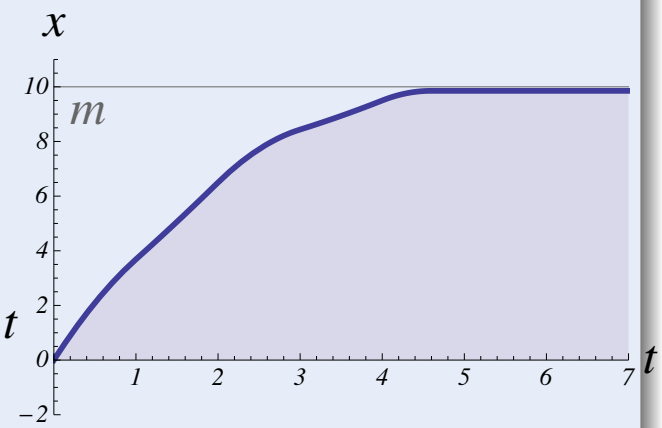
test

nondet. choice

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

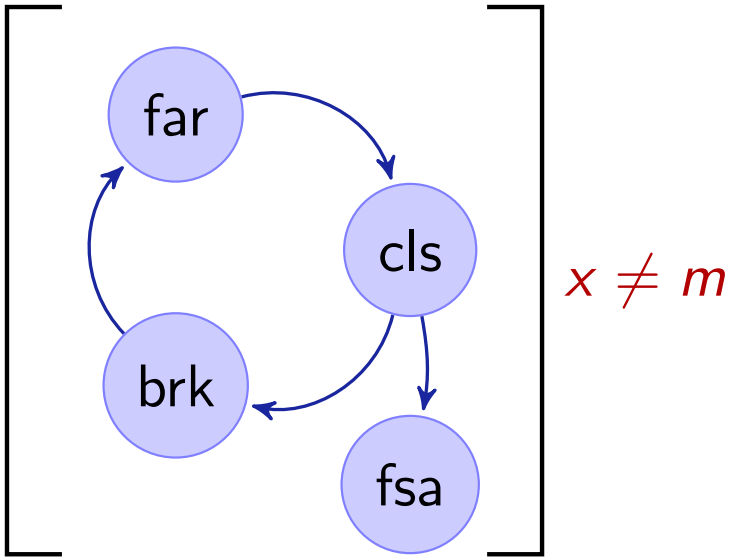






Hybrid Programs vs. Hybrid Automata

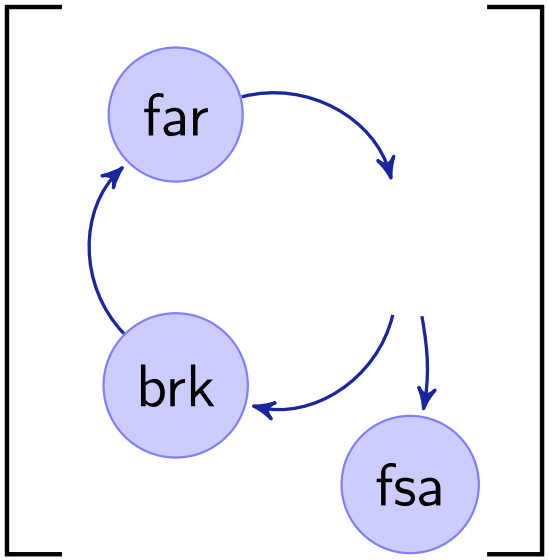
Want: Compositional verification

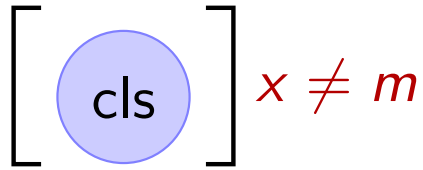


$$\text{far} \equiv x' = v, v' = A \,\&\, \neg \text{SB}(x, m)$$
$$\text{brk} \equiv x' = v, v' = -b \,\&\, \text{SB}(x, m) \lor \mathit{true}$$
$$\text{cls} \equiv x' = v, v' = \ldots \,\&\, \ldots$$
$$\text{fsa} \equiv x' = 0, v' = 0 \,\&\, v = 0$$

Hybrid Programs vs. Hybrid Automata

Want: Compositional verification

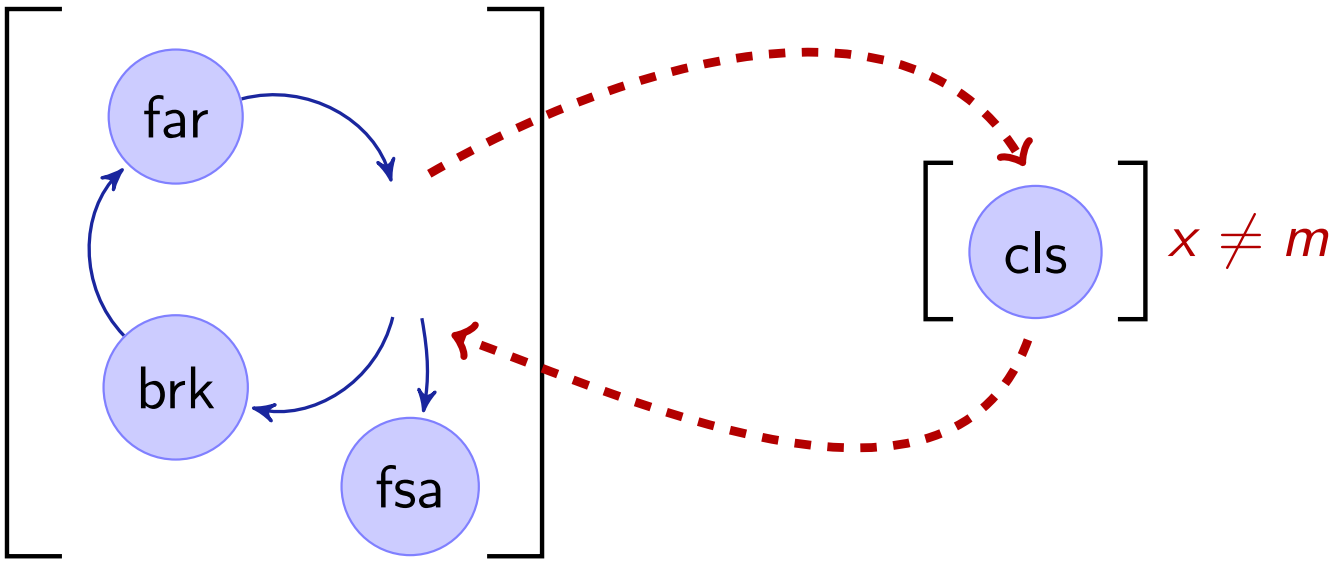




$$\text{far} \equiv x' = v, v' = A \,\&\, \neg \text{SB}(x, m)$$
$$\text{brk} \equiv x' = v, v' = -b \,\&\, \text{SB}(x, m) \lor \mathit{true}$$
$$\text{cls} \equiv x' = v, v' = \ldots \,\&\, \ldots$$
$$\text{fsa} \equiv x' = 0, v' = 0 \,\&\, v = 0$$

Hybrid Programs vs. Hybrid Automata

Want: Compositional verification



$$\text{far} \equiv x' = v, v' = A \,\&\, \neg \text{SB}(x, m)$$

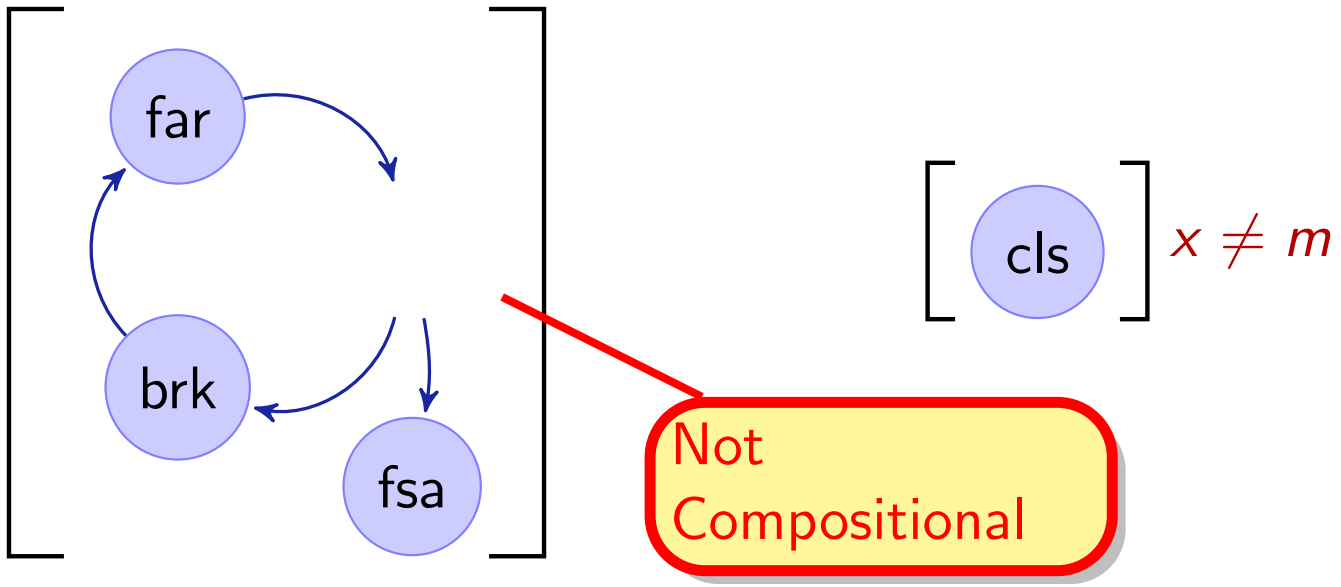
$$\text{brk} \equiv x' = v, v' = -b \,\&\, \text{SB}(x, m) \lor \mathit{true}$$

$$\text{cls} \equiv x' = v, v' = \ldots \,\&\, \ldots$$

$$\text{fsa} \equiv x' = 0, v' = 0 \,\&\, v = 0$$

Hybrid Programs vs. Hybrid Automata

Want: Compositional verification



$$\text{far} \equiv x' = v, v' = A \,\&\, \neg \text{SB}(x, m)$$
$$\text{brk} \equiv x' = v, v' = -b \,\&\, \text{SB}(x, m) \lor \mathit{true}$$
$$\text{cls} \equiv x' = v, v' = \ldots \,\&\, \ldots$$
$$\text{fsa} \equiv x' = 0, v' = 0 \,\&\, v = 0$$

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

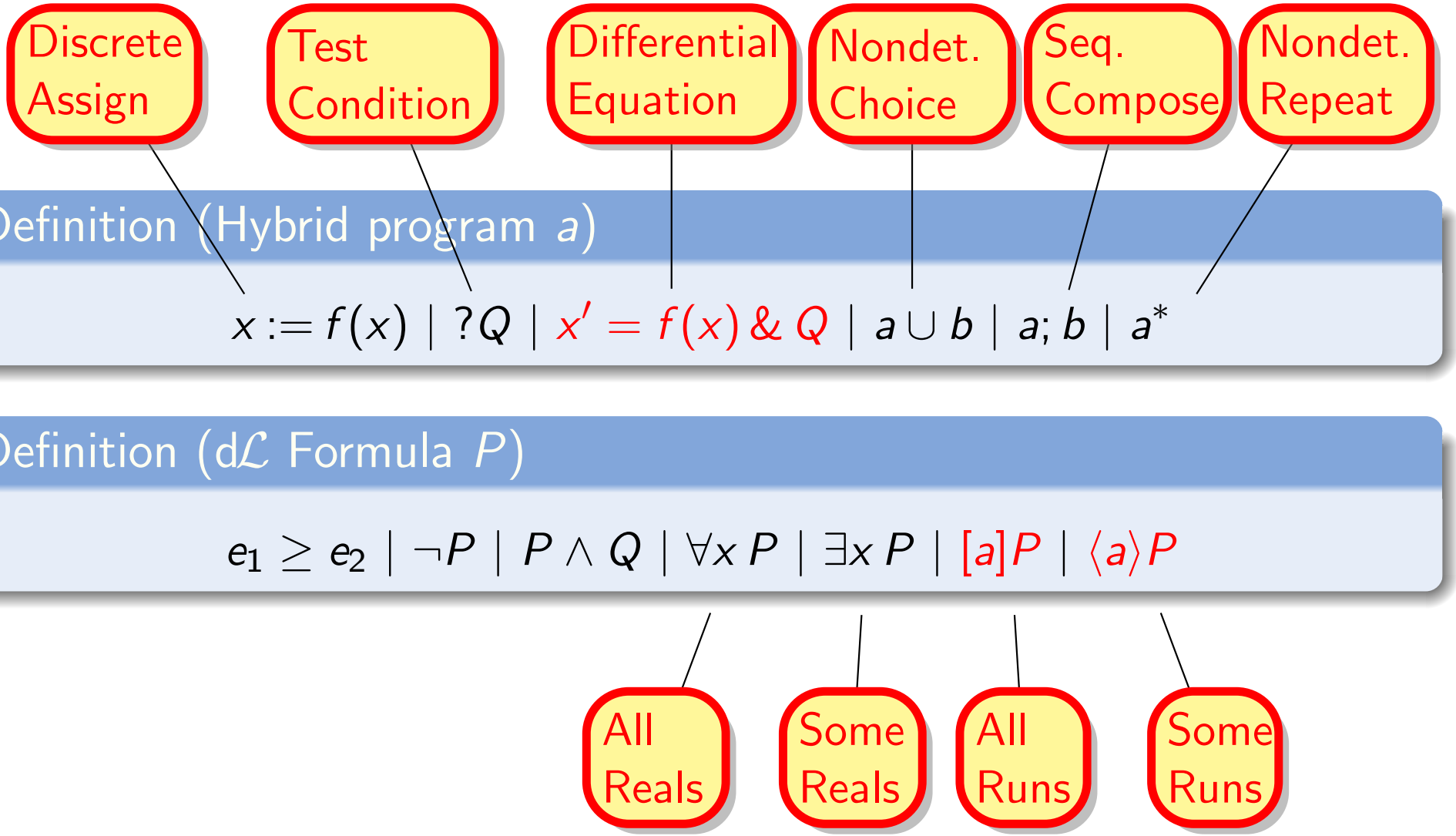
Definition (Hybrid program a)

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

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

$$e_1 \geq e_2 \mid \neg P \mid P \wedge Q \mid \forall x\, P \mid \exists x\, P \mid [a]P \mid \langle a \rangle P$$

Differential Dynamic Logic dℒ: Syntax



Definition (Hybrid program a)

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

Definition (dℒ Formula P)

$$e_1 \geq e_2 \mid \neg P \mid P \wedge Q \mid \forall x\, P \mid \exists x\, P \mid [a]P \mid \langle a \rangle P$$

All Reals | Some Reals | All Runs | Some Runs

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

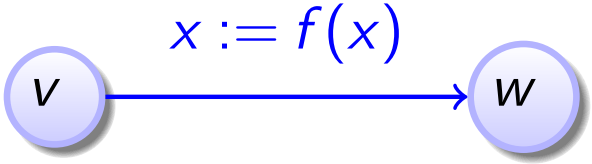
Definition (Hybrid program semantics) $([\![\cdot]\!] : \text{HP} \to \wp(\mathcal{S} \times \mathcal{S}))$

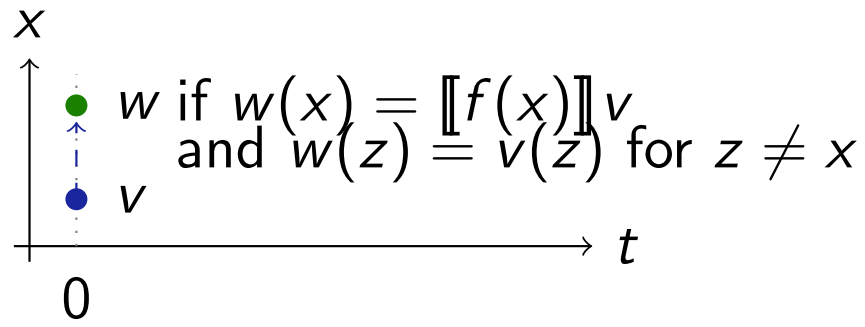
$$
\begin{aligned}
[\![x := f(x)]\!] &= \{(v,w) \;:\; w = v \text{ except } [\![x]\!]w = [\![f(x)]\!]v\} \\
[\![?Q]\!] &= \{(v,v) \;:\; v \in [\![Q]\!]\} \\
[\![x' = f(x)]\!] &= \{(\varphi(0),\varphi(r)) \;:\; \varphi \models x' = f(x) \text{ for some duration } r\} \\
[\![a \cup b]\!] &= [\![a]\!] \cup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

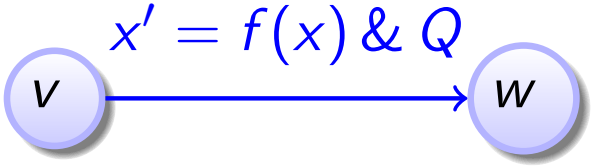
Definition (d$\mathcal{L}$ semantics) $([\![\cdot]\!] : \text{Fml} \to \wp(\mathcal{S}))$

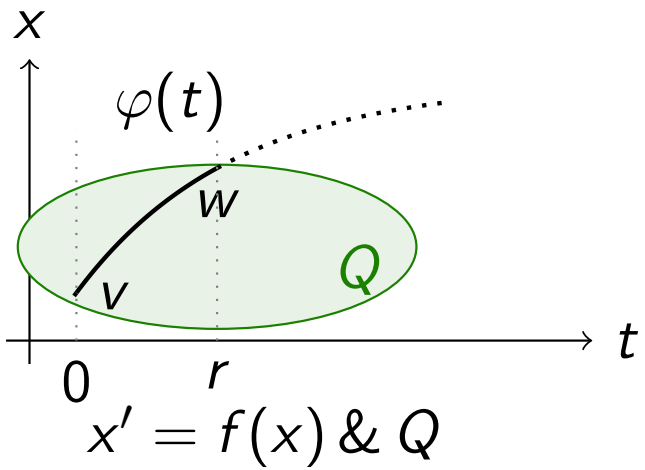
$$
\begin{aligned}
[\![e_1 \geq e_2]\!] &= \{v \;:\; [\![e_1]\!]v \geq [\![e_2]\!]v\} \\
[\![\neg P]\!] &= ([\![P]\!])^{\complement} \\
[\![P \wedge Q]\!] &= [\![P]\!] \cap [\![Q]\!] \\
[\![\langle a \rangle P]\!] &= [\![a]\!] \circ [\![P]\!] = \{v \;:\; w \in [\![P]\!] \text{ for some } w \; (v,w) \in [\![a]\!]\} \\
[\![[a]P]\!] &= [\![\neg\langle a \rangle \neg P]\!] = \{v \;:\; w \in [\![P]\!] \text{ for all } w \; (v,w) \in [\![a]\!]\} \\
[\![\exists x \, P]\!] &= \{v \;:\; v_x^r \in [\![P]\!] \text{ for some } r \in \mathbb{R}\}
\end{aligned}
$$

Differential Dynamic Logic dℒ: Transition Semantics

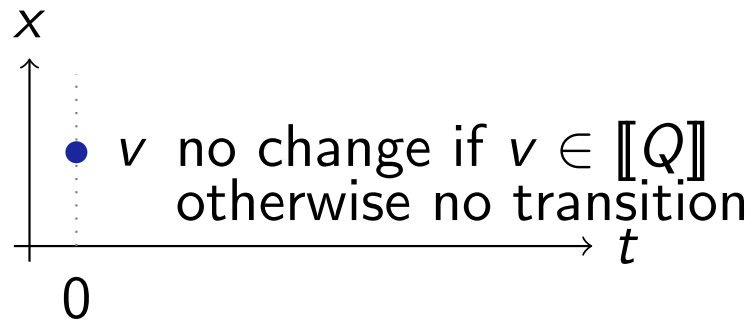




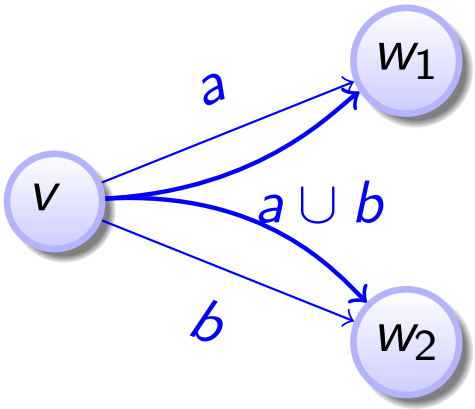


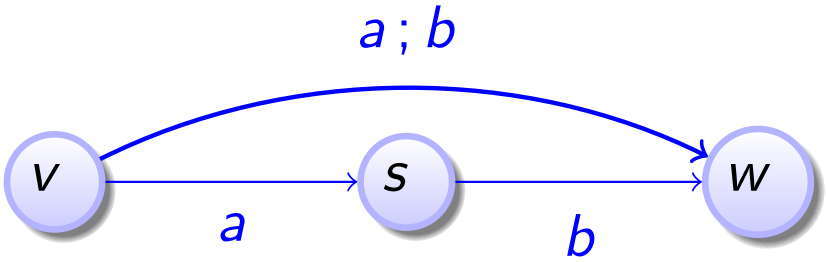


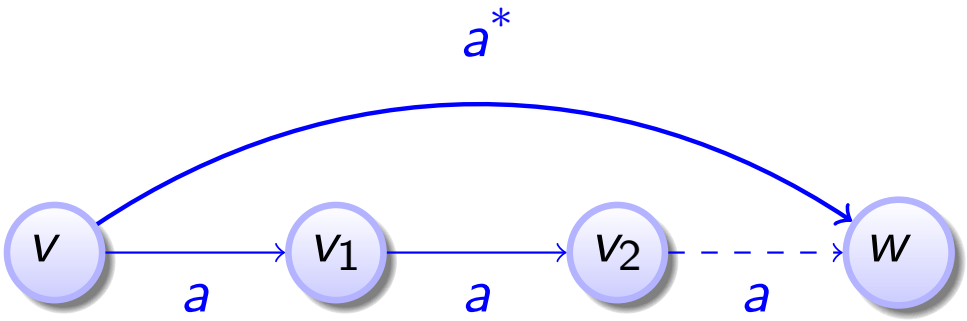
if $v \in [\![Q]\!]$

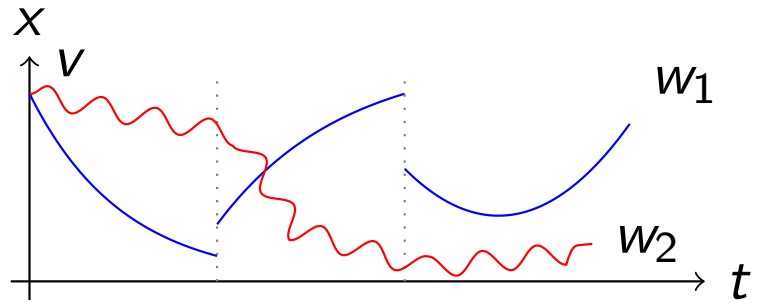


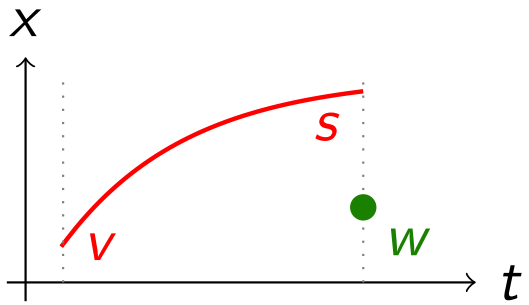
Differential Dynamic Logic dℒ: Transition Semantics

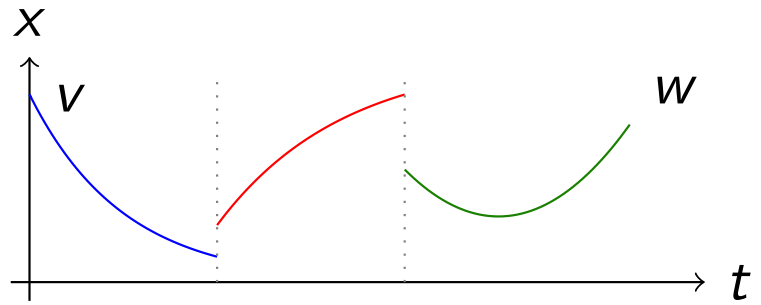




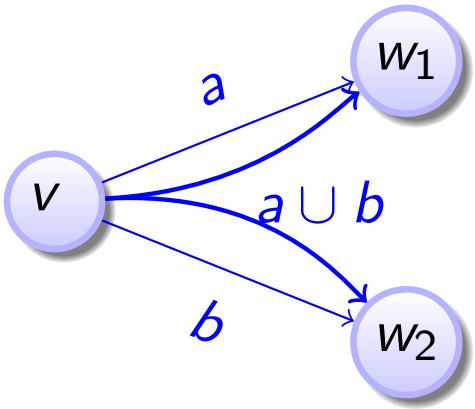


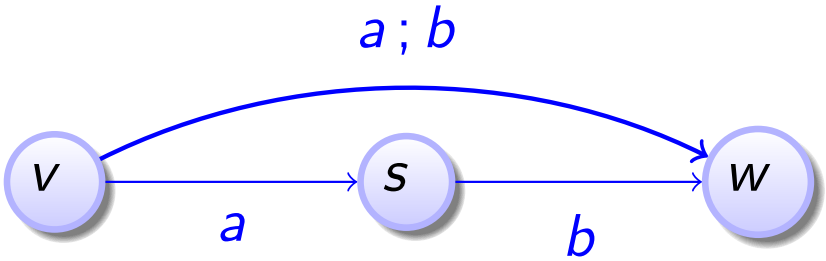


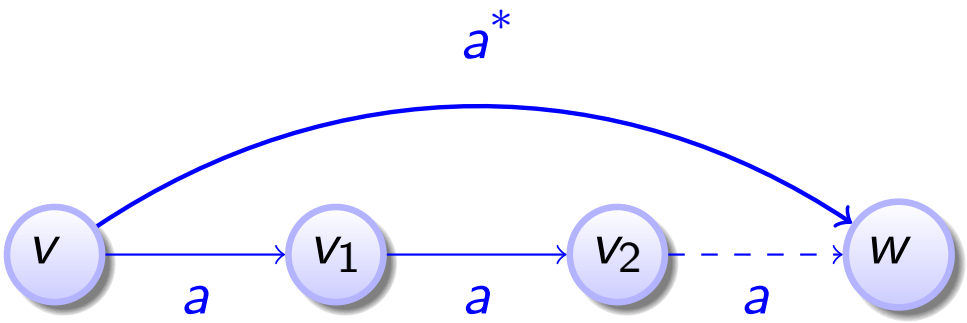


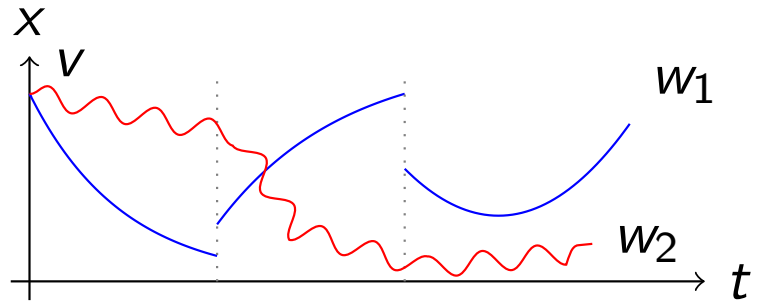


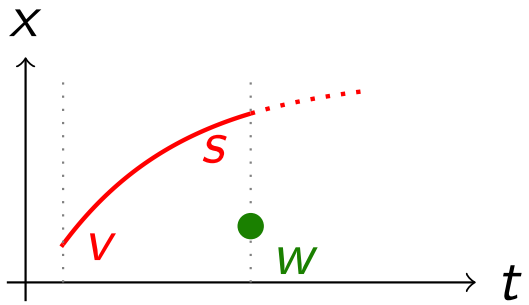
Differential Dynamic Logic d$\mathcal{L}$: Transition Semantics

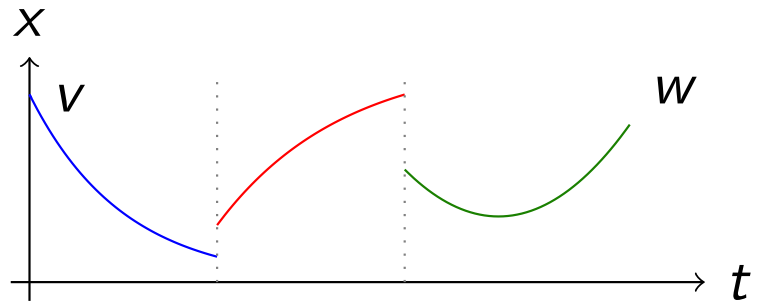




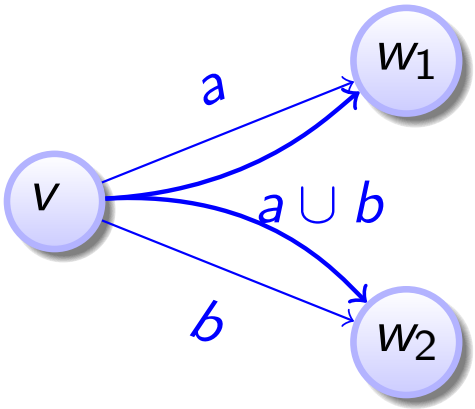


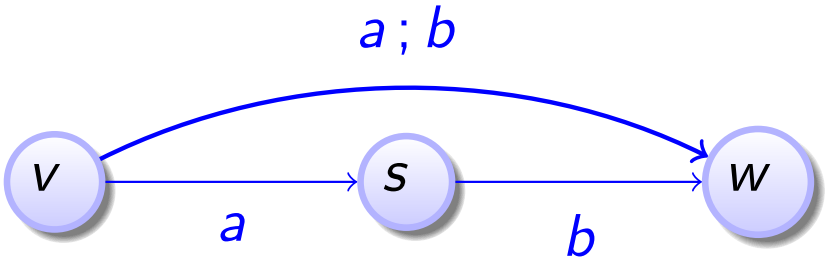


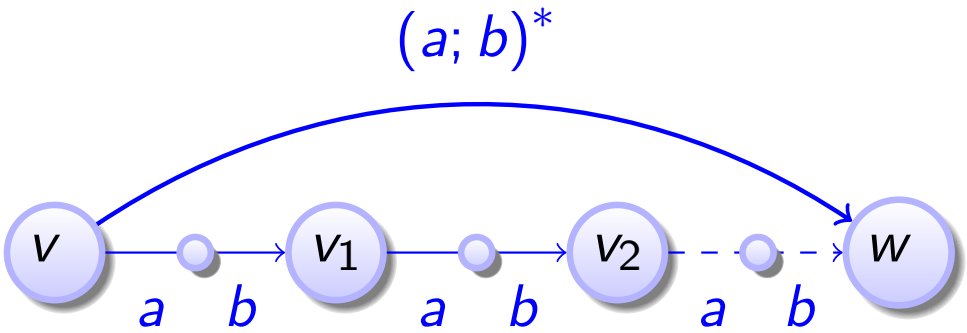


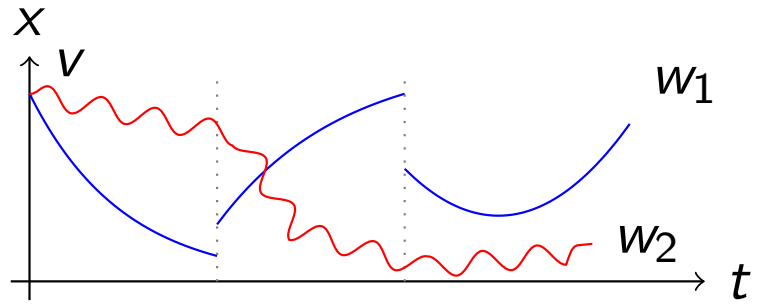


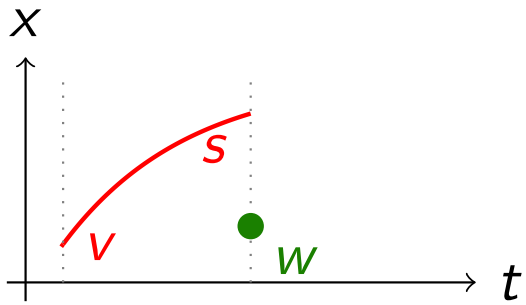
Differential Dynamic Logic dℒ: Transition Semantics

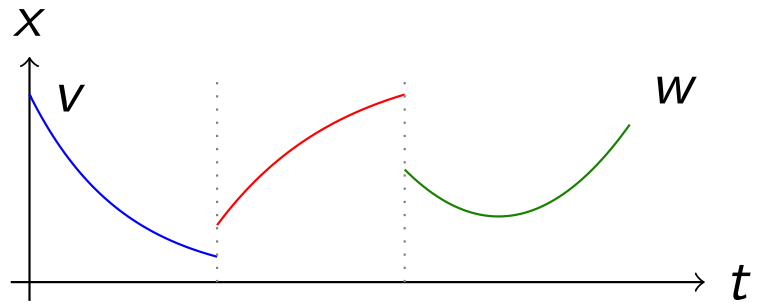




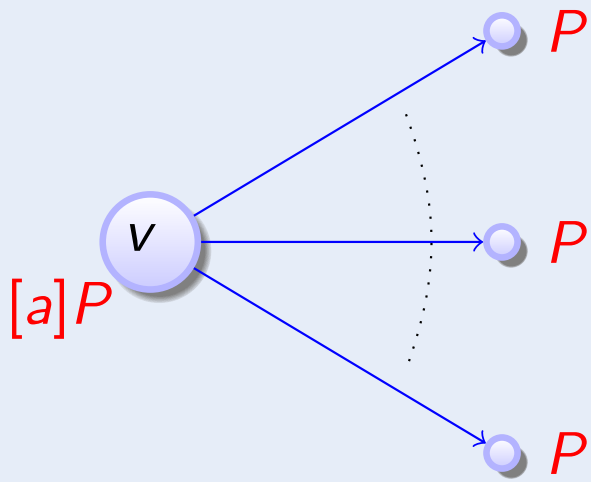




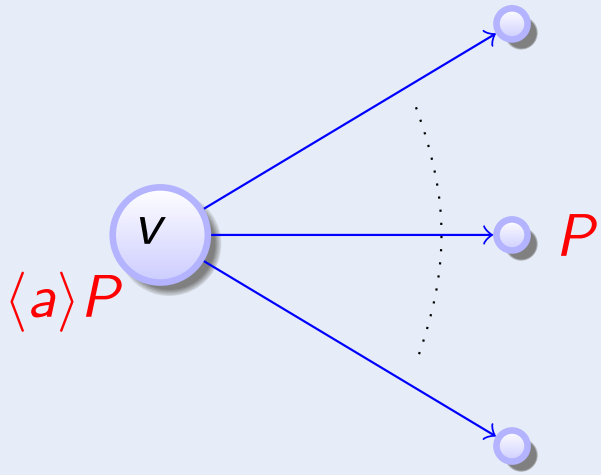




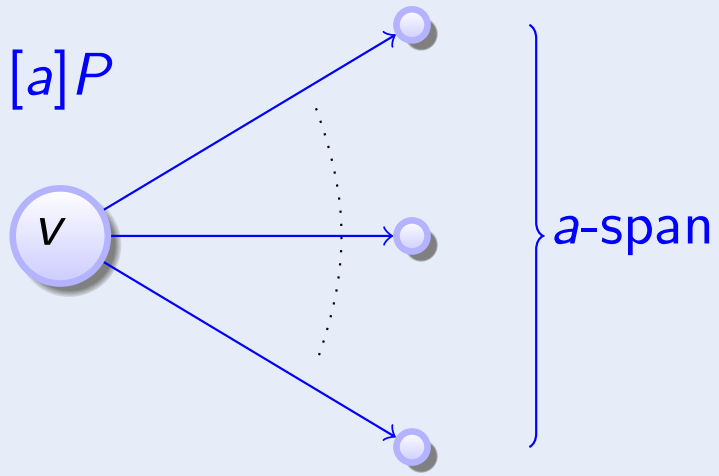
Definition (dℒ Formulas)



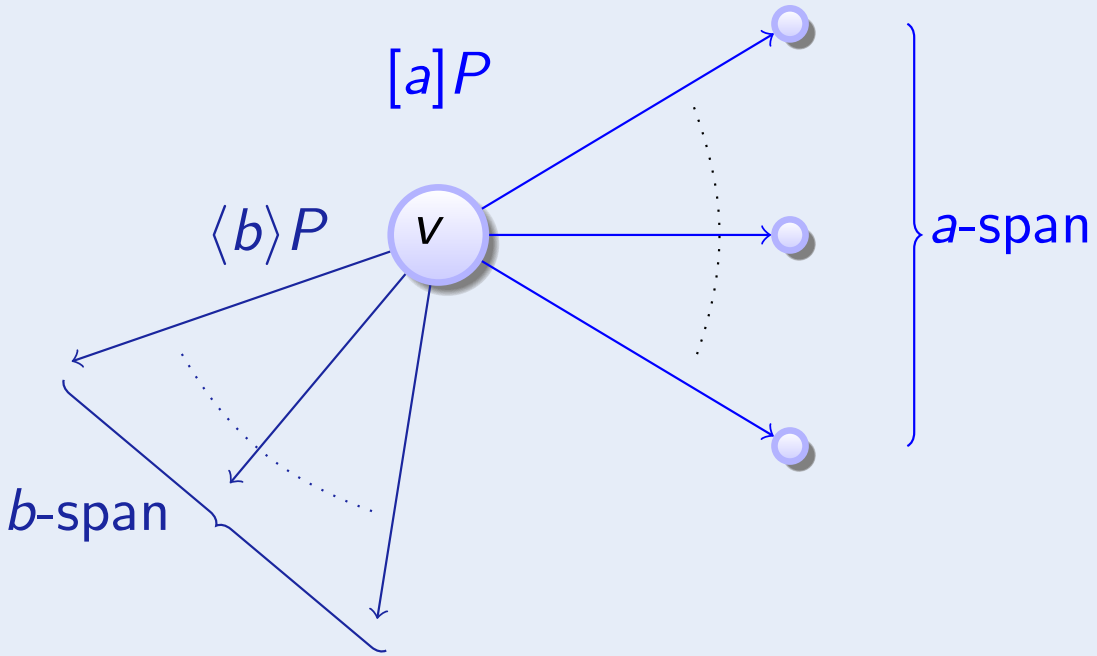
Definition (dℒ Formulas)



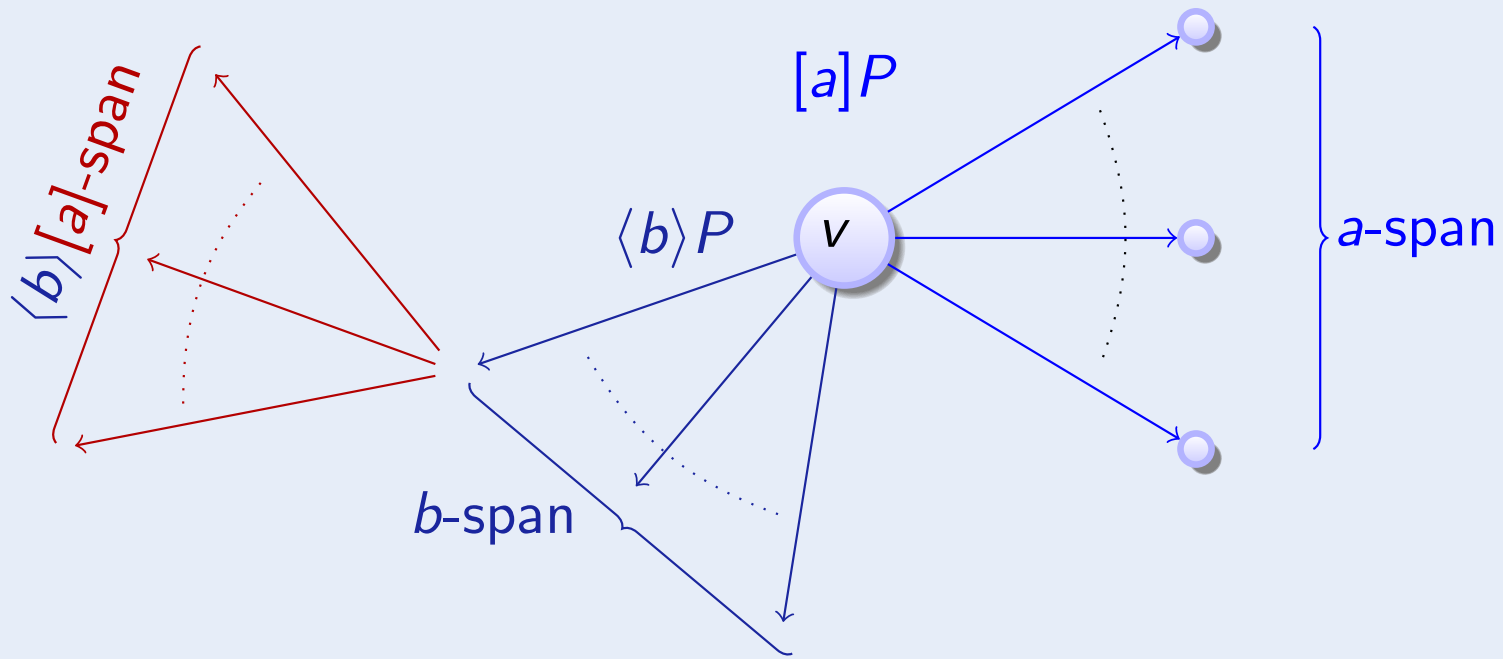
Definition (dℒ Formulas)



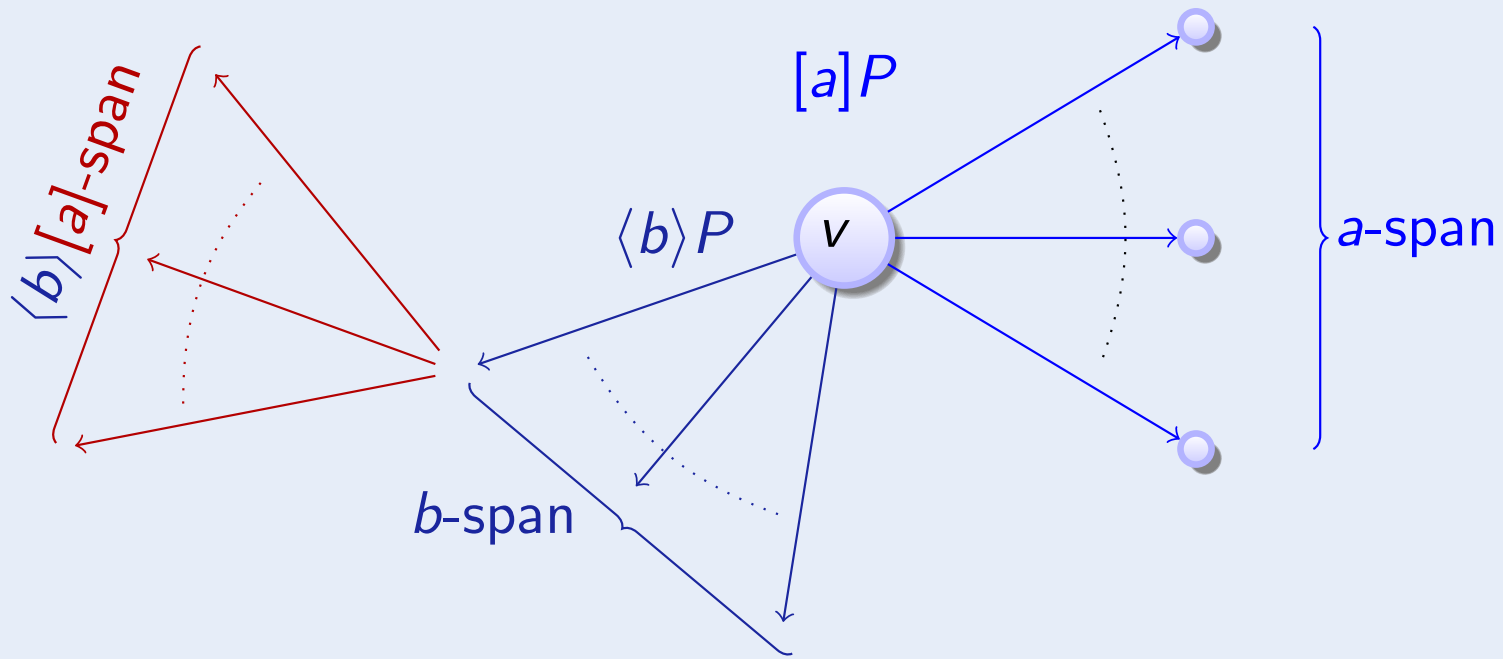
Definition (dℒ Formulas)



Definition (dℒ Formulas)



Definition (dℒ Formulas)



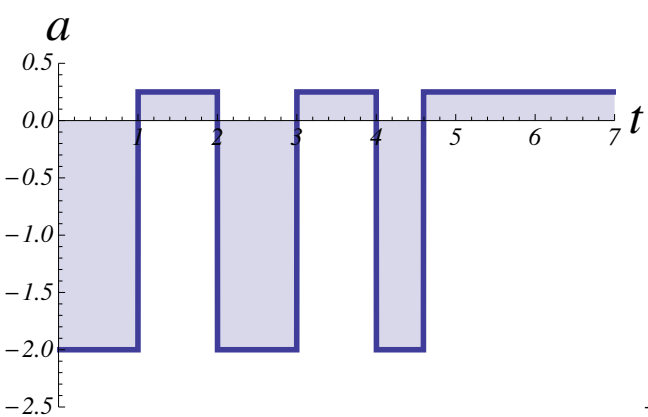
compositional semantics ⇒ compositional proofs!

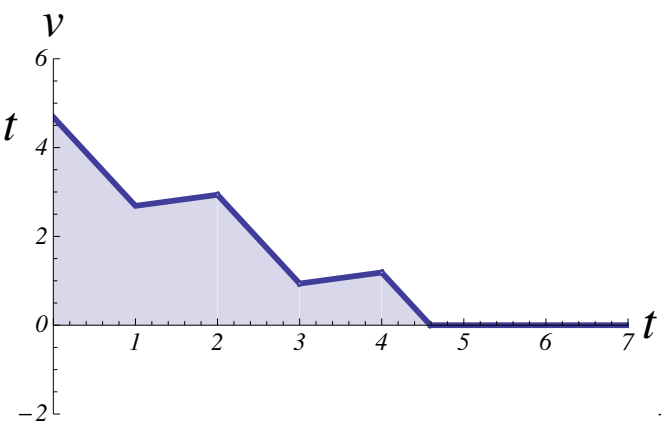
Ex: Car Control

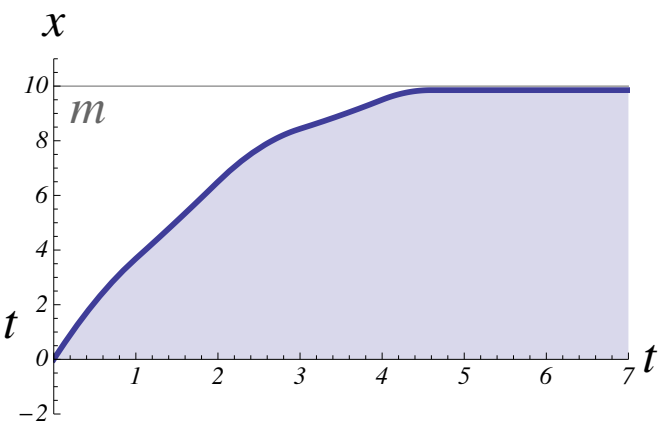
Accelerate condition $?H$

Example (Single car car_s)

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







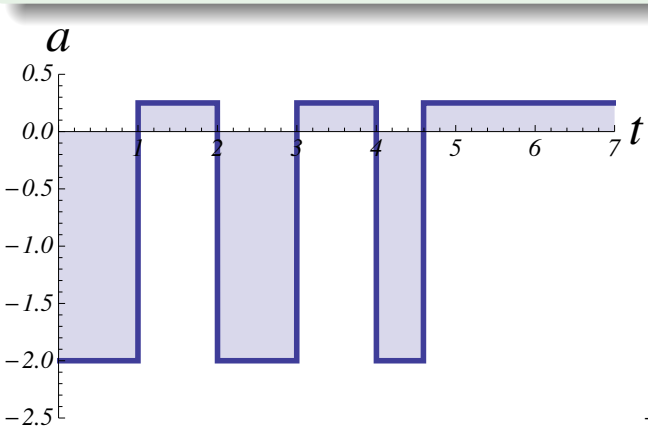
$$H \equiv 2b(m-x) \geq v^2 + (A+b)(A\varepsilon^2 + 2\varepsilon v)$$

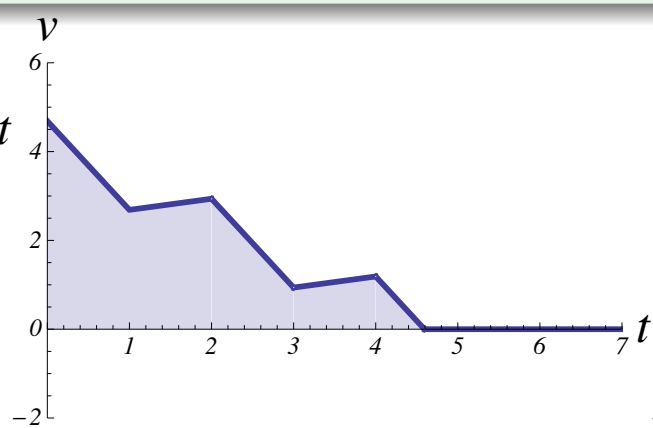
Example (Single car car_ε time-triggered)

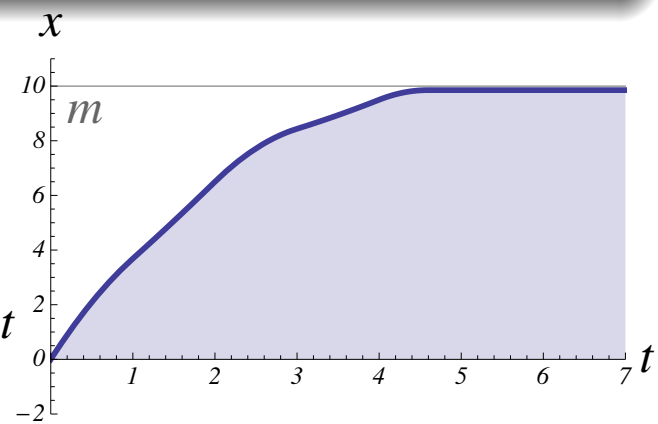
$$\left(((?H; a := A) \cup a := -b);\ t := 0;\ x' = v, v' = a, t' = 1 \,\&\, v \geq 0 \wedge t \leq \varepsilon\right)^*$$

Example (Safely stays before traffic light m)

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







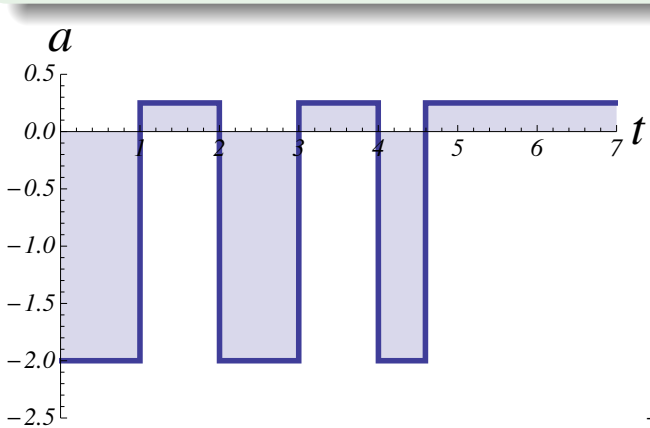
$$H \equiv 2b(m-x) \geq v^2 + (A+b)(A\varepsilon^2 + 2\varepsilon v)$$

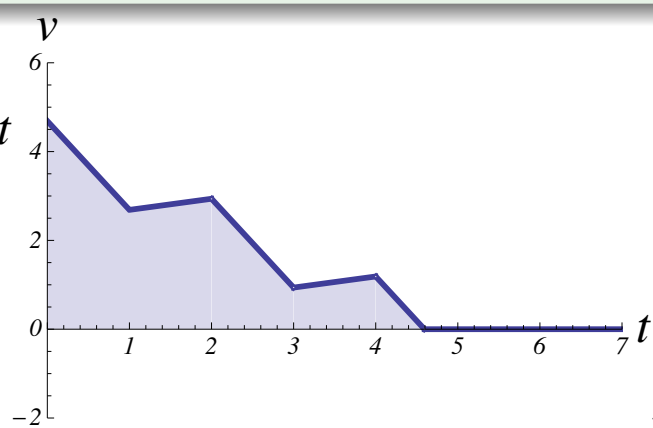
Example (Single car car_ε time-triggered)

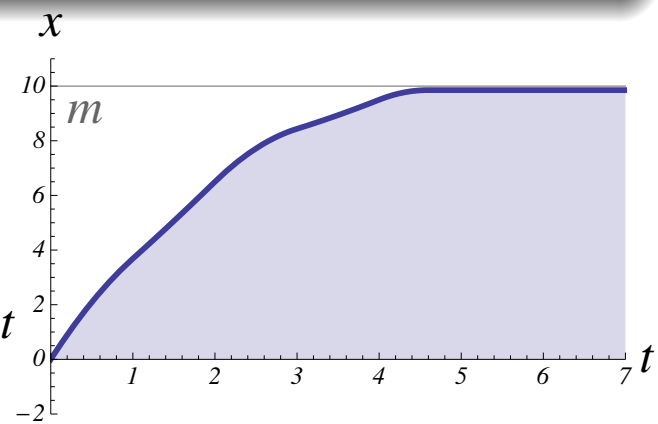
$$\left(((?H; a := A) \cup a := -b);\ t := 0;\ x' = v, v' = a, t' = 1 \,\&\, v \geq 0 \wedge t \leq \varepsilon\right)^*$$

Example (Live, can move everywhere)

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







Outline

Differential Dynamic Logic: Axioms

$$[:=] \quad [x := f]p(x) \leftrightarrow p(f)$$

$$[?] \quad [?q]p \leftrightarrow (q \rightarrow p)$$

$$[\cup] \quad [a \cup b]p(x) \leftrightarrow [a]p(x) \wedge [b]p(x)$$

$$[;] \quad [a; b]p(x) \leftrightarrow [a][b]p(x)$$

$$[^*] \quad [a^*]p(x) \leftrightarrow p(x) \wedge [a][a^*]p(x)$$

$$\mathsf{K} \quad [a](p(x) \rightarrow q(x)) \rightarrow ([a]p(x) \rightarrow [a]q(x))$$

$$\mathsf{I} \quad [a^*](p(x) \rightarrow [a]p(x)) \rightarrow (p(x) \rightarrow [a^*]p(x))$$

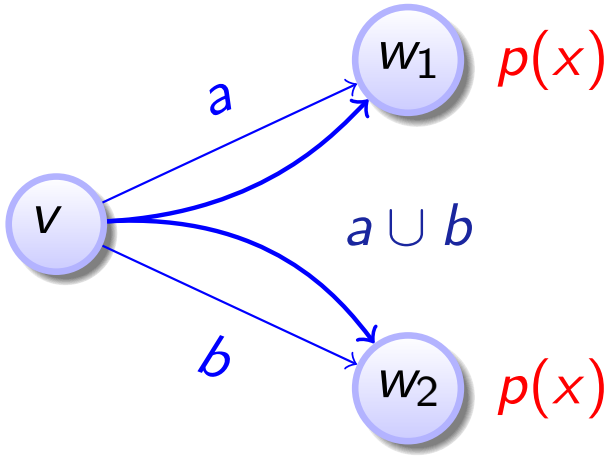
$$\mathsf{V} \quad p \rightarrow [a]p$$

$$\mathsf{DS} \quad [x' = f]p(x) \leftrightarrow \forall t \geq 0\, [x := x + ft]p(x)$$

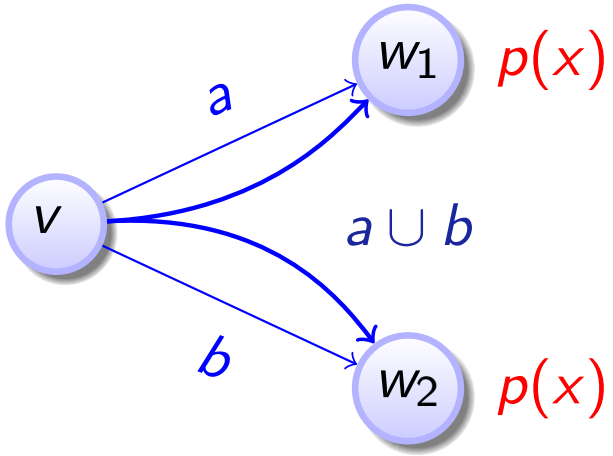
LICS'12,CADE'15

compositional semantics $\Rightarrow$ compositional rules!

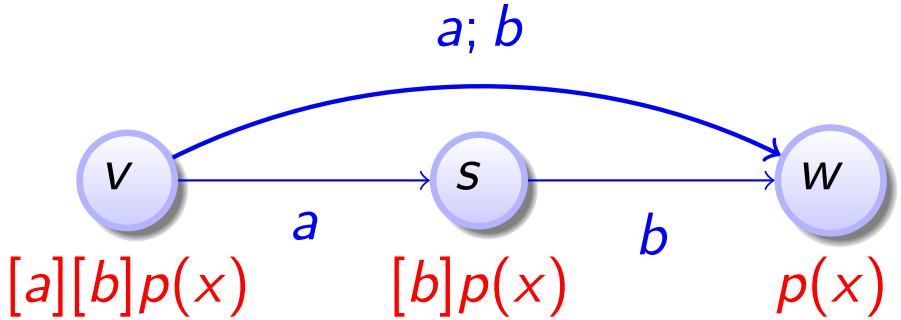
$$\frac{[a]p(x) \land [b]p(x)}{[a \cup b]p(x)}$$



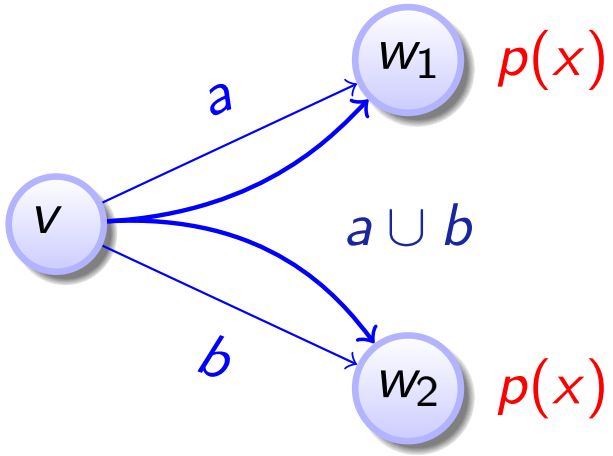
$$\frac{[a]p(x) \wedge [b]p(x)}{[a \cup b]p(x)}$$



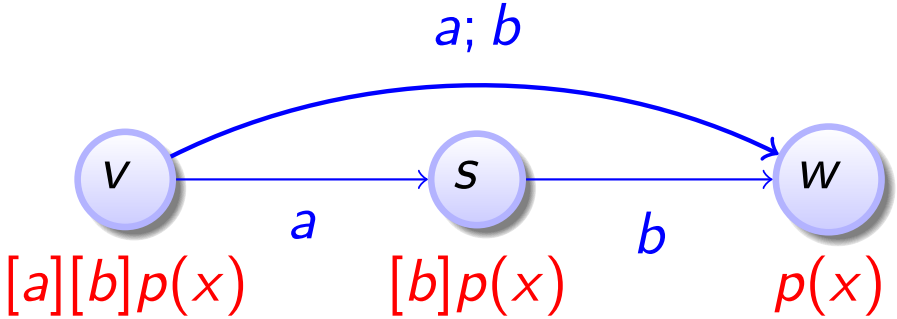
$$\frac{[a][b]p(x)}{[a;b]p(x)}$$



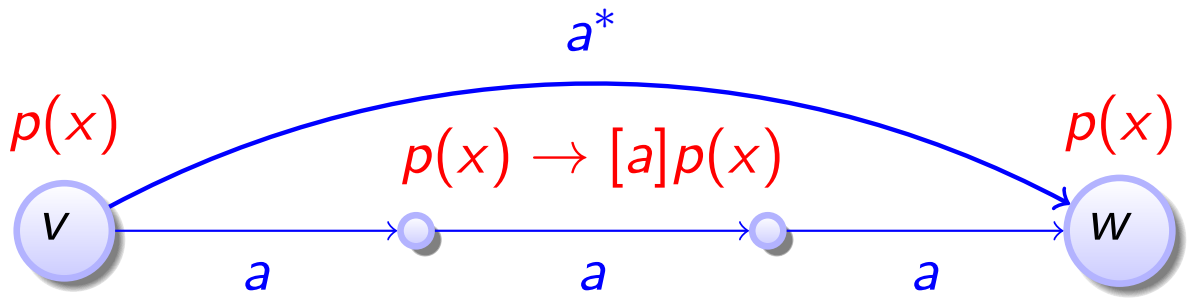
$$\frac{[a]p(x) \wedge [b]p(x)}{[a \cup b]p(x)}$$



$$\frac{[a][b]p(x)}{[a;b]p(x)}$$



$$\frac{p(x) \quad p(x) \rightarrow [a]p(x)}{[a^*]p(x)}$$



Example Proof: Safe Driving

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

$$[;]\ \frac{}{J(x,v) \rightarrow [a := -b; (x' = v, v' = a)]J(x,v)}$$

CADE'15

Example Proof: Safe Driving

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

$$[:=]\frac{}{J(x,v) \rightarrow [a := -b][x' = v, v' = a]J(x,v)}$$
$$[;]\frac{}{J(x,v) \rightarrow [a := -b; (x' = v, v' = a)]J(x,v)}$$

Example Proof: Safe Driving

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

$$[']\ \frac{}{J(x,v) \rightarrow [x' = v, v' = -b]J(x,v)}$$
$$[:=]\ \frac{J(x,v) \rightarrow [a := -b][x' = v, v' = a]J(x,v)}{}$$
$$[;]\ \frac{}{J(x,v) \rightarrow [a := -b; (x' = v, v' = a)]J(x,v)}$$

CADE'15

Example Proof: Safe Driving

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

$$[:=]\frac{J(x,v) \rightarrow \forall t{\geq}0\, [x := -\frac{b}{2}t^2 + vt + x]J(x,v)}{[']\ \dfrac{J(x,v) \rightarrow [x' = v, v' = -b]J(x,v)}{[:=]\ \dfrac{J(x,v) \rightarrow [a := -b][x' = v, v' = a]J(x,v)}{[;]\ \dfrac{J(x,v) \rightarrow [a := -b; (x' = v, v' = a)]J(x,v)}{}}}}$$

Example Proof: Safe Driving

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

$$\text{QE}\,\frac{}{J(x,v) \rightarrow \forall t{\geq}0\,(-\tfrac{b}{2}t^2 + vt + x \leq m)}$$
$$[:=]\,\frac{J(x,v) \rightarrow \forall t{\geq}0\,(-\tfrac{b}{2}t^2 + vt + x \leq m)}{J(x,v) \rightarrow \forall t{\geq}0\,[x := -\tfrac{b}{2}t^2 + vt + x]J(x,v)}$$
$$[']\,\frac{J(x,v) \rightarrow \forall t{\geq}0\,[x := -\tfrac{b}{2}t^2 + vt + x]J(x,v)}{J(x,v) \rightarrow [x' = v, v' = -b]J(x,v)}$$
$$[:=]\,\frac{J(x,v) \rightarrow [x' = v, v' = -b]J(x,v)}{J(x,v) \rightarrow [a := -b][x' = v, v' = a]J(x,v)}$$
$$[;]\,\frac{J(x,v) \rightarrow [a := -b][x' = v, v' = a]J(x,v)}{J(x,v) \rightarrow [a := -b; (x' = v, v' = a)]J(x,v)}$$

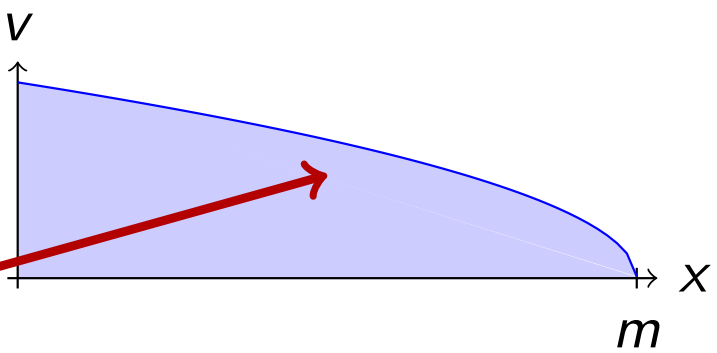
Example Proof: Safe Driving

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

$$\text{QE}\,\frac{J(x,v) \rightarrow v^2 \leq 2b(m-x)}{J(x,v) \rightarrow \forall t{\geq}0\,(-\tfrac{b}{2}t^2 + vt + x \leq m)}$$
$$[:=]\,\frac{J(x,v) \rightarrow \forall t{\geq}0\,(-\tfrac{b}{2}t^2 + vt + x \leq m)}{J(x,v) \rightarrow \forall t{\geq}0\,[x := -\tfrac{b}{2}t^2 + vt + x]J(x,v)}$$
$$[']\,\frac{J(x,v) \rightarrow \forall t{\geq}0\,[x := -\tfrac{b}{2}t^2 + vt + x]J(x,v)}{J(x,v) \rightarrow [x' = v, v' = -b]J(x,v)}$$
$$[:=]\,\frac{J(x,v) \rightarrow [x' = v, v' = -b]J(x,v)}{J(x,v) \rightarrow [a := -b][x' = v, v' = a]J(x,v)}$$
$$[;]\,\frac{J(x,v) \rightarrow [a := -b][x' = v, v' = a]J(x,v)}{J(x,v) \rightarrow [a := -b; (x' = v, v' = a)]J(x,v)}$$

Example Proof: Safe Driving

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



$$\dfrac{J(x,v) \rightarrow v^2 \leq 2b(m-x)}{J(x,v) \rightarrow \forall t{\geq}0\,(-\frac{b}{2}t^2+vt+x \leq m)}\,\text{QE}$$

$$\dfrac{J(x,v) \rightarrow \forall t{\geq}0\,(-\frac{b}{2}t^2+vt+x \leq m)}{J(x,v) \rightarrow \forall t{\geq}0\,[x:=-\frac{b}{2}t^2+vt+x]J(x,v)}\,[:=]$$

$$\dfrac{J(x,v) \rightarrow \forall t{\geq}0\,[x:=-\frac{b}{2}t^2+vt+x]J(x,v)}{J(x,v) \rightarrow [x'=v,v'=-b]J(x,v)}\,[']$$

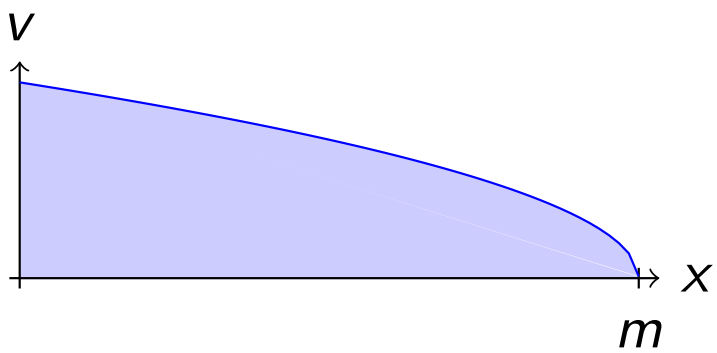
$$\dfrac{J(x,v) \rightarrow [x'=v,v'=-b]J(x,v)}{J(x,v) \rightarrow [a:=-b][x'=v,v'=a]J(x,v)}\,[:=]$$

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

CADE'15

Example Proof: Safe Driving

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

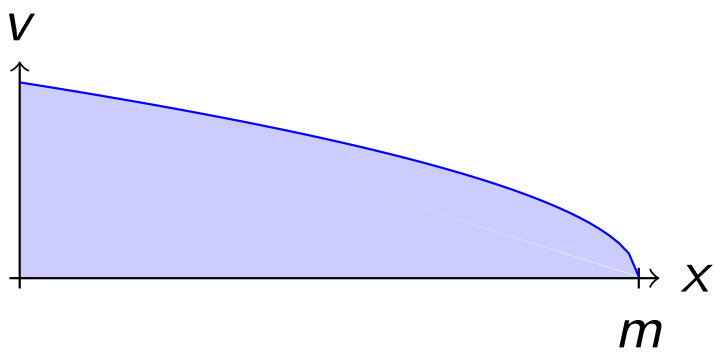


$$[;]\ \frac{}{J(x,v) \rightarrow [?\neg \mathsf{SB}; a := A; (x' = v, v' = a, t' = 1 \,\&\, t \leq \varepsilon)]J(x,v)}$$

CADE'15

Example Proof: Safe Driving

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

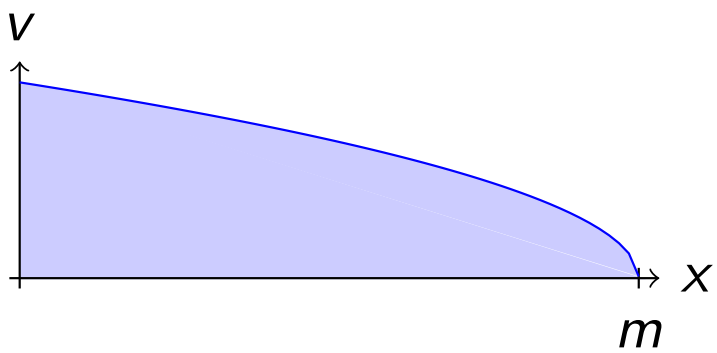


$$[?]\ \frac{}{J(x,v) \rightarrow [?\neg \mathsf{SB}][a := A; (x' = v, v' = a, t' = 1 \,\&\, t \leq \varepsilon)]J(x,v)}$$
$$[;]\ \frac{}{J(x,v) \rightarrow [?\neg \mathsf{SB}; a := A; (x' = v, v' = a, t' = 1 \,\&\, t \leq \varepsilon)]J(x,v)}$$

CADE'15

Example Proof: Safe Driving

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



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

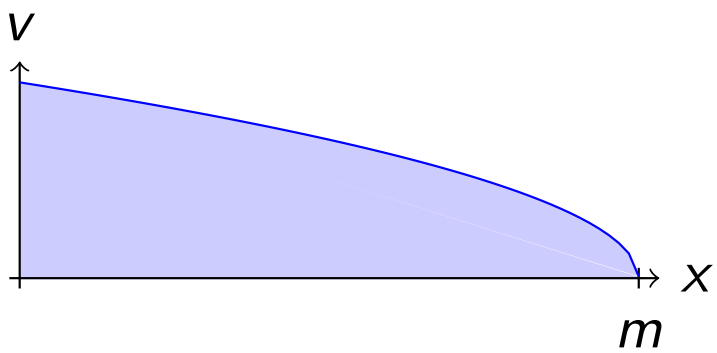
$$[?]\ \frac{J(x,v) \rightarrow [?\neg \mathsf{SB}][a := A; (x' = v, v' = a, t' = 1 \,\&\, t \leq \varepsilon)]J(x,v)}{J(x,v) \rightarrow [?\neg \mathsf{SB}; a := A; (x' = v, v' = a, t' = 1 \,\&\, t \leq \varepsilon)]J(x,v)}$$

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

CADE'15

Example Proof: Safe Driving

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

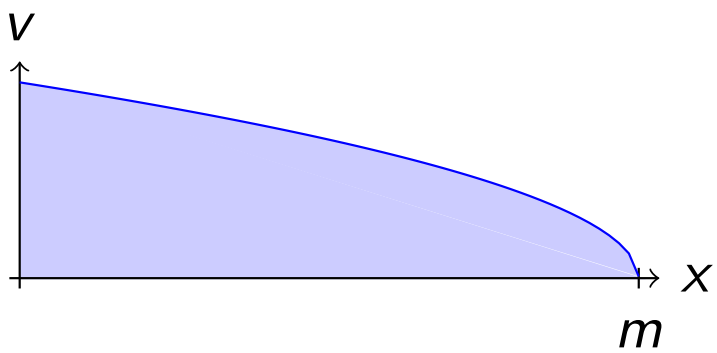


$$\dfrac{\dfrac{\dfrac{\dfrac{}{J(x,v) \to \neg \mathsf{SB} \to [a := A][x' = v, v' = a, t' = 1 \,\&\, t \leq \varepsilon]J(x,v)}[:=]}{J(x,v) \to \neg \mathsf{SB} \to [a := A; (x' = v, v' = a, t' = 1 \,\&\, t \leq \varepsilon)]J(x,v)}[;]}{J(x,v) \to [?\neg \mathsf{SB}][a := A; (x' = v, v' = a, t' = 1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

CADE'15

Example Proof: Safe Driving

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



$$[']\ \frac{}{J(x,v) \rightarrow \neg \mathsf{SB} \rightarrow [x' = v, v' = A, t' = 1 \,\&\, t \leq \varepsilon] J(x,v)}$$

$$[:=]\ \frac{}{J(x,v) \rightarrow \neg \mathsf{SB} \rightarrow [a := A][x' = v, v' = a, t' = 1 \,\&\, t \leq \varepsilon] J(x,v)}$$

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

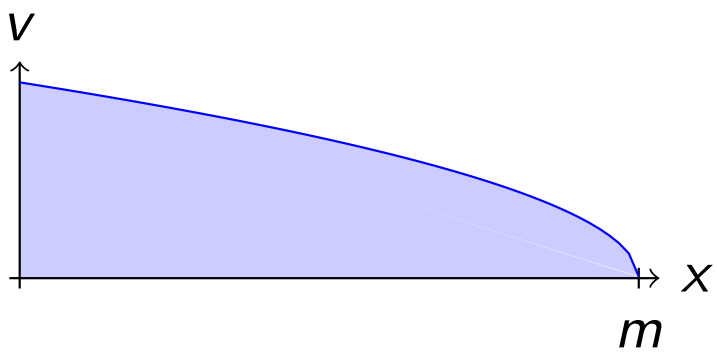
$$[?]\ \frac{}{J(x,v) \rightarrow [?\neg \mathsf{SB}][a := A; (x' = v, v' = a, t' = 1 \,\&\, t \leq \varepsilon)] J(x,v)}$$

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

CADE'15

Example Proof: Safe Driving

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



$$[:=]\ \frac{J(x,v) \rightarrow \neg \mathsf{SB} \rightarrow \forall t{\geq}0\,(t \leq \varepsilon \rightarrow [x := \frac{A}{2}t^2 + vt + x]J(x,v))}{}$$

$$[']\ \frac{J(x,v) \rightarrow \neg \mathsf{SB} \rightarrow [x' = v, v' = A, t' = 1 \,\&\, t \leq \varepsilon]J(x,v)}{}$$

$$[:=]\ \frac{J(x,v) \rightarrow \neg \mathsf{SB} \rightarrow [a := A][x' = v, v' = a, t' = 1 \,\&\, t \leq \varepsilon]J(x,v)}{}$$

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

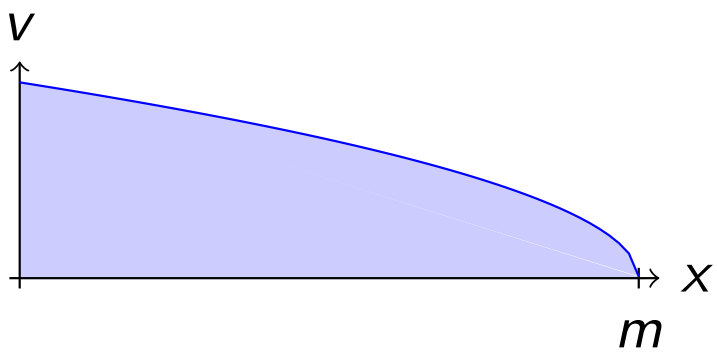
$$[?]\ \frac{J(x,v) \rightarrow [?\neg \mathsf{SB}][a := A; (x' = v, v' = a, t' = 1 \,\&\, t \leq \varepsilon)]J(x,v)}{}$$

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

CADE'15

Example Proof: Safe Driving

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



$$\frac{}{J(x,v) \rightarrow \neg \mathsf{SB} \rightarrow \forall t{\geq}0\,(t \leq \varepsilon \rightarrow J(\tfrac{A}{2}t^2 + vt + x, At + v))}$$

$$[:=]\ \frac{J(x,v) \rightarrow \neg \mathsf{SB} \rightarrow \forall t{\geq}0\,(t \leq \varepsilon \rightarrow [x := \tfrac{A}{2}t^2 + vt + x]J(x,v))}{J(x,v) \rightarrow \neg \mathsf{SB} \rightarrow \forall t{\geq}0\,(t \leq \varepsilon \rightarrow J(\tfrac{A}{2}t^2 + vt + x, At + v))}$$

$$[']\ \frac{J(x,v) \rightarrow \neg \mathsf{SB} \rightarrow [x' = v, v' = A, t' = 1\,\&\, t \leq \varepsilon]J(x,v)}{J(x,v) \rightarrow \neg \mathsf{SB} \rightarrow \forall t{\geq}0\,(t \leq \varepsilon \rightarrow [x := \tfrac{A}{2}t^2 + vt + x]J(x,v))}$$

$$[:=]\ \frac{J(x,v) \rightarrow \neg \mathsf{SB} \rightarrow [a := A][x' = v, v' = a, t' = 1\,\&\, t \leq \varepsilon]J(x,v)}{J(x,v) \rightarrow \neg \mathsf{SB} \rightarrow [x' = v, v' = A, t' = 1\,\&\, t \leq \varepsilon]J(x,v)}$$

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

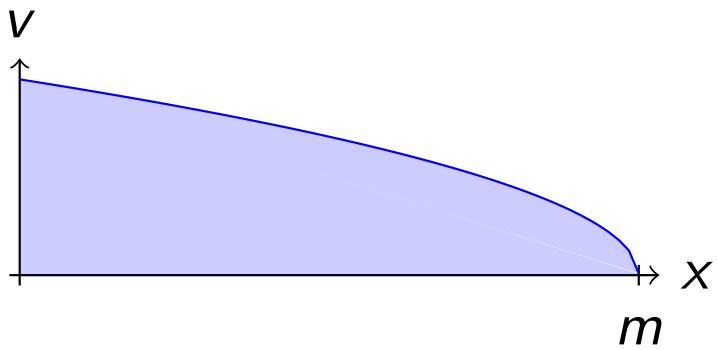
$$[?]\ \frac{J(x,v) \rightarrow [?\neg \mathsf{SB}][a := A; (x' = v, v' = a, t' = 1\,\&\, t \leq \varepsilon)]J(x,v)}{J(x,v) \rightarrow \neg \mathsf{SB} \rightarrow [a := A; (x' = v, v' = a, t' = 1\,\&\, t \leq \varepsilon)]J(x,v)}$$

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

CADE'15

Example Proof: Safe Driving

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



$$\text{QE}\ \frac{J(x,v) \rightarrow \neg\text{SB} \rightarrow \forall t{\geq}0\,(t \leq \varepsilon \rightarrow (At+v)^2 \leq 2b(m-\frac{A}{2}t^2-vt-x))}{J(x,v) \rightarrow \neg\text{SB} \rightarrow \forall t{\geq}0\,(t \leq \varepsilon \rightarrow J(\frac{A}{2}t^2+vt+x, At+v))}$$

$$[:=]\ \frac{J(x,v) \rightarrow \neg\text{SB} \rightarrow \forall t{\geq}0\,(t \leq \varepsilon \rightarrow [x := \frac{A}{2}t^2+vt+x]J(x,v))}{J(x,v) \rightarrow \neg\text{SB} \rightarrow \forall t{\geq}0\,(t \leq \varepsilon \rightarrow J(\frac{A}{2}t^2+vt+x, At+v))}$$

$$[']\ \frac{J(x,v) \rightarrow \neg\text{SB} \rightarrow [x'=v, v'=A, t'=1\,\&\,t \leq \varepsilon]J(x,v)}{J(x,v) \rightarrow \neg\text{SB} \rightarrow \forall t{\geq}0\,(t \leq \varepsilon \rightarrow [x := \frac{A}{2}t^2+vt+x]J(x,v))}$$

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

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

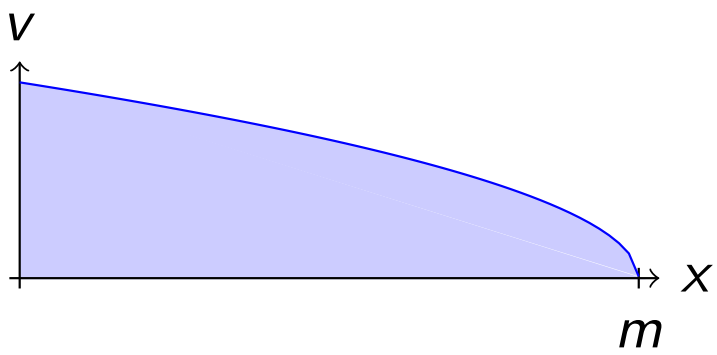
$$[?]\ \frac{J(x,v) \rightarrow [?\neg\text{SB}][a := A; (x'=v, v'=a, t'=1\,\&\,t \leq \varepsilon)]J(x,v)}{J(x,v) \rightarrow \neg\text{SB} \rightarrow [a := A; (x'=v, v'=a, t'=1\,\&\,t \leq \varepsilon)]J(x,v)}$$

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

CADE'15

Example Proof: Safe Driving

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



$$\text{QE}\ \frac{J(x,v) \to \neg\text{SB} \to (A\varepsilon+v)^2 \leq 2b(m-\frac{A}{2}\varepsilon^2-v\varepsilon-x)}{J(x,v) \to \neg\text{SB} \to \forall t{\geq}0\,(t \leq \varepsilon \to (At+v)^2 \leq 2b(m-\frac{A}{2}t^2-vt-x))}$$

$$\frac{J(x,v) \to \neg\text{SB} \to \forall t{\geq}0\,(t \leq \varepsilon \to J(\frac{A}{2}t^2+vt+x, At+v))}{J(x,v) \to \neg\text{SB} \to \forall t{\geq}0\,(t \leq \varepsilon \to [x := \frac{A}{2}t^2+vt+x]J(x,v))}\ [:=]$$

$$\frac{J(x,v) \to \neg\text{SB} \to [x'=v, v'=A, t'=1\,\&\,t \leq \varepsilon]J(x,v)}{J(x,v) \to \neg\text{SB} \to \forall t{\geq}0\,(t \leq \varepsilon \to [x := \frac{A}{2}t^2+vt+x]J(x,v))}\ [']$$

$$\frac{J(x,v) \to \neg\text{SB} \to [a := A][x'=v, v'=a, t'=1\,\&\,t \leq \varepsilon]J(x,v)}{J(x,v) \to \neg\text{SB} \to [x'=v, v'=A, t'=1\,\&\,t \leq \varepsilon]J(x,v)}\ [:=]$$

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

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

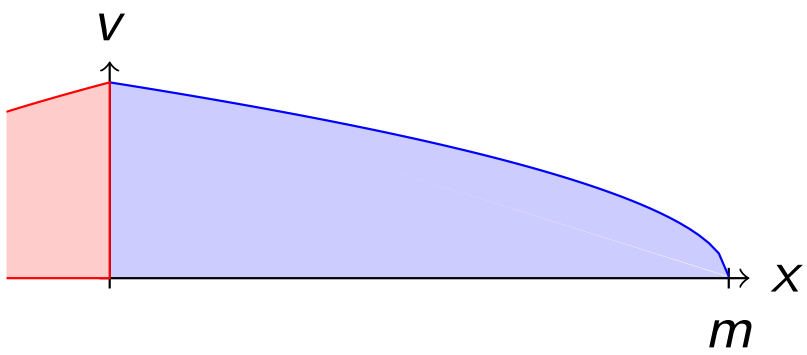
$$\frac{J(x,v) \to [?\neg\text{SB}; a := A; (x'=v, v'=a, t'=1\,\&\,t \leq \varepsilon)]J(x,v)}{J(x,v) \to [?\neg\text{SB}][a := A; (x'=v, v'=a, t'=1\,\&\,t \leq \varepsilon)]J(x,v)}\ [;]$$

CADE'15

Example Proof: Safe Driving

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

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

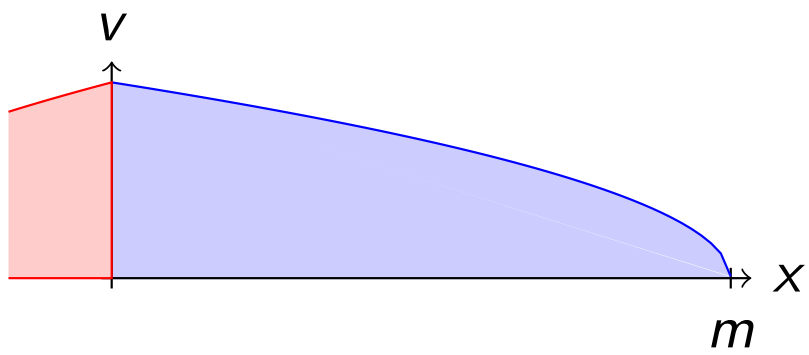


$$
\begin{array}{ll}
 & J(x,v) \rightarrow \neg\text{SB} \rightarrow (A\varepsilon + v)^2 \leq 2b(m - \frac{A}{2}\varepsilon^2 - v\varepsilon - x) \\
\hline
\text{QE} & J(x,v) \rightarrow \neg\text{SB} \rightarrow \forall t{\geq}0\,(t \leq \varepsilon \rightarrow (At+v)^2 \leq 2b(m - \tfrac{A}{2}t^2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

CADE'15

Example Proof: Safe Driving

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



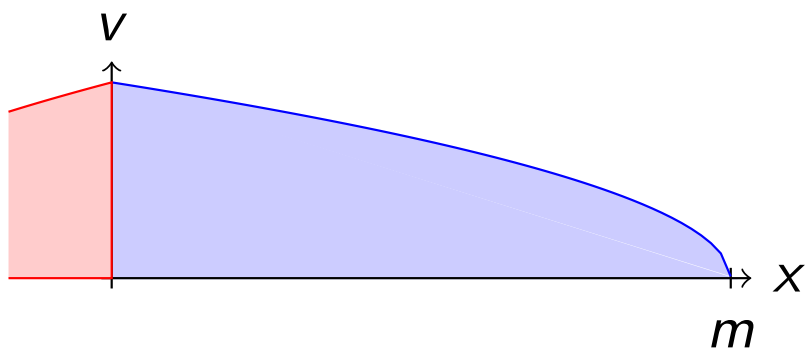
$$\text{ind}\frac{}{J(x,v) \rightarrow [((a := -b \cup ?\neg\text{SB}; a := A); x'' = a, t' = 1 \,\&\, t \leq \varepsilon)^*]J(x,v)}$$

CADE'15

Example Proof: Safe Driving

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

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



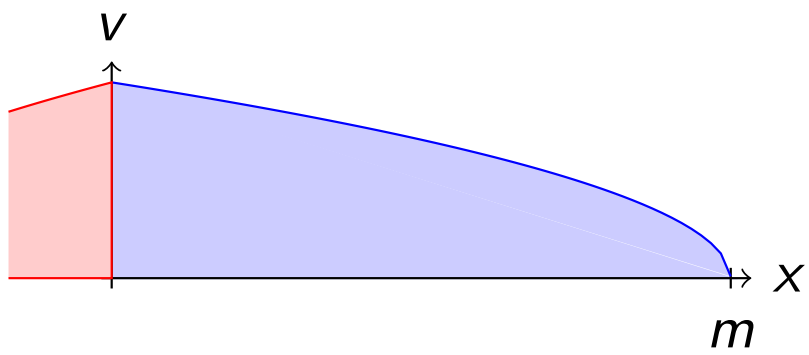
$$\text{ind}\,\frac{\text{[;]}\,\dfrac{J(x,v) \rightarrow [(a := -b \cup ?\neg \text{SB}; a := A); x'' = a, t' = 1 \,\&\, t \leq \varepsilon] J(x,v)}{J(x,v) \rightarrow [((a := -b \cup ?\neg \text{SB}; a := A); x'' = a, t' = 1 \,\&\, t \leq \varepsilon)^*] J(x,v)}$$

CADE'15

Example Proof: Safe Driving

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

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



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

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

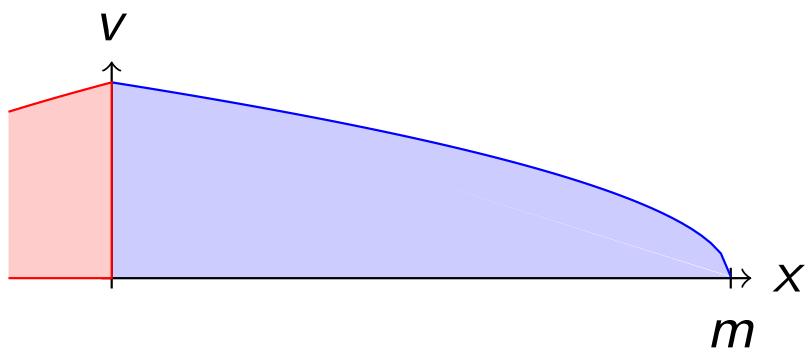
$$\text{ind}\ \frac{}{J(x,v) \rightarrow [\big((a := -b \cup ?\neg\text{SB}; a := A); x'' = a, t' = 1 \,\&\, t \leq \varepsilon\big)^*]J(x,v)}$$

CADE'15

Example Proof: Safe Driving

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

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



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

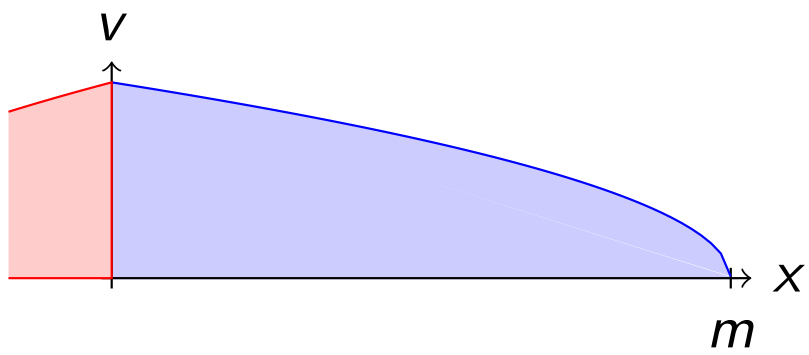
$$\dfrac{}{J(x,v) \to [\big((a := -b \cup ?\neg \text{SB}; a := A); x'' = a, t' = 1 \,\&\, t \leq \varepsilon\big)^*]J(x,v)}\text{ind}$$

CADE'15

Example Proof: Safe Driving

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

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



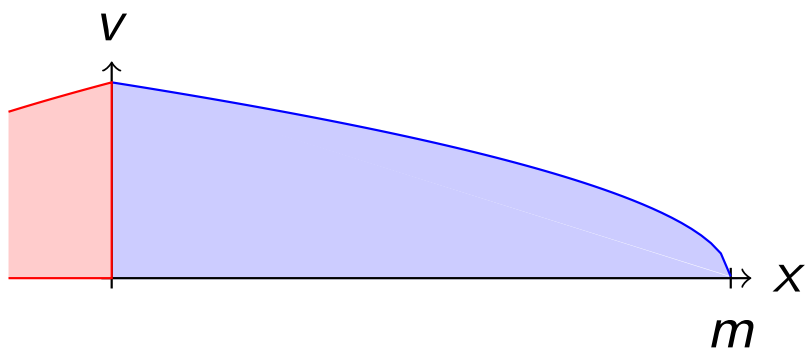
previous proofs for braking and acceleration

$$\cfrac{\cfrac{\cfrac{\cfrac{J(x,v) \rightarrow [a := -b][x'' = a\,..]J(x,v) \wedge [?\neg \text{SB}; a := A][x'' = a\,..]J(x,v)}{J(x,v) \rightarrow [a := -b \cup ?\neg \text{SB}; a := A][x'' = a, t' = 1 \,\&\, t \leq \varepsilon]J(x,v)}\,[\cup]}{J(x,v) \rightarrow [(a := -b \cup ?\neg \text{SB}; a := A); x'' = a, t' = 1 \,\&\, t \leq \varepsilon]J(x,v)}\,[;]}{J(x,v) \rightarrow [\big((a := -b \cup ?\neg \text{SB}; a := A); x'' = a, t' = 1 \,\&\, t \leq \varepsilon\big)^*]J(x,v)}\,\text{ind}$$

Example Proof: Safe Driving

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

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



previous proofs for braking and acceleration

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

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

1. Proof is essentially deterministic "follow your nose"
2. Synthesize invariant $J(,)$ and parameter constraint SB
3. $J(x,v)$ is a predicate symbol to prove only once and instantiate later

Outline

Complete Proof Theory of Hybrid Systems

Theorem (Sound & Complete) (J.Autom.Reas. 2008, LICS'12)

$d\mathcal{L}$ calculus is a sound & complete axiomatization of hybrid systems relative to either differential equations **or** *discrete dynamics.* ▸ Proof 25pp

Corollary (Complete Proof-theoretical Alignment & Bridging)

$$\text{proving continuous} = \text{proving hybrid} = \text{proving discrete}$$

JAutomReas'08,LICS'12

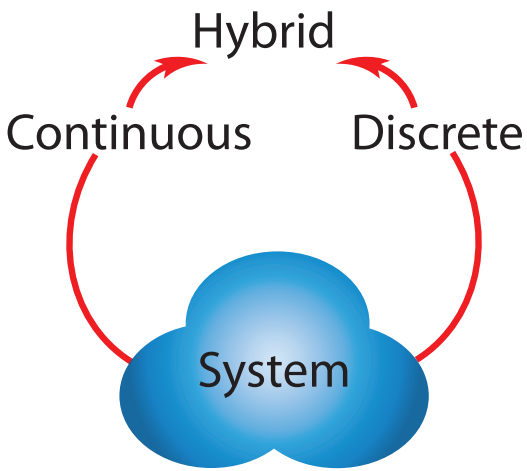
Complete Proof Theory of Hybrid Systems

Theorem (Sound & Complete) (J.Autom.Reas. 2008, LICS'12)

dL calculus is a sound & complete axiomatization of hybrid systems relative to either differential equations **or** *discrete dynamics.* ▸ Proof 25pp

Corollary (Complete Proof-theoretical Alignment & Bridging)

proving continuous = proving hybrid = proving discrete



JAutomReas'08,LICS'12

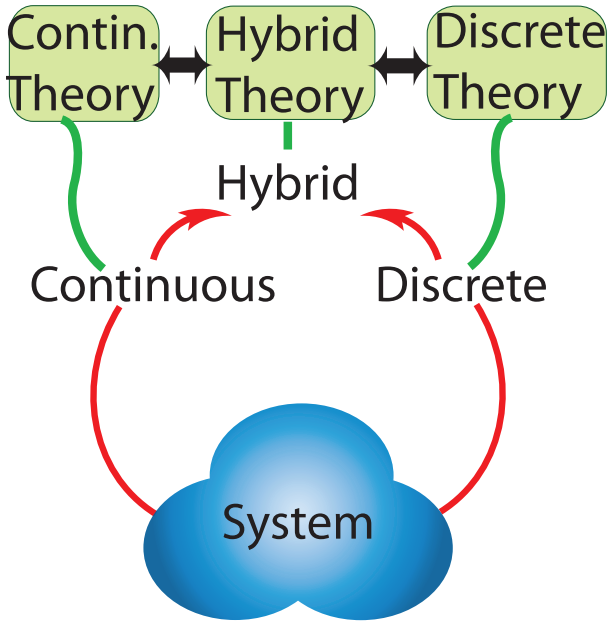
Complete Proof Theory of Hybrid Systems

Theorem (Sound & Complete) (J.Autom.Reas. 2008, LICS'12)

dℒ calculus is a sound & complete axiomatization of hybrid systems relative to either differential equations **or** *discrete dynamics.* ▸ Proof 25pp

Corollary (Complete Proof-theoretical Alignment & Bridging)

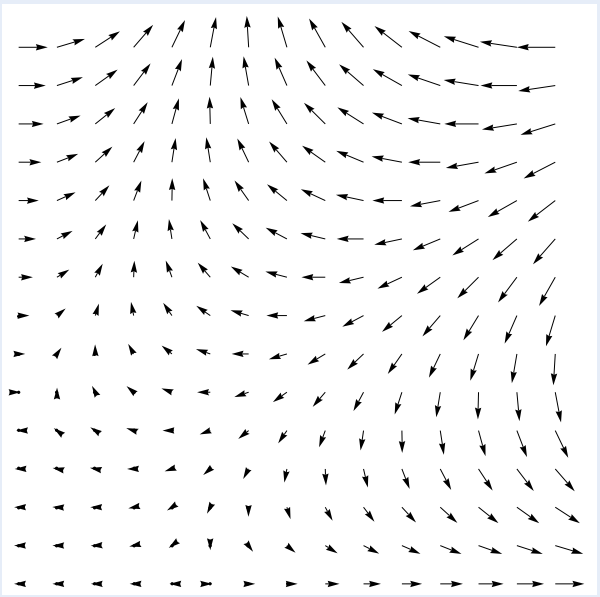
proving continuous = proving hybrid = proving discrete



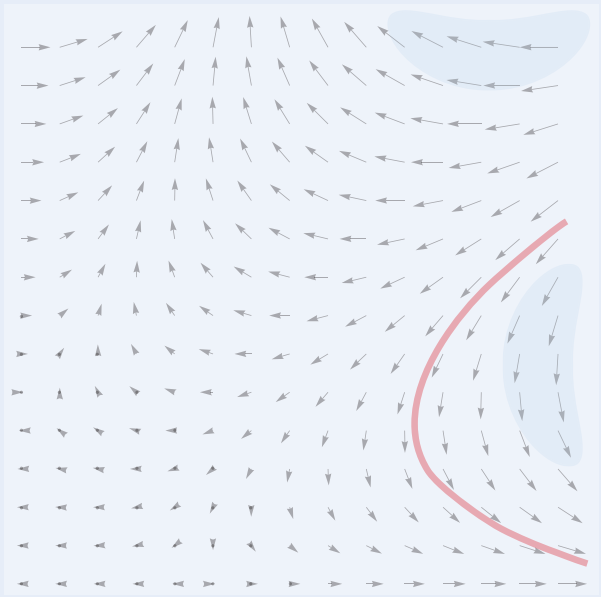
JAutomReas'08,LICS'12

Differential Invariants for Differential Equations

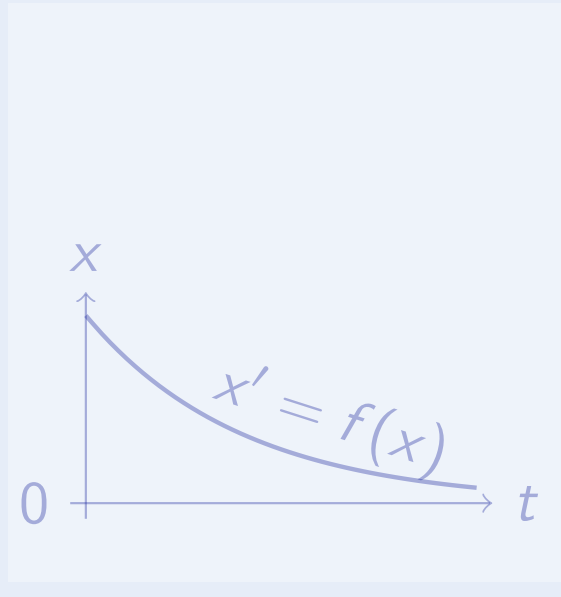
Differential Invariant

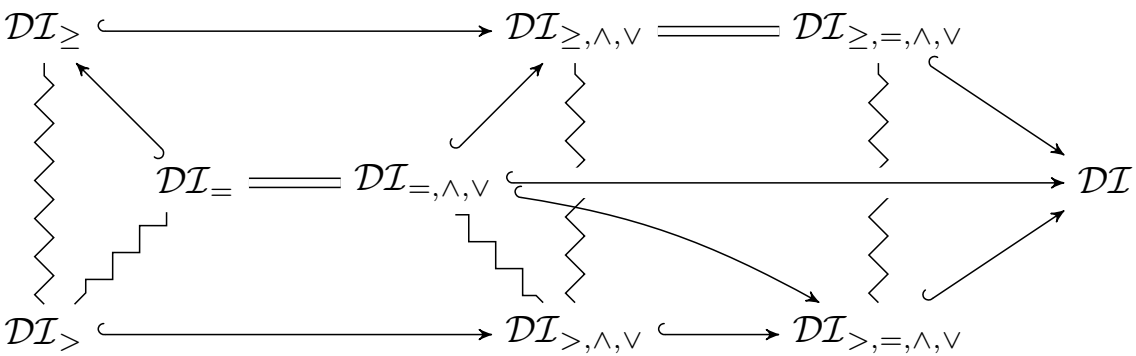


Differential Cut



Differential Ghost





Logic

Provability theory

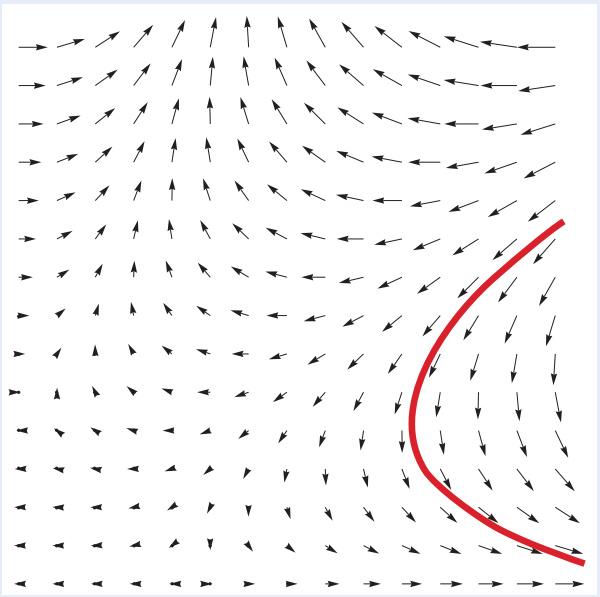
Math

Characteristic PDE

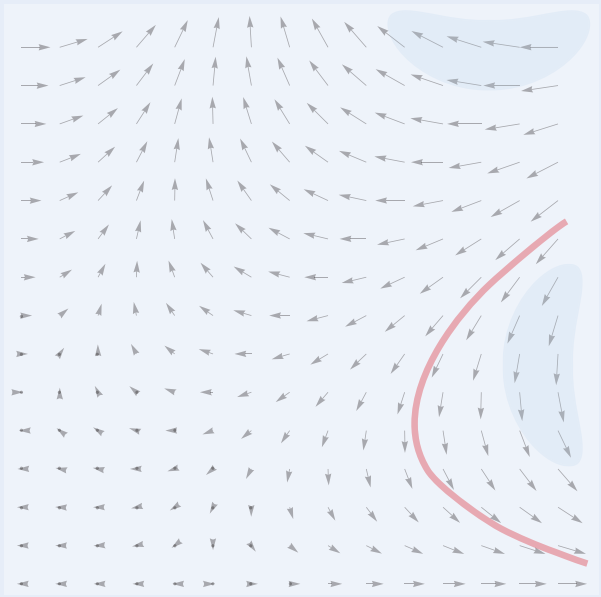
JLogComput'10,CAV'08,FMSD'09,LMCS'12,ITP'12

Differential Invariants for Differential Equations

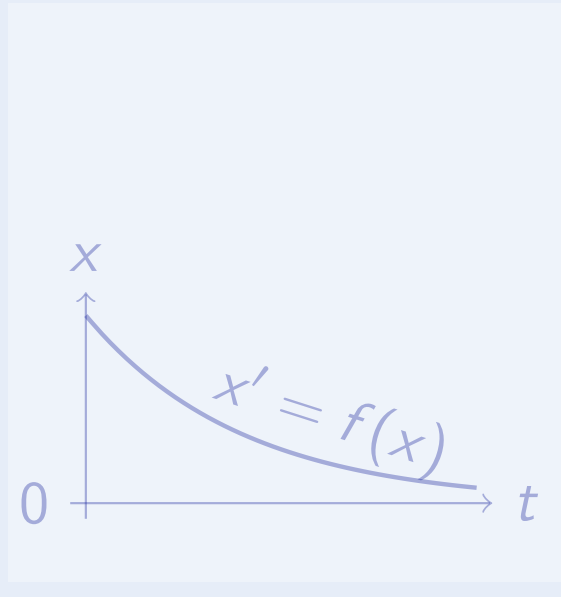
Differential Invariant

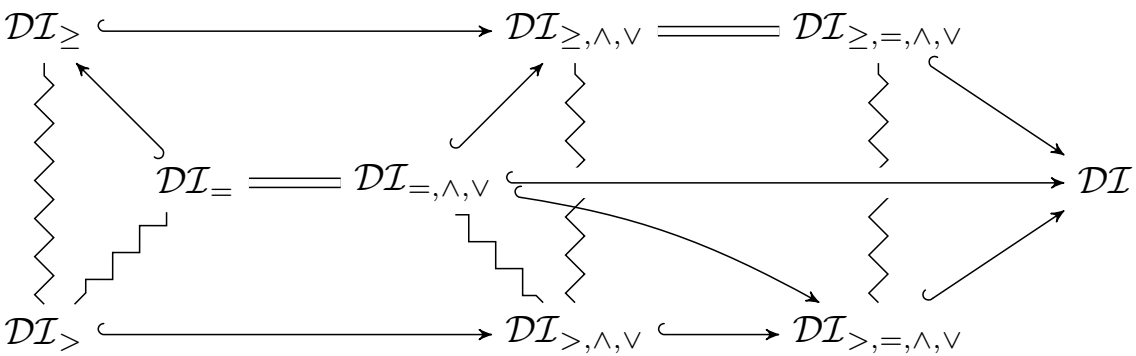


Differential Cut



Differential Ghost





Logic

Provability theory

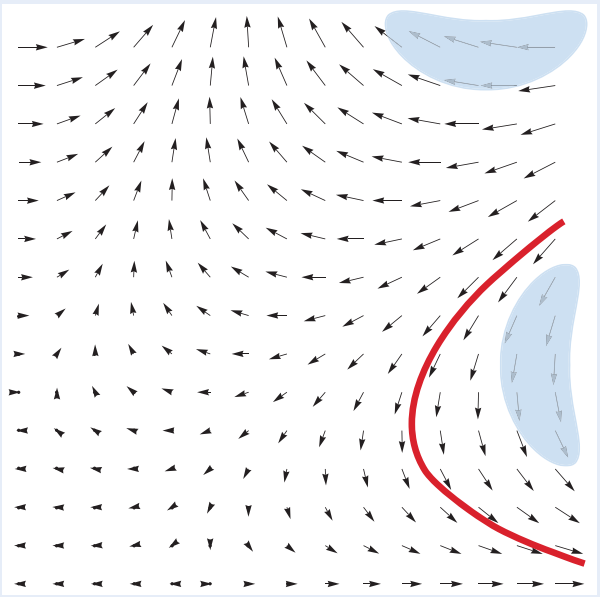
Math

Characteristic PDE

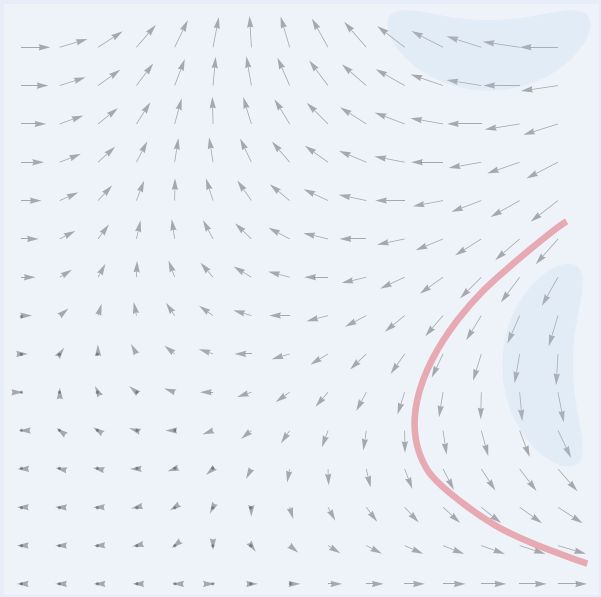
JLogComput'10,CAV'08,FMSD'09,LMCS'12,ITP'12

Differential Invariants for Differential Equations

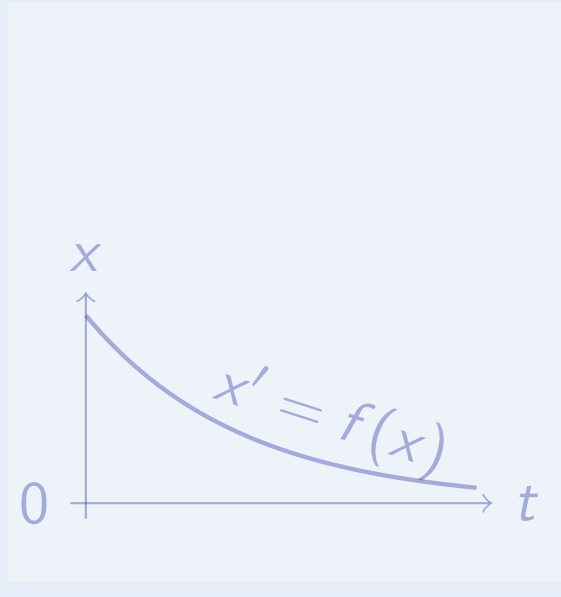
Differential Invariant

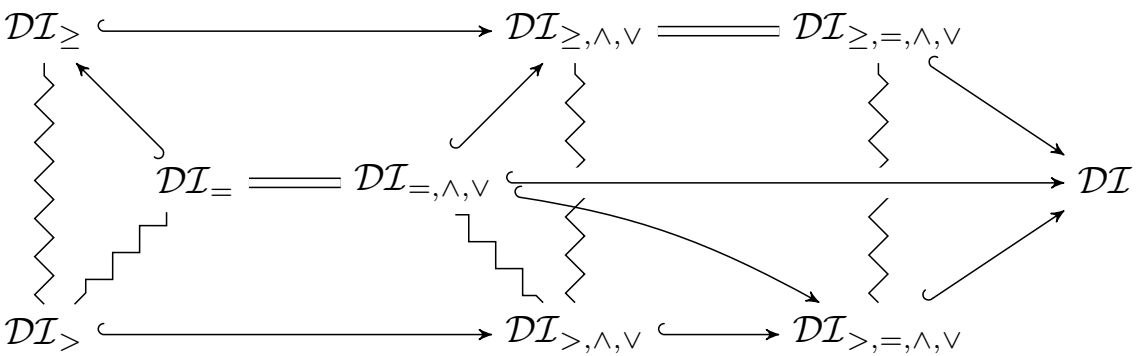


Differential Cut



Differential Ghost





Logic

Provability theory

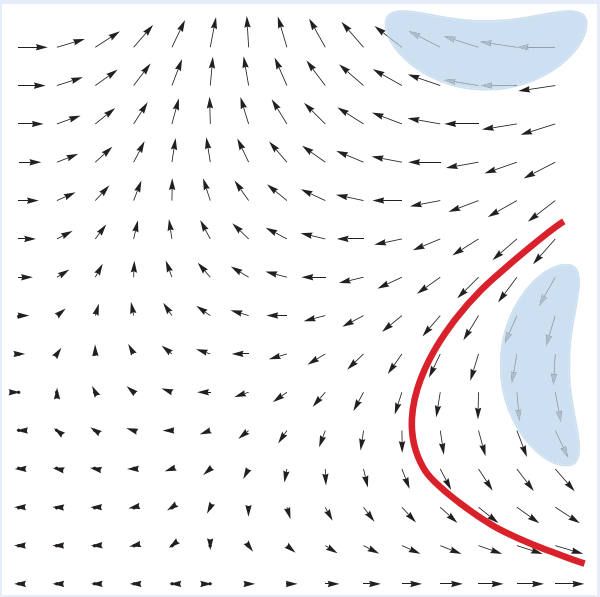
Math

Characteristic PDE

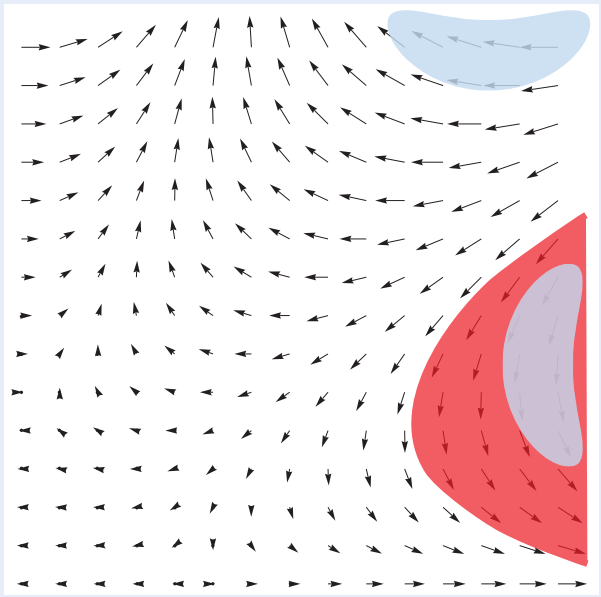
JLogComput'10,CAV'08,FMSD'09,LMCS'12,ITP'12

Differential Invariants for Differential Equations

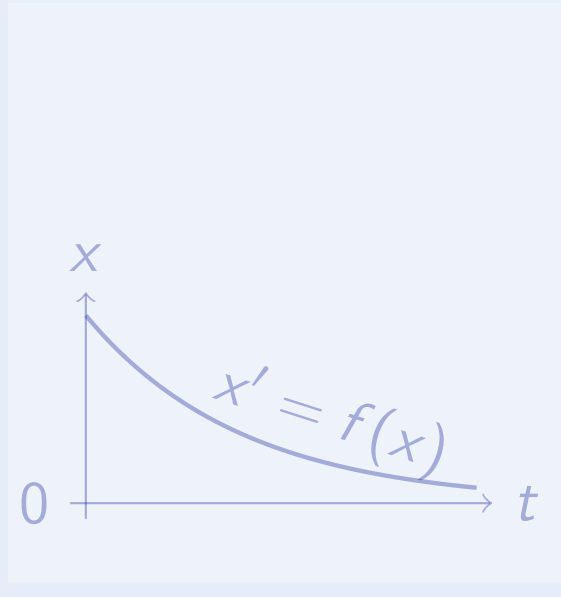
Differential Invariant

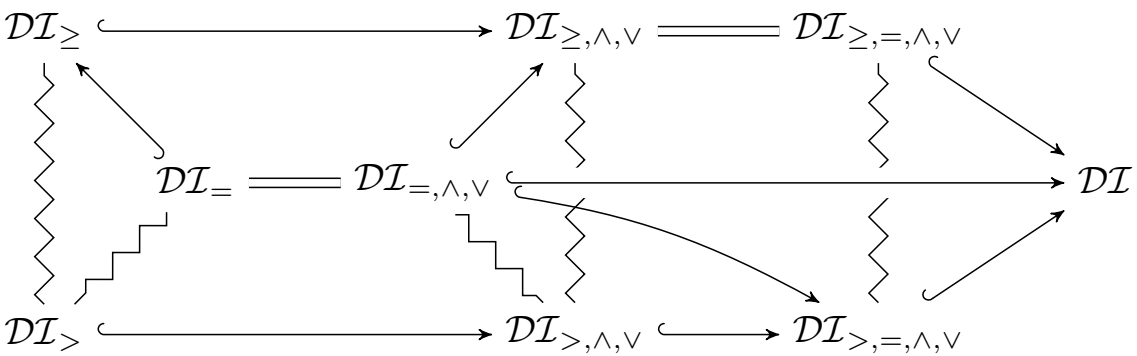


Differential Cut



Differential Ghost





Logic

Provability theory

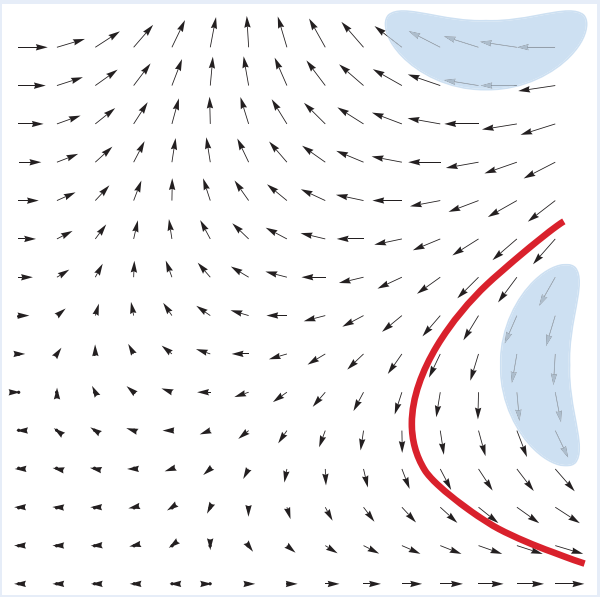
Math

Characteristic PDE

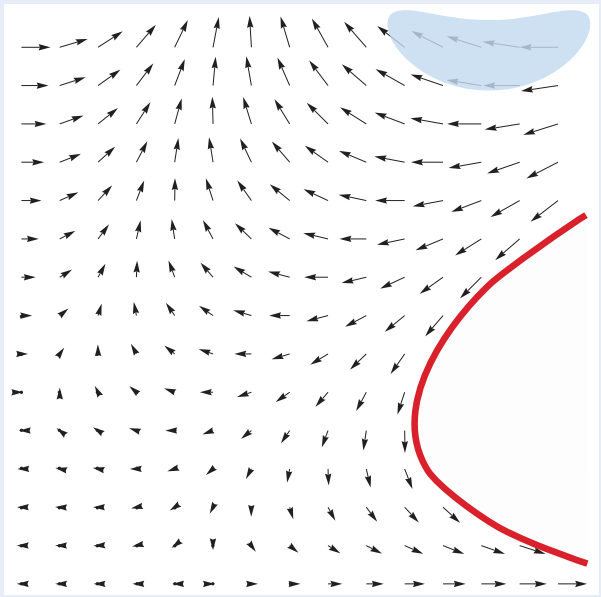
JLogComput'10,CAV'08,FMSD'09,LMCS'12,ITP'12

Differential Invariants for Differential Equations

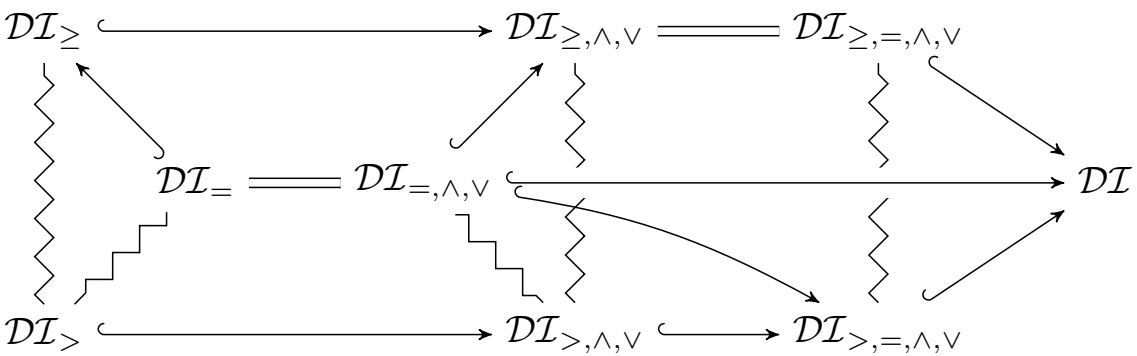
Differential Invariant



Differential Cut



Differential Ghost



Logic

Provability theory

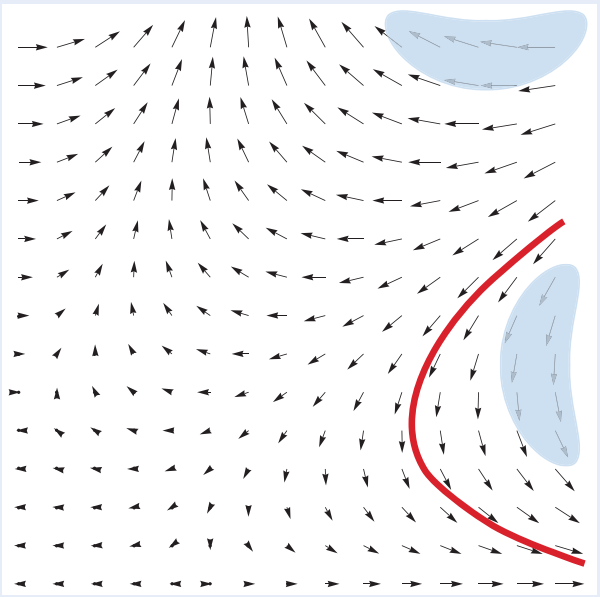
Math

Characteristic PDE

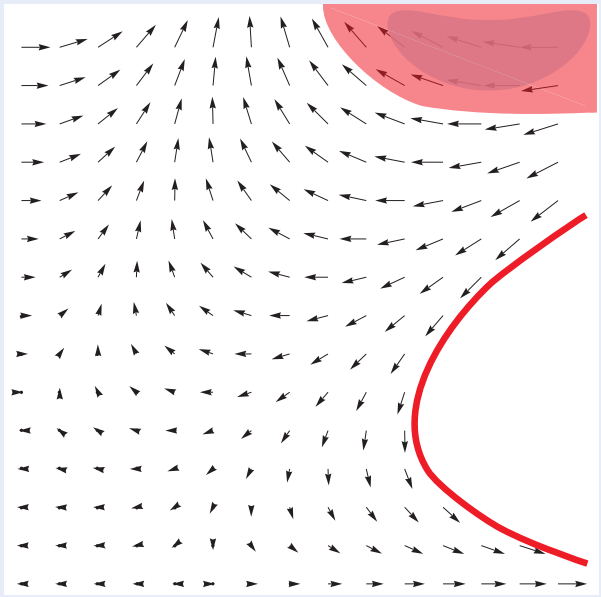
JLogComput'10,CAV'08,FMSD'09,LMCS'12,ITP'12

Differential Invariants for Differential Equations

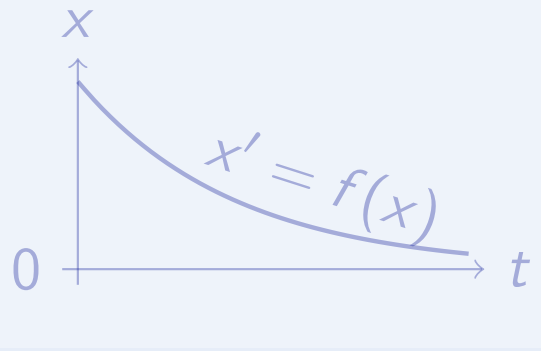
Differential Invariant

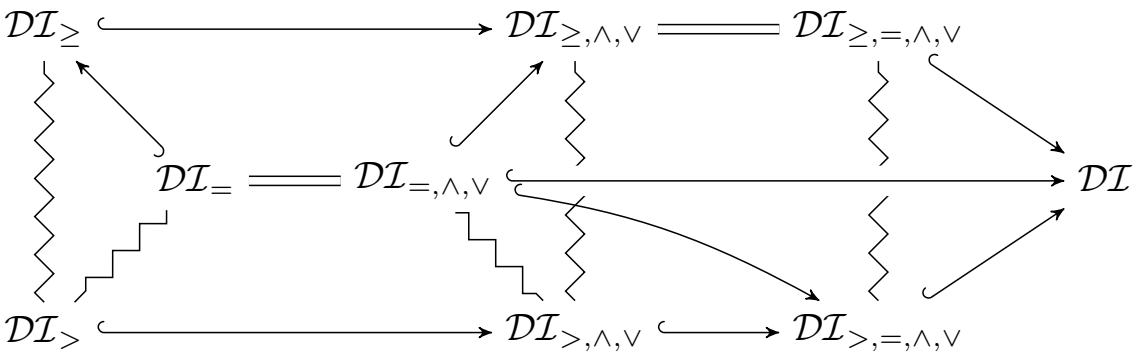


Differential Cut



Differential Ghost





Logic

Provability theory

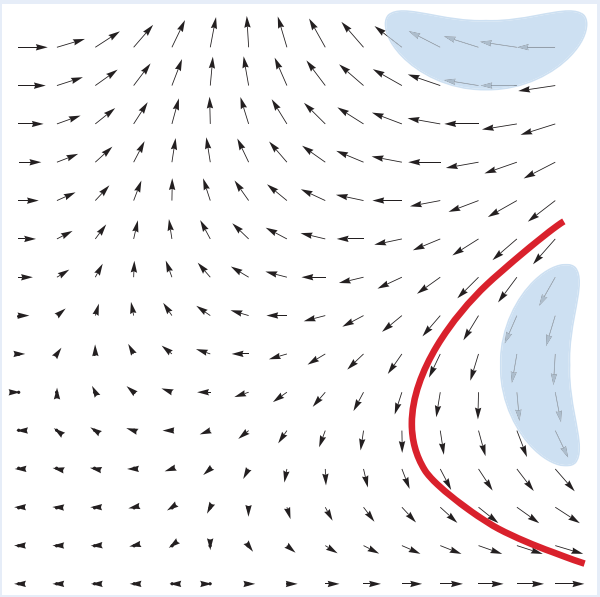
Math

Characteristic PDE

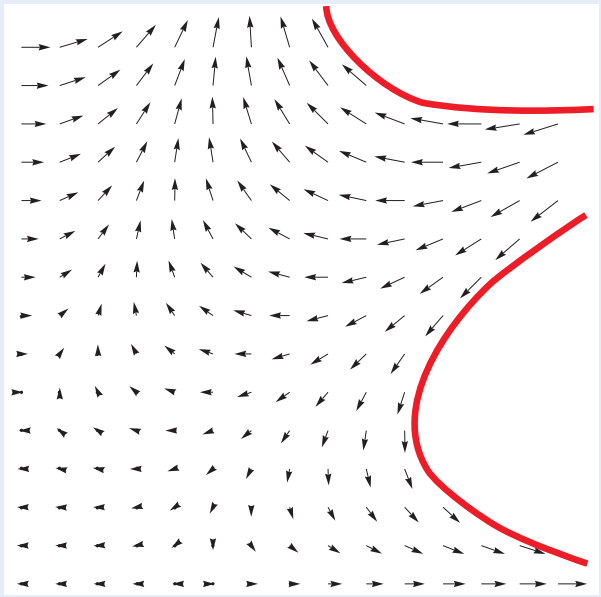
JLogComput'10,CAV'08,FMSD'09,LMCS'12,ITP'12

Differential Invariants for Differential Equations

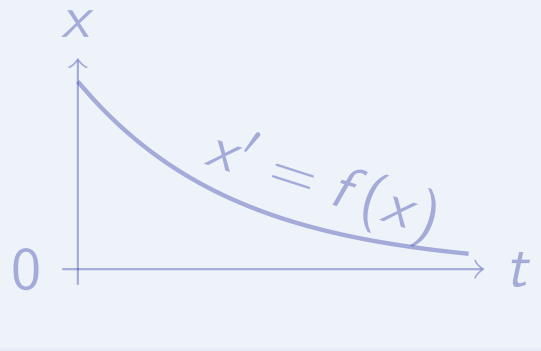
Differential Invariant

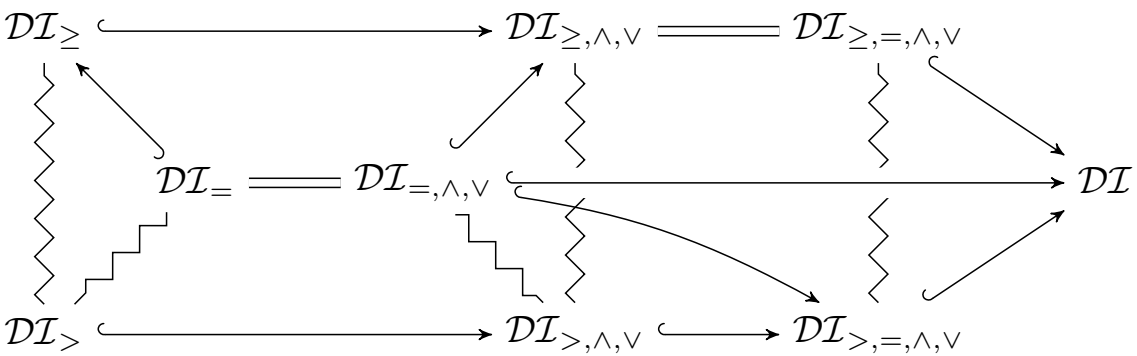


Differential Cut



Differential Ghost





Logic

Provability theory

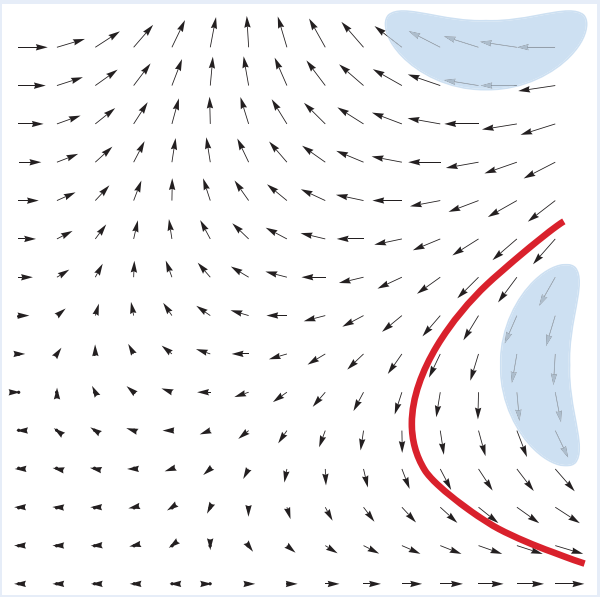
Math

Characteristic PDE

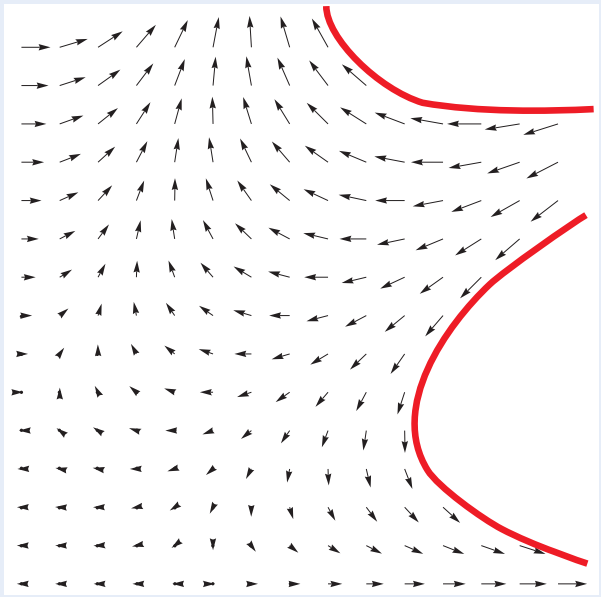
JLogComput'10,CAV'08,FMSD'09,LMCS'12,ITP'12

Differential Invariants for Differential Equations

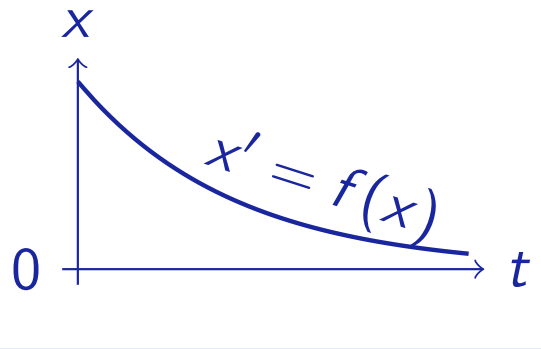
Differential Invariant

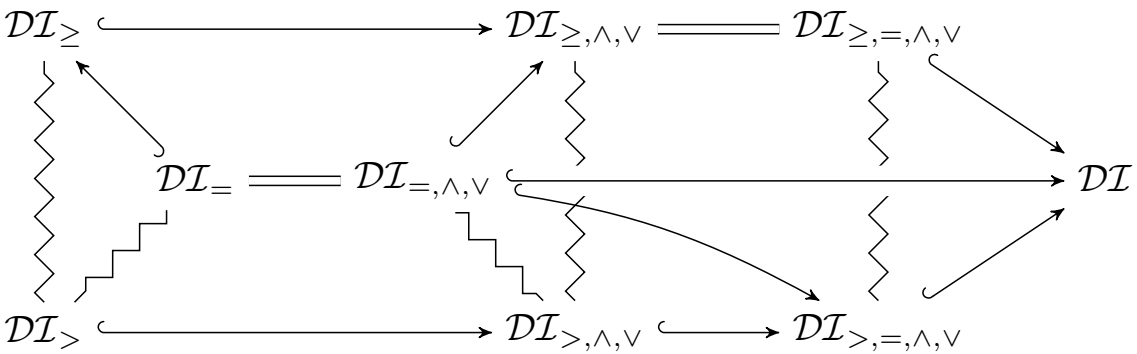


Differential Cut



Differential Ghost





Logic

Provability theory

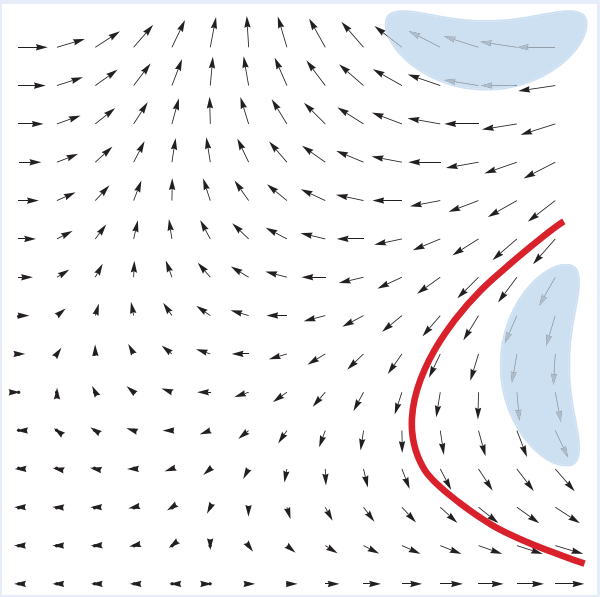
Math

Characteristic PDE

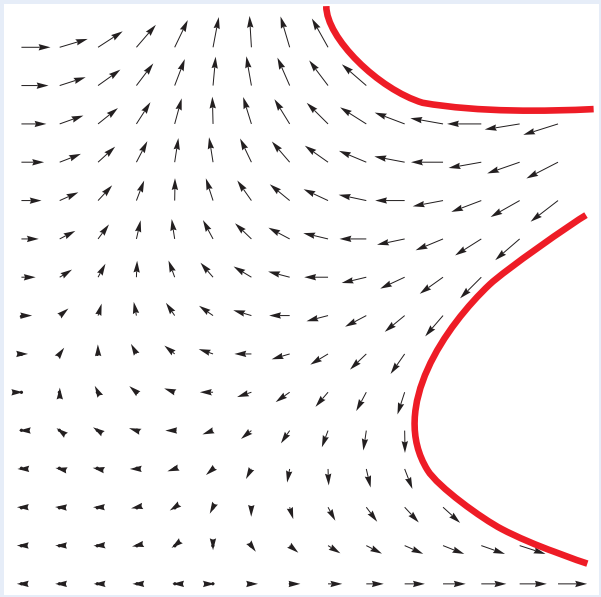
JLogComput'10,CAV'08,FMSD'09,LMCS'12,ITP'12

Differential Invariants for Differential Equations

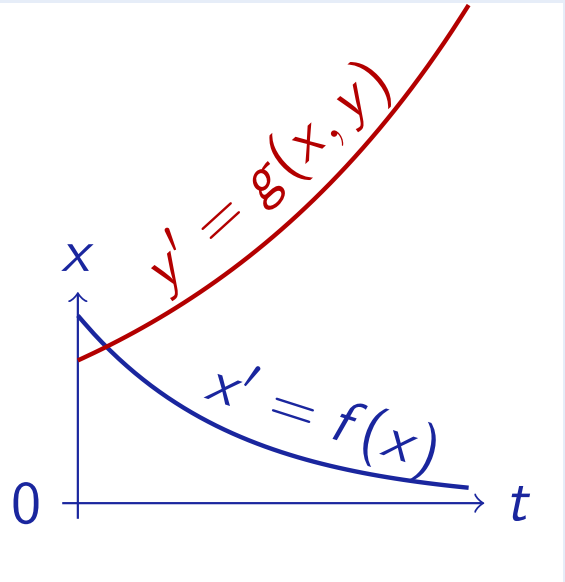
Differential Invariant

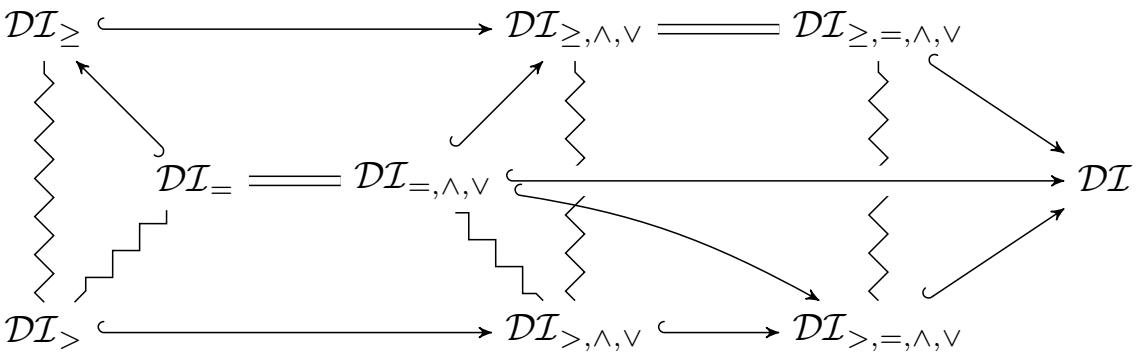


Differential Cut



Differential Ghost





Logic

Provability theory

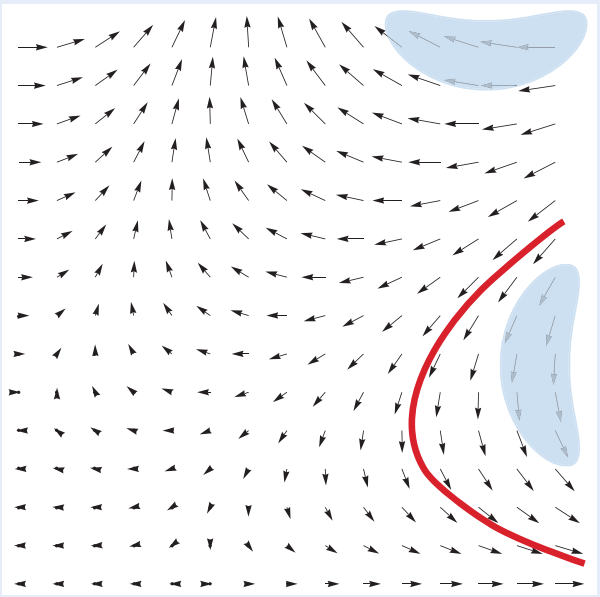
Math

Characteristic PDE

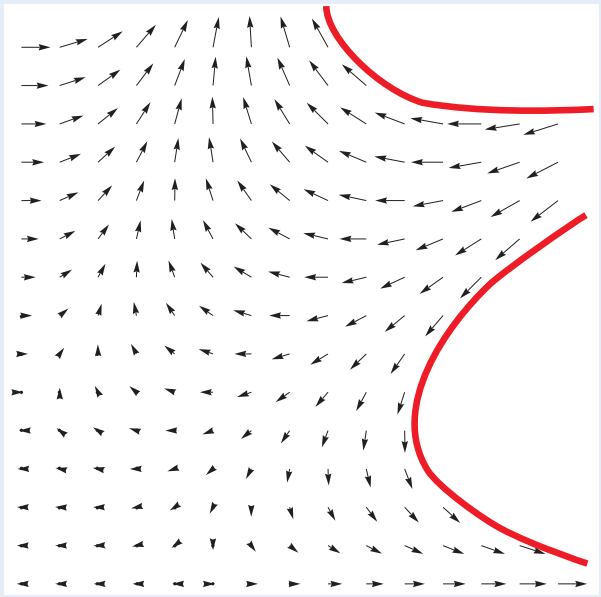
JLogComput'10,CAV'08,FMSD'09,LMCS'12,ITP'12

Differential Invariants for Differential Equations

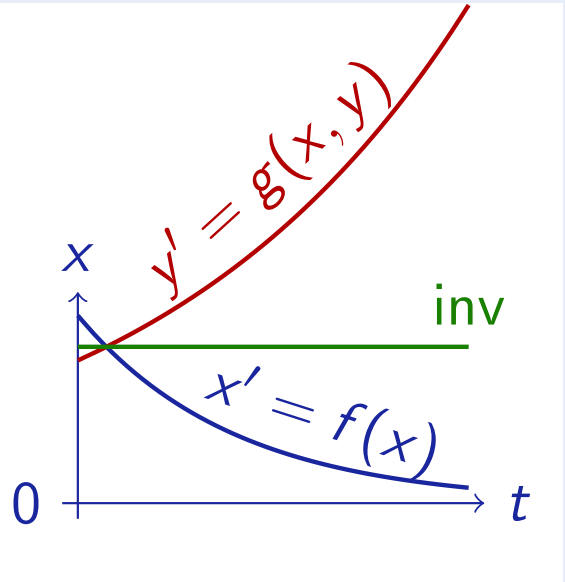
Differential Invariant

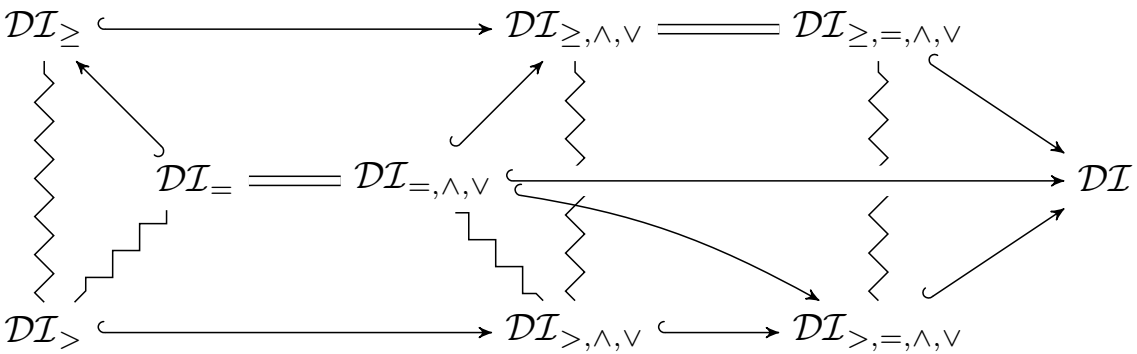


Differential Cut



Differential Ghost





Logic

Provability theory

Math

Characteristic PDE

JLogComput'10,CAV'08,FMSD'09,LMCS'12,ITP'12

Differential Invariant

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

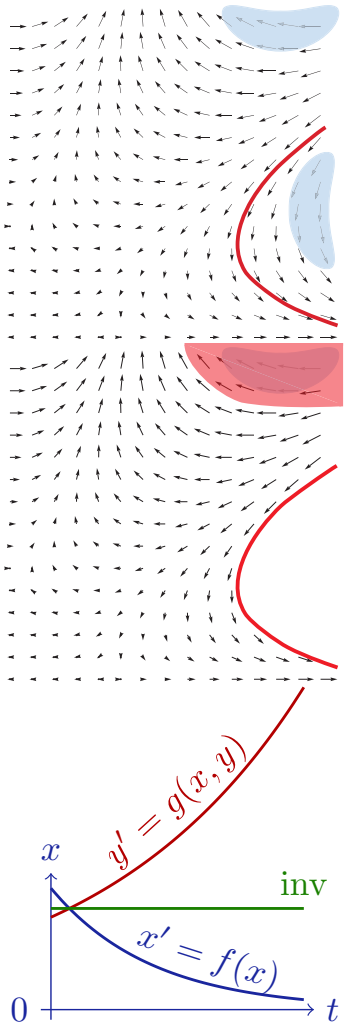
Differential Cut

$$\frac{F \rightarrow [x' = f(x)]C \quad F \rightarrow [x' = f(x) \,\&\, C]F}{F \rightarrow [x' = f(x)]F}$$

Differential Ghost

$$\frac{F \leftrightarrow \exists y\, G \quad G \rightarrow [x' = f(x), y' = g(x,y) \,\&\, H]G}{F \rightarrow [x' = f(x) \,\&\, H]F}$$

if new $y' = g(x,y)$ has a global solution



Differential Invariant

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

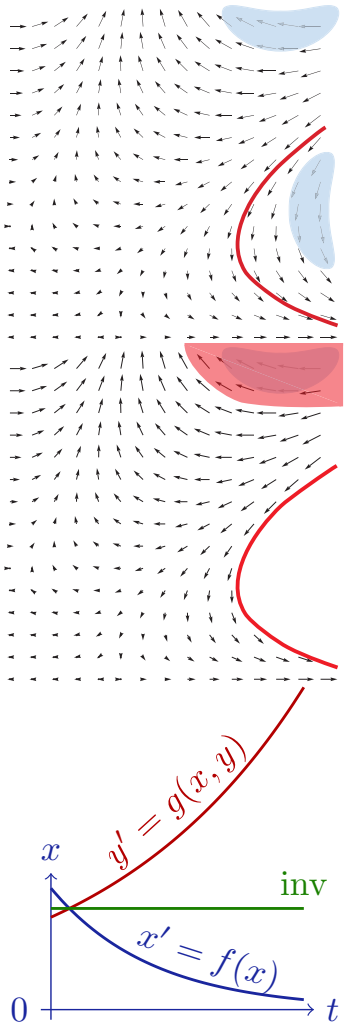
Differential Cut

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

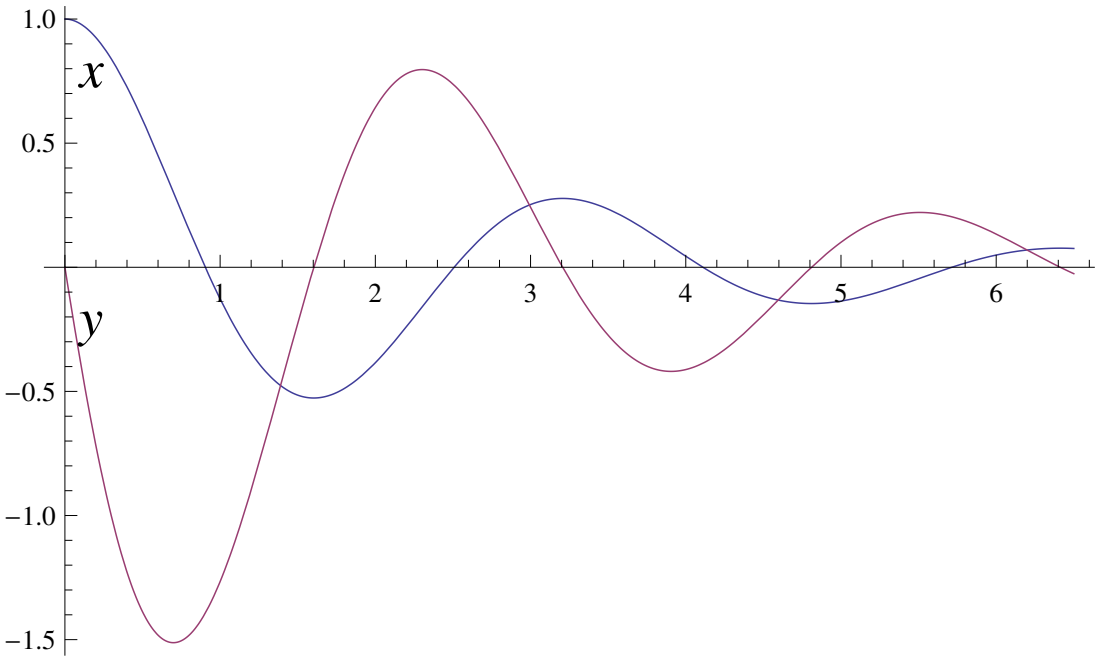
Differential Ghost

$$\frac{F \leftrightarrow \exists y\, G \quad G \rightarrow [x' = f(x), y' = g(x,y) \,\&\, H]G}{F \rightarrow [x' = f(x) \,\&\, H]F}$$

if new $y' = g(x,y)$ has a global solution

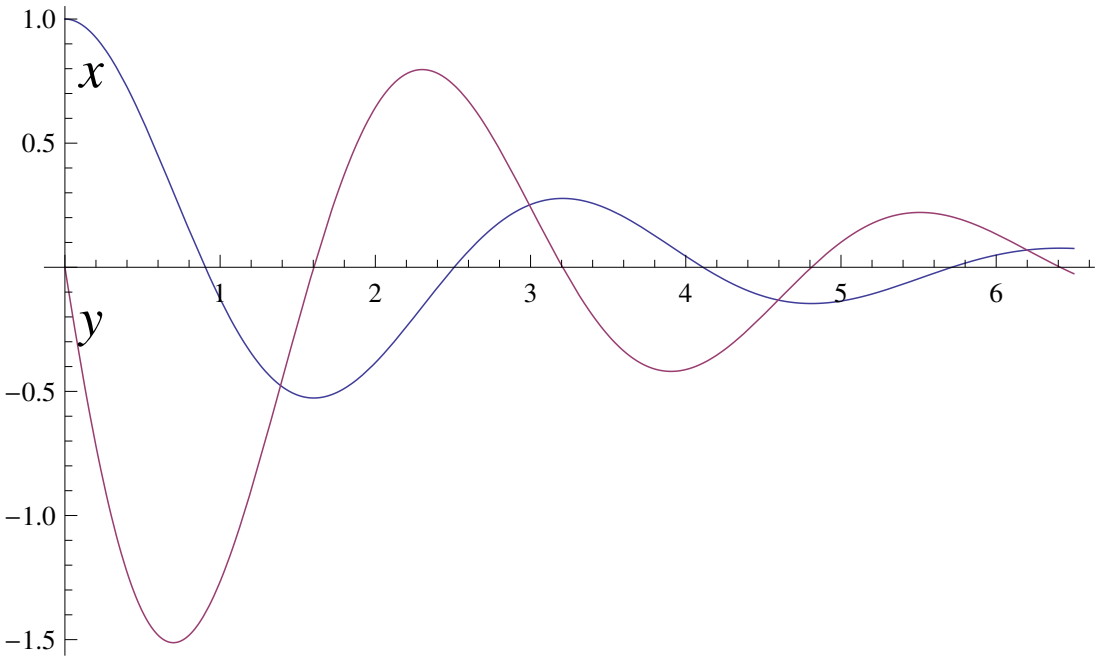


$$\omega^2x^2+y^2\leq c^2 \rightarrow [x' = y, y' = -\omega^2 x - 2d\omega y \,\&\, (\omega\geq 0 \wedge d\geq 0)]\, \omega^2x^2+y^2\leq c^2$$



$$\omega \geq 0 \land d \geq 0 \rightarrow [x' := y][y' := -\omega^2 x - 2d\omega y] 2\omega^2 x x' + 2y y' \leq 0$$

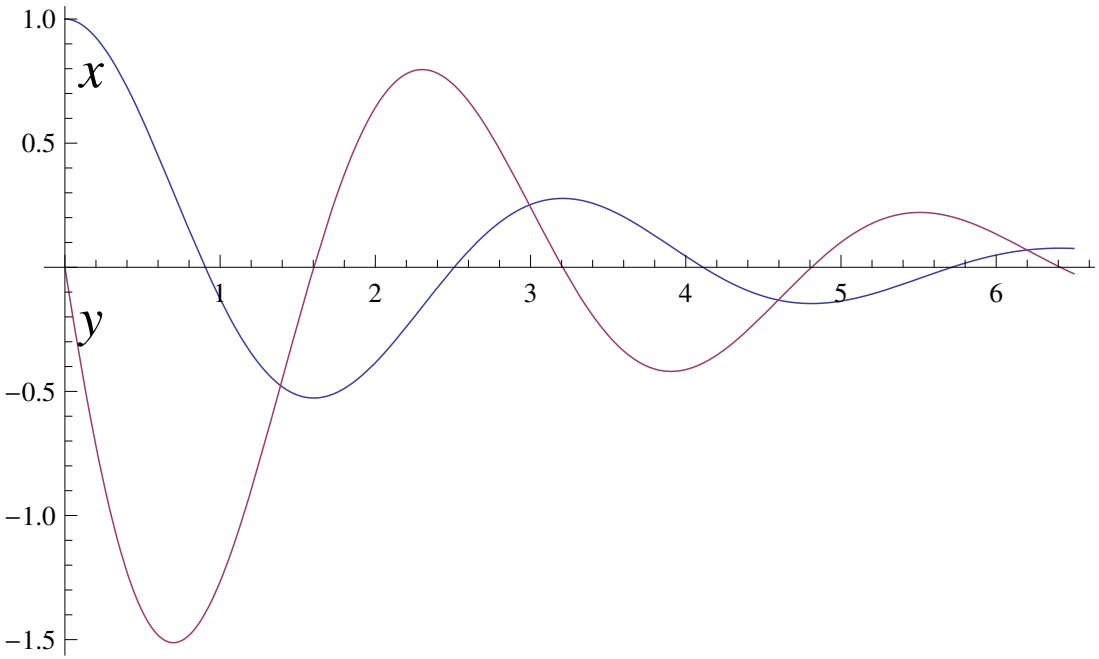
$$\omega^2 x^2 + y^2 \leq c^2 \rightarrow [x' = y, y' = -\omega^2 x - 2d\omega y \,\&\, (\omega \geq 0 \land d \geq 0)]\, \omega^2 x^2 + y^2 \leq c^2$$



$$\omega \geq 0 \wedge d \geq 0 \rightarrow 2\omega^2 xy + 2y(-\omega^2 x - 2d\omega y) \leq 0$$

$$\omega \geq 0 \wedge d \geq 0 \rightarrow [x' := y][y' := -\omega^2 x - 2d\omega y] 2\omega^2 x x' + 2y y' \leq 0$$

$$\omega^2 x^2 + y^2 \leq c^2 \rightarrow [x' = y, y' = -\omega^2 x - 2d\omega y \,\&\, (\omega \geq 0 \wedge d \geq 0)]\, \omega^2 x^2 + y^2 \leq c^2$$

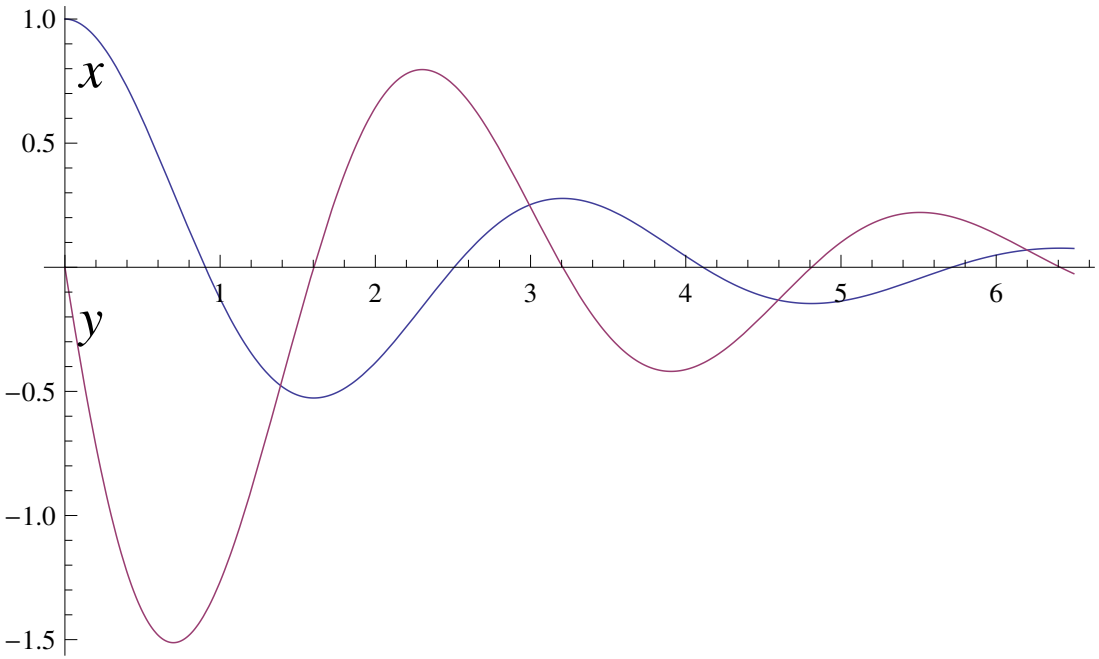


$*$

$$\omega\geq 0 \land d\geq 0 \rightarrow 2\omega^2 xy + 2y(-\omega^2 x - 2d\omega y) \leq 0$$

$$\omega\geq 0 \land d\geq 0 \rightarrow [x' := y][y' := -\omega^2 x - 2d\omega y] 2\omega^2 x x' + 2y y' \leq 0$$

$$\omega^2 x^2 + y^2 \leq c^2 \rightarrow [x' = y, y' = -\omega^2 x - 2d\omega y \,\&\, (\omega\geq 0 \land d\geq 0)]\, \omega^2 x^2 + y^2 \leq c^2$$

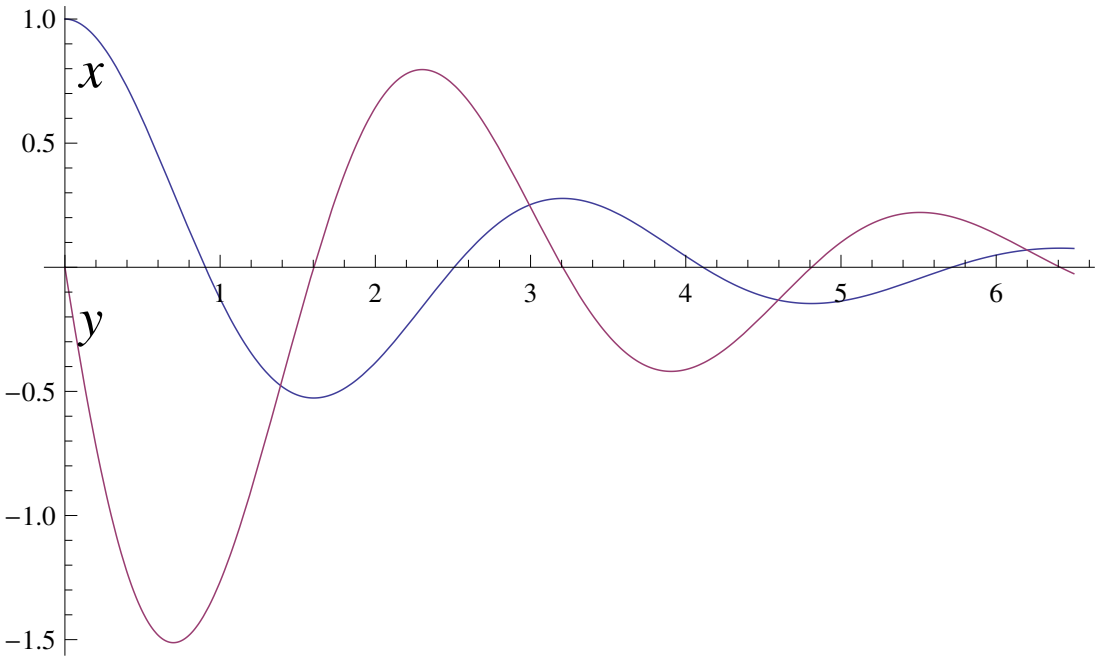


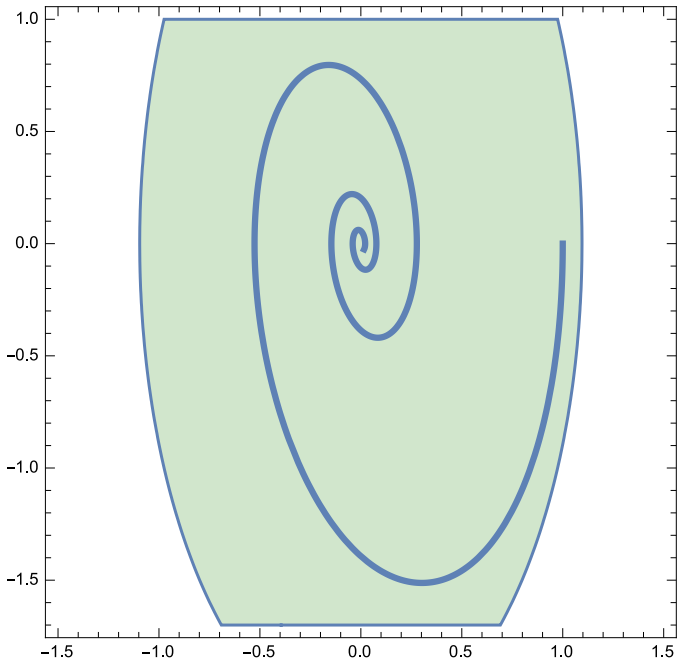
$*$

$$\omega\geq 0 \land d\geq 0 \rightarrow 2\omega^2 xy + 2y(-\omega^2 x - 2d\omega y) \leq 0$$

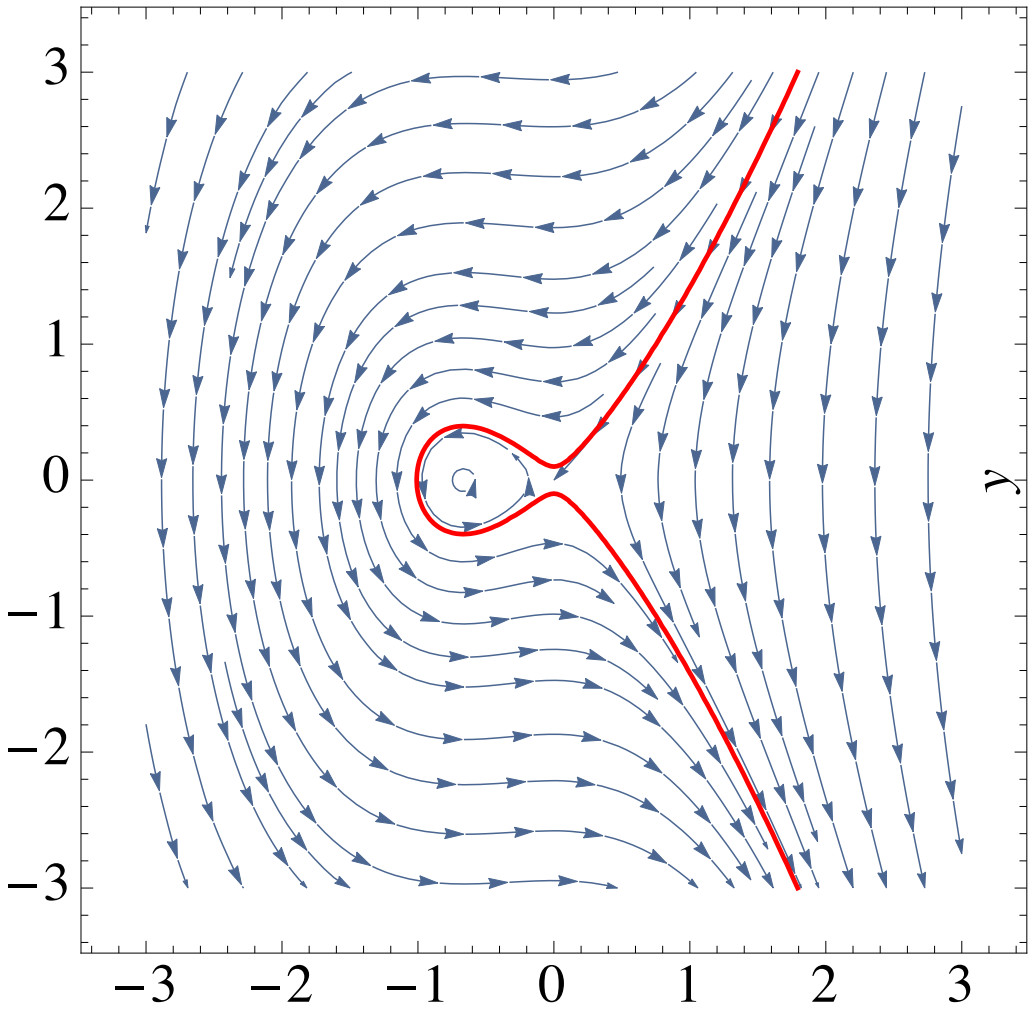
$$\omega\geq 0 \land d\geq 0 \rightarrow [x' := y][y' := -\omega^2 x - 2d\omega y] 2\omega^2 x x' + 2y y' \leq 0$$

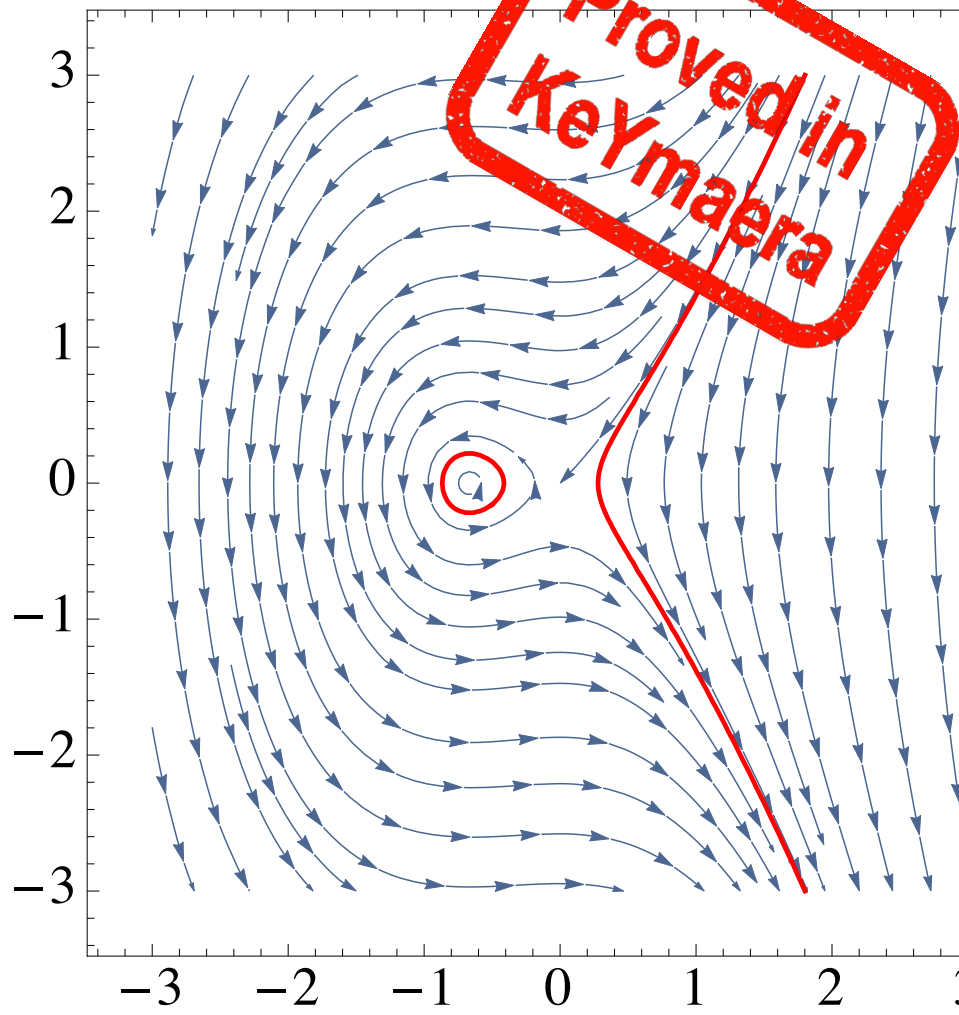
$$\omega^2 x^2 + y^2 \leq c^2 \rightarrow [x' = y, y' = -\omega^2 x - 2d\omega y \,\&\, (\omega\geq 0 \land d\geq 0)]\, \omega^2 x^2 + y^2 \leq c^2$$





Differential Invariants for Differential Equations



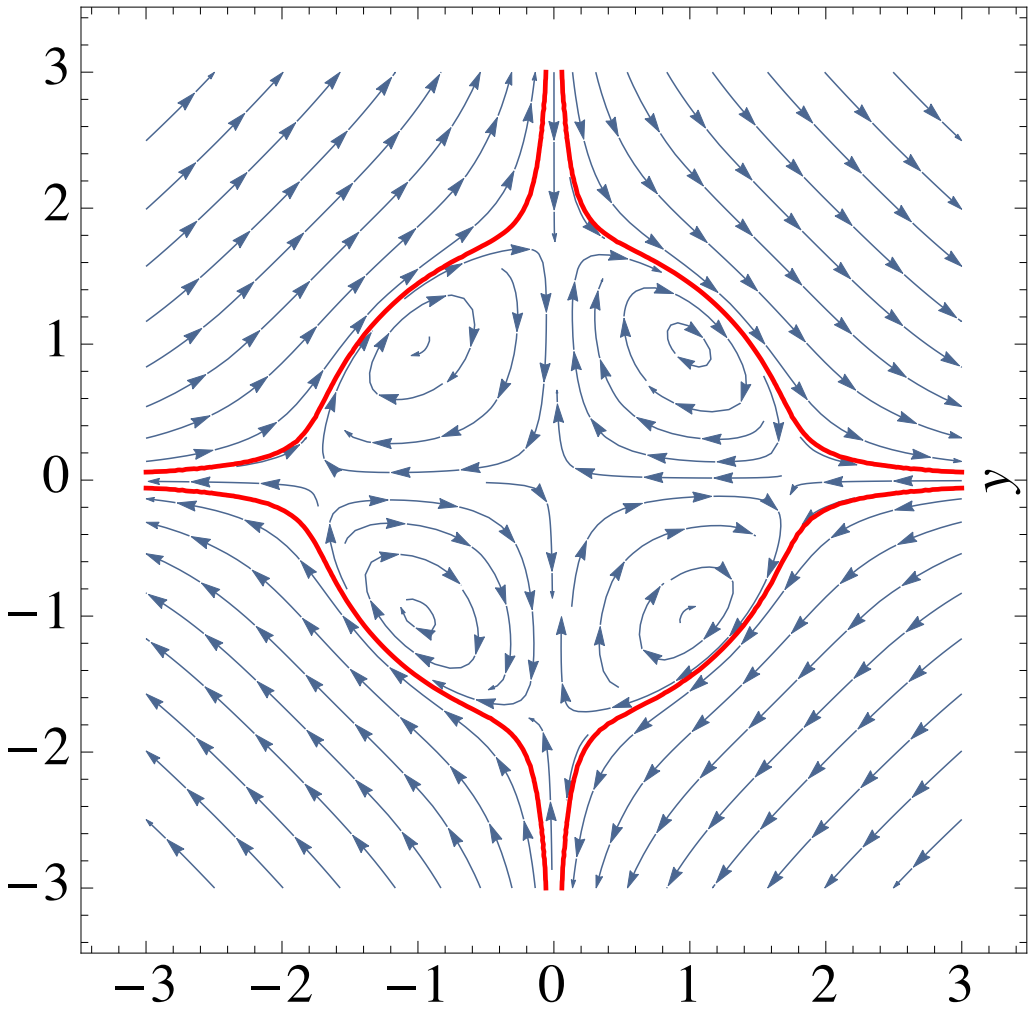


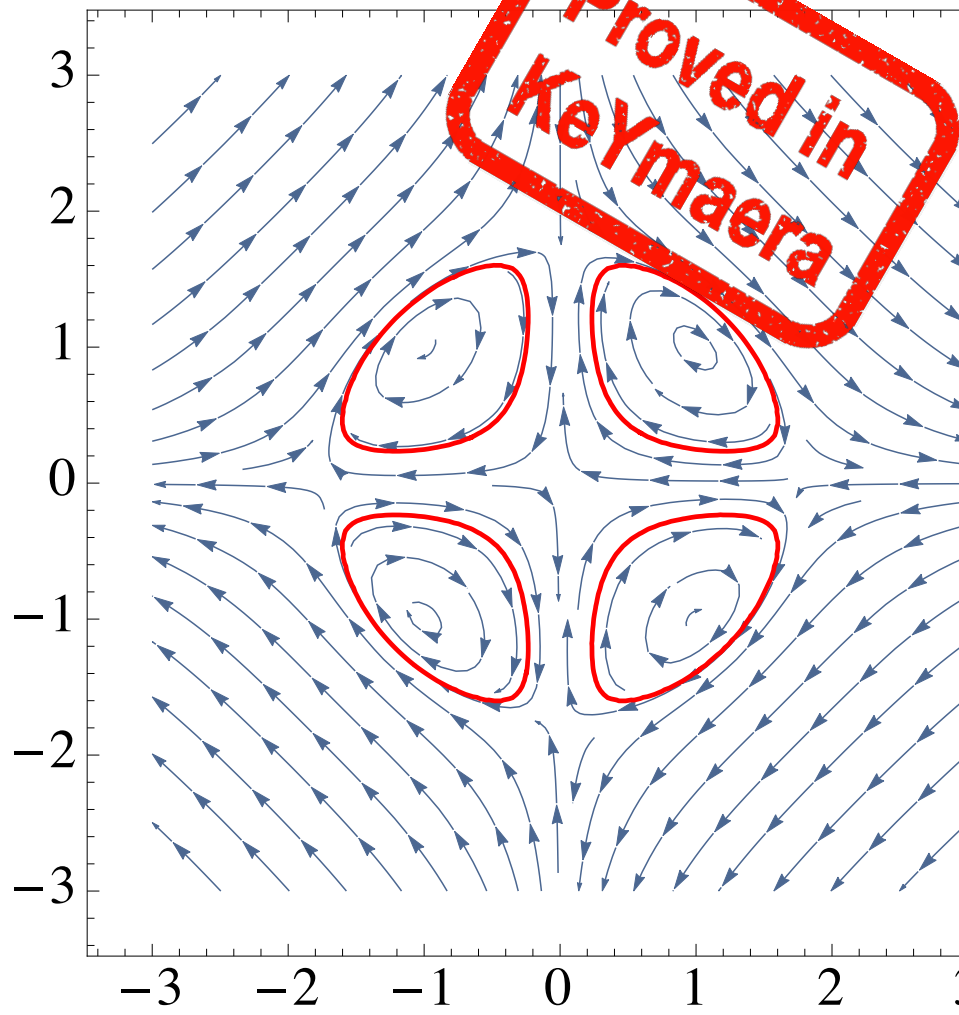
Proved in KeYmaera

$$x^2 + x^3 - y^2 - c = 0 \rightarrow [x' = -2y, y' = -2x - 3x^2]\, x^2 + x^3 - y^2 - c = 0$$

SAS'14

Differential Invariants for Differential Equations



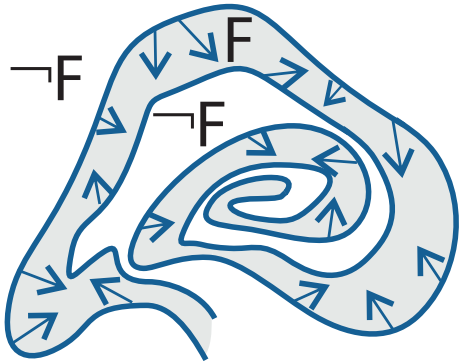


Proved in KeYmaera

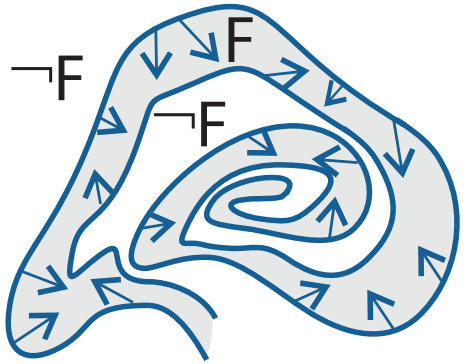
$$[x' = 2x^4y+4x^2y^3-6x^2y, y' = -4x^3y^2-2xy^4+6xy^2]x^4y^2+x^2y^4-3x^2y^2 \leq c$$

SAS'14

Assuming Differential Invariance

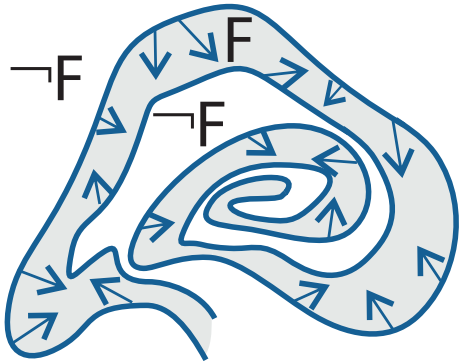


$$\frac{H \rightarrow [x' := f(x)]F'}{F \rightarrow [x' = f(x)\,\&\,H]F}$$

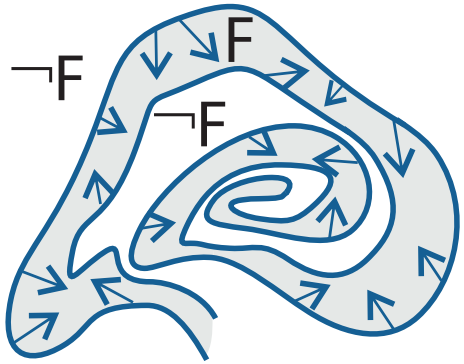


$$\frac{F \wedge H \rightarrow [x' := f(x)]F'}{F \rightarrow [x' = \theta\,\&\,H]F}$$

Assuming Differential Invariance



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

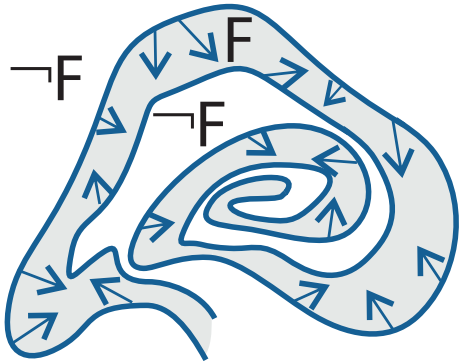


$$\frac{F \wedge H \rightarrow [x' := f(x)]F'}{F \rightarrow [x' = \theta\,\&\,H]F}$$

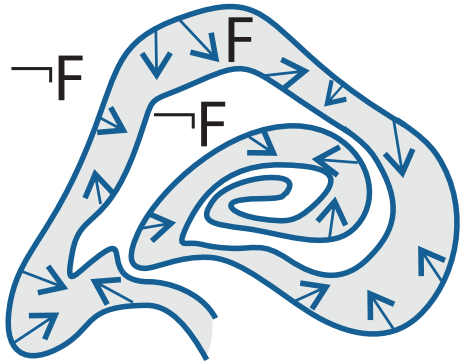
Example (Restrictions)

$$\frac{}{d^2 - 2d + 1 = 0 \rightarrow [d' = e, e' = -d]d^2 - 2d + 1 = 0}$$

Assuming Differential Invariance



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

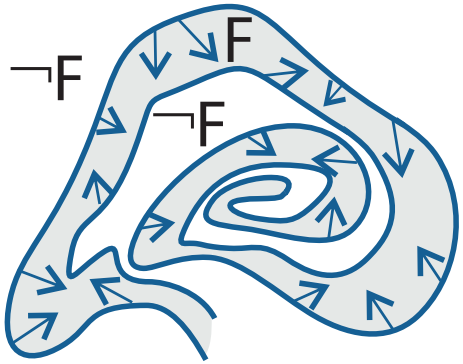


$$\frac{F \wedge H \rightarrow [x' := f(x)]F'}{F \rightarrow [x' = \theta\,\&\,H]F}$$

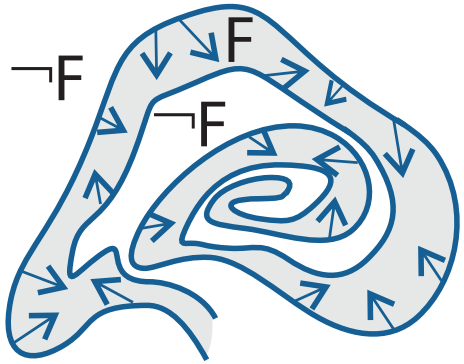
Example (Restrictions)

$$\frac{d^2 - 2d + 1 = 0 \rightarrow [d' := e][e' := -d]2dd' - 2d' = 0}{d^2 - 2d + 1 = 0 \rightarrow [d' = e, e' = -d]d^2 - 2d + 1 = 0}$$

Assuming Differential Invariance



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



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

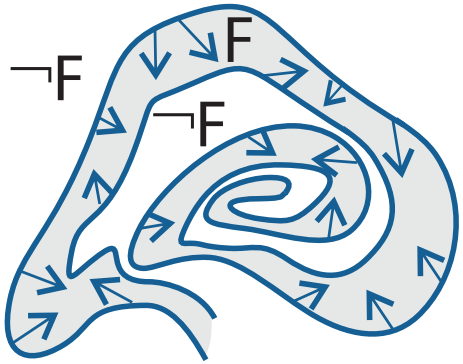
Example (Restrictions)

$$\frac{}{d^2 - 2d + 1 = 0 \rightarrow 2de - 2e = 0}$$

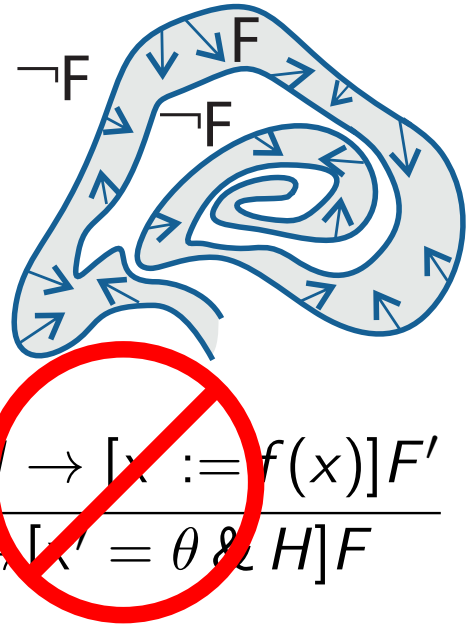
$$\frac{d^2 - 2d + 1 = 0 \rightarrow 2de - 2e = 0}{d^2 - 2d + 1 = 0 \rightarrow [d' := e][e' := -d]2dd' - 2d' = 0}$$

$$\frac{d^2 - 2d + 1 = 0 \rightarrow [d' := e][e' := -d]2dd' - 2d' = 0}{d^2 - 2d + 1 = 0 \rightarrow [d' = e, e' = -d]d^2 - 2d + 1 = 0}$$

Assuming Differential Invariance



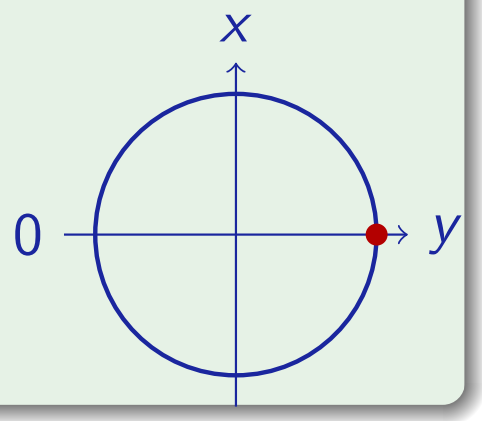
$$\frac{H \rightarrow [x' := f(x)]F'}{F \rightarrow [x' = f(x)\,\&\,H]F}$$



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

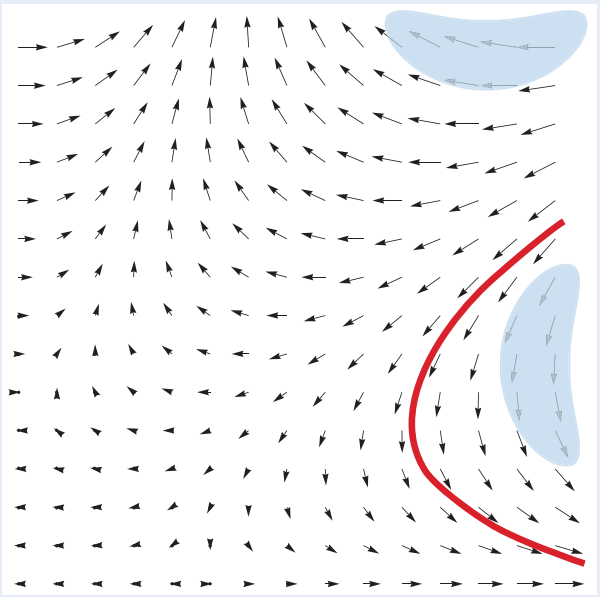
Example (Restrictions are unsound!)

$$\frac{\text{(unsound)}}{\dfrac{\dfrac{d^2 - 2d + 1 = 0 \rightarrow 2de - 2e = 0}{d^2 - 2d + 1 = 0 \rightarrow [d' := e][e' := -d]2dd' - 2d' = 0}}{d^2 - 2d + 1 = 0 \rightarrow [d' = e, e' = -d]d^2 - 2d + 1 = 0}}$$

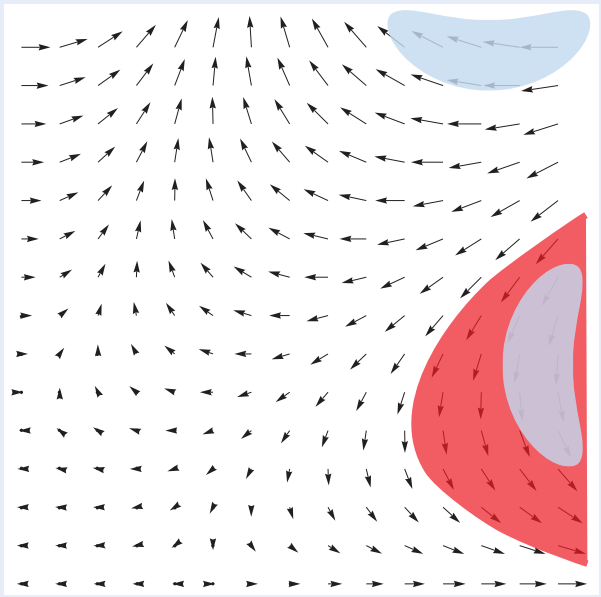


Differential Invariants for Differential Equations

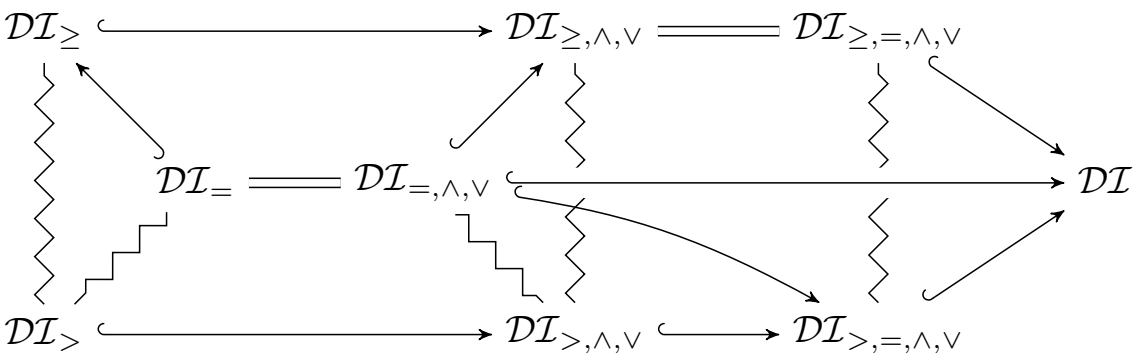
Differential Invariant



Differential Cut



Differential Ghost



Logic

Provability theory

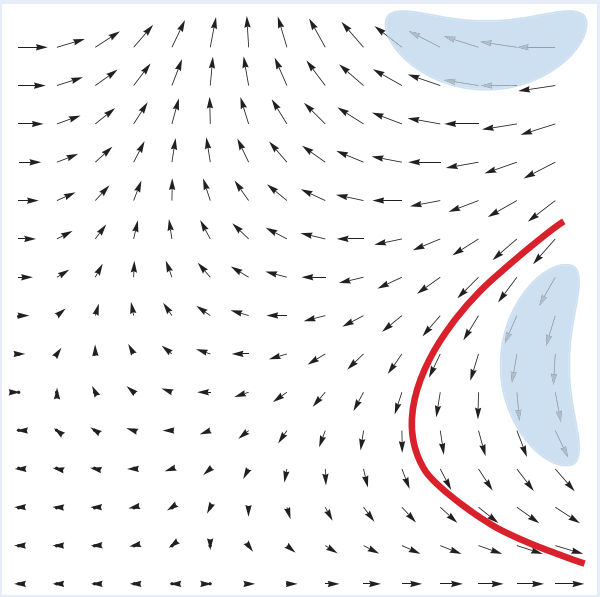
Math

Characteristic PDE

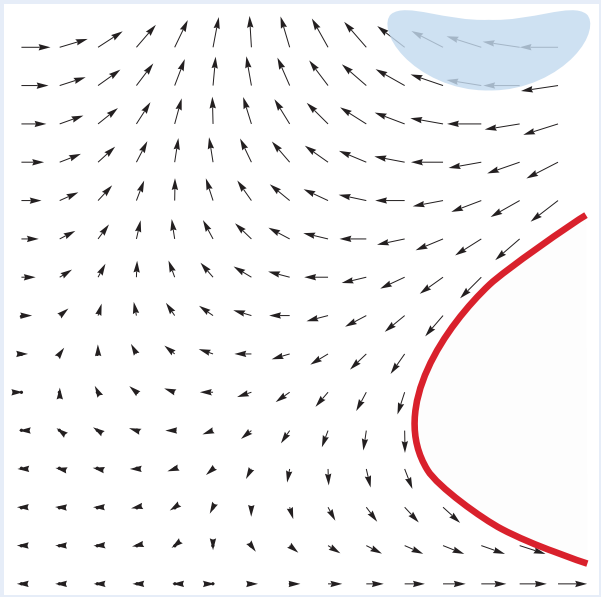
JLogComput'10,CAV'08,FMSD'09,LMCS'12,ITP'12

Differential Invariants for Differential Equations

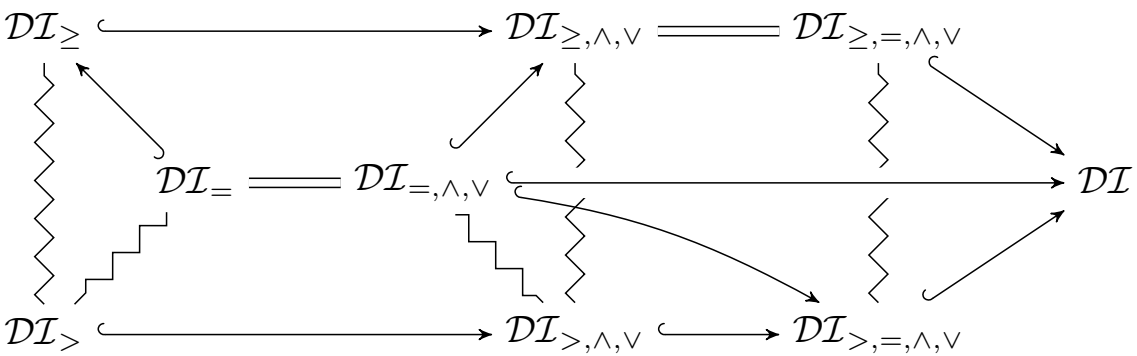
Differential Invariant



Differential Cut



Differential Ghost



Logic

Provability theory

Math

Character-istic PDE

JLogComput'10,CAV'08,FMSD'09,LMCS'12,ITP'12

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

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

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

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

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

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

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

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

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

$$\text{DC}\,\dfrac{\text{DI}\,\dfrac{}{x^3 \geq -1 \to [x' = (x-2)^4 + y^5, y' = y^2 \,\&\, y^5 \geq 0]x^3 \geq -1}\ \triangleright}{x^3 \geq -1 \wedge y^5 \geq 0 \to [x' = (x-2)^4 + y^5, y' = y^2]x^3 \geq -1}$$

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

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

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

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

Ex: Differential Cuts

$$\dfrac{\dfrac{\dfrac{\dfrac{}{y^5 \geq 0 \to 2x^2((x-2)^4+y^5) \geq 0}\,\text{QE}}{y^5 \geq 0 \to [x' := (x-2)^4+y^5][y' := y^2]2x^2x' \geq 0}}{x^3 \geq -1 \to [x' = (x-2)^4+y^5, y' = y^2 \,\&\, y^5 \geq 0]x^3 \geq -1}\,\text{DI}\ \triangleright}{x^3 \geq -1 \wedge y^5 \geq 0 \to [x' = (x-2)^4+y^5, y' = y^2]x^3 \geq -1}\,\text{DC}$$

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

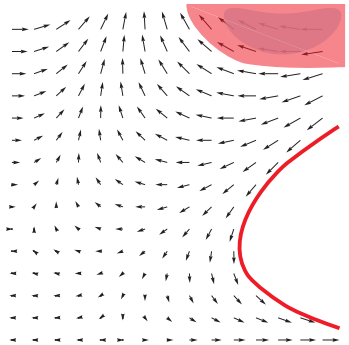
$$\dfrac{\dfrac{\dfrac{\dfrac{*}{y^5 \geq 0 \rightarrow 2x^2((x-2)^4+y^5) \geq 0}\,\text{QE}}{y^5 \geq 0 \rightarrow [x' := (x-2)^4+y^5][y' := y^2]2x^2x' \geq 0}}{x^3 \geq -1 \rightarrow [x' = (x-2)^4+y^5, y' = y^2 \,\&\, y^5 \geq 0]x^3 \geq -1}\,\text{DI}\ \triangleright}{x^3 \geq -1 \wedge y^5 \geq 0 \rightarrow [x' = (x-2)^4+y^5, y' = y^2]x^3 \geq -1}\,\text{DC}$$

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

Differential Cuts

Differential Cut

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



Theorem (Gentzen's Cut Elimination)

$$\frac{A\rightarrow B\vee C \quad A\wedge C\rightarrow B}{A\rightarrow B}$$

cut can be eliminated

Theorem (No Differential Cut Elimination) (LMCS 2012)

Deductive power with differential cut exceeds deductive power without.

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

JLogComput'10,LMCS'12

Differential Equation Axioms & Differential Axioms

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

DC $\big([x' = f(x) \,\&\, q(x)]p(x) \leftrightarrow [x' = f(x) \,\&\, q(x) \wedge r(x)]p(x)\big)$
$\leftarrow [x' = f(x) \,\&\, q(x)]r(x)$

DE $[x' = f(x) \,\&\, q(x)]p(x, x') \leftrightarrow [x' = f(x) \,\&\, q(x)][x' := f(x)]p(x, x')$

DI $[x' = f(x) \,\&\, q(x)]p(x) \leftarrow \big(q(x) \rightarrow p(x) \wedge [x' = f(x) \,\&\, q(x)](p(x))'\big)$

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

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

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

$+'$ $(f(\bar{x}) + g(\bar{x}))' = (f(\bar{x}))' + (g(\bar{x}))'$

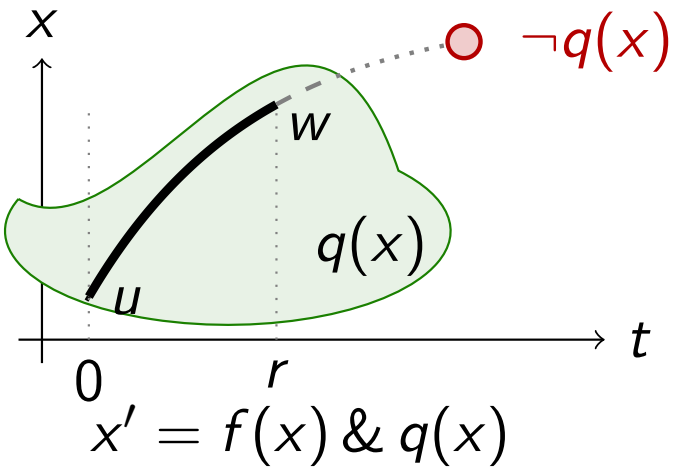
$\cdot'$ $(f(\bar{x}) \cdot g(\bar{x}))' = (f(\bar{x}))' \cdot g(\bar{x}) + f(\bar{x}) \cdot (g(\bar{x}))'$

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

CADE'15

Axiom (Differential Weakening) (CADE'15)

$$\text{(DW)}\quad [x' = f(x)\,\&\,q(x)]q(x)$$

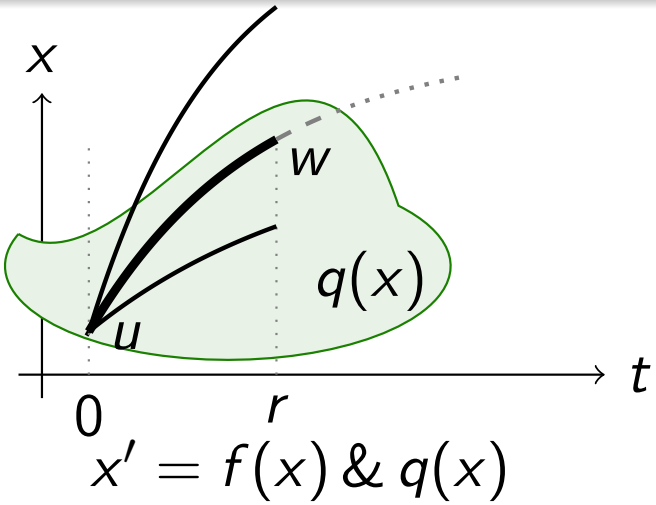


Differential equations cannot leave their evolution domains. Implies:

$$[x' = f(x)\,\&\,q(x)]p(x) \leftrightarrow [x' = f(x)\,\&\,q(x)]\big(q(x) \rightarrow p(x)\big)$$

Axiom (Differential Cut) (CADE'15)

$$\text{(DC)}\quad \big([x' = f(x)\,\&\,q(x)]p(x) \leftrightarrow [x' = f(x)\,\&\,q(x)\wedge r(x)]p(x)\big) \leftarrow [x' = f(x)\,\&\,q(x)]r(x)$$

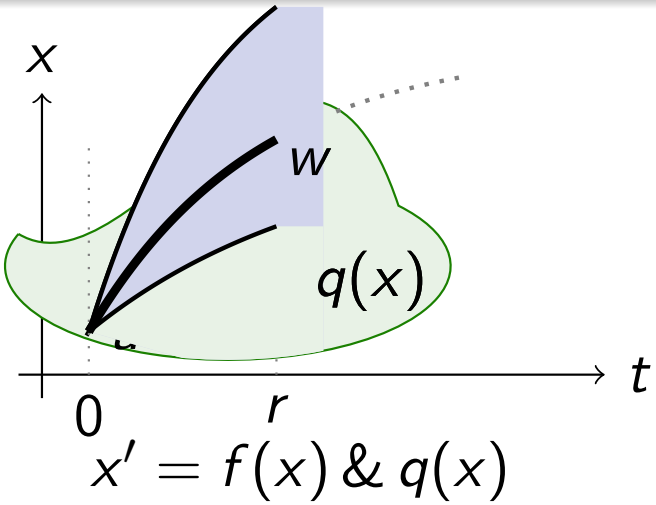


DC is a cut for differential equations.
DC is a differential modal modus ponens K.
Can't leave $r(x)$, then might as well restrict state space to $r(x)$.

Differential Equation Axioms

Axiom (Differential Cut) (CADE'15)

$$\text{(DC)}\quad \big([x' = f(x)\,\&\,q(x)]p(x) \leftrightarrow [x' = f(x)\,\&\,q(x)\wedge r(x)]p(x)\big) \leftarrow [x' = f(x)\,\&\,q(x)]r(x)$$

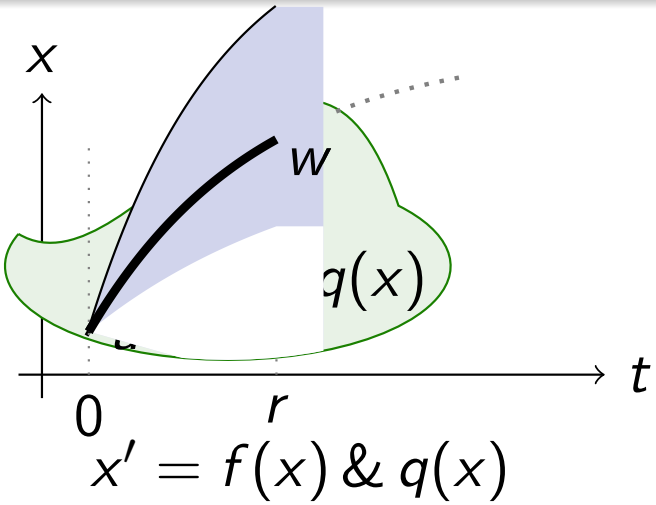


DC is a cut for differential equations.
DC is a differential modal modus ponens K.
Can't leave $r(x)$, then might as well restrict state space to $r(x)$.

Differential Equation Axioms

Axiom (Differential Cut) (CADE'15)

$$\text{(DC)}\quad \big([x' = f(x)\,\&\,q(x)]p(x) \leftrightarrow [x' = f(x)\,\&\,q(x)\wedge r(x)]p(x)\big) \leftarrow [x' = f(x)\,\&\,q(x)]r(x)$$

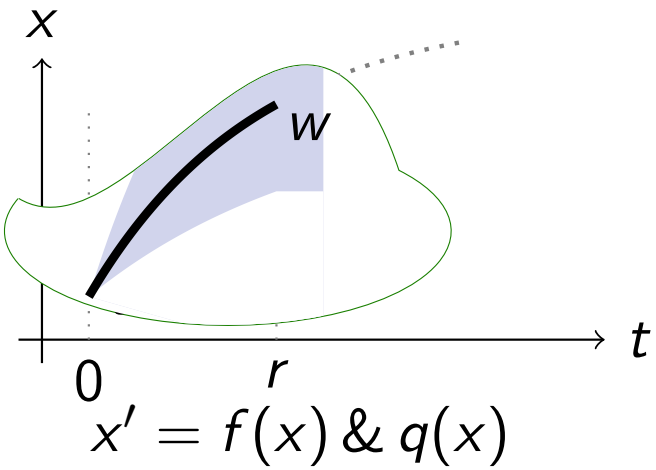


DC is a cut for differential equations.
DC is a differential modal modus ponens K.
Can't leave $r(x)$, then might as well restrict state space to $r(x)$.

Differential Equation Axioms

Axiom (Differential Cut) (CADE'15)

$$\text{(DC)}\quad \big([x' = f(x)\,\&\,q(x)]p(x) \leftrightarrow [x' = f(x)\,\&\,q(x)\wedge r(x)]p(x)\big) \leftarrow [x' = f(x)\,\&\,q(x)]r(x)$$

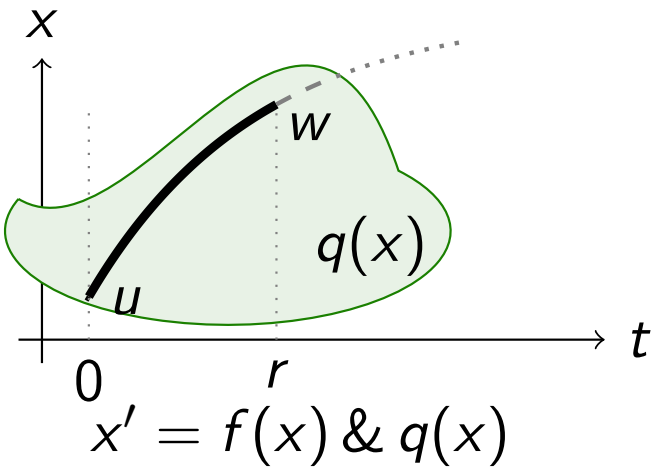


DC is a cut for differential equations.
DC is a differential modal modus ponens K.
Can't leave $r(x)$, then might as well restrict state space to $r(x)$.

Differential Equation Axioms

Axiom (Differential Cut) (CADE'15)

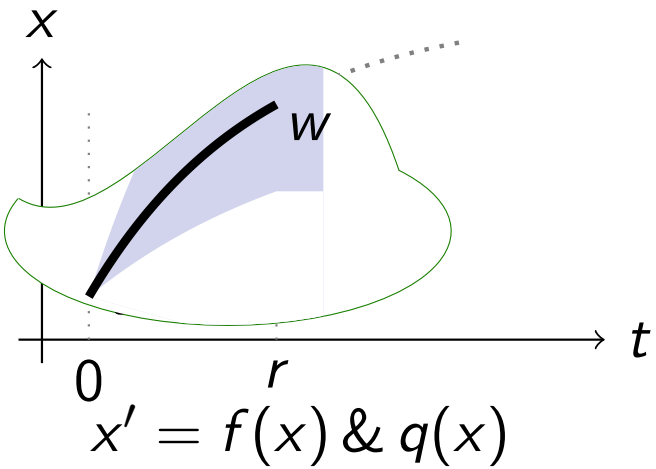
$$\text{(DC)}\quad \big([x' = f(x)\,\&\,q(x)]p(x) \leftrightarrow [x' = f(x)\,\&\,q(x)\wedge r(x)]p(x)\big) \leftarrow [x' = f(x)\,\&\,q(x)]r(x)$$

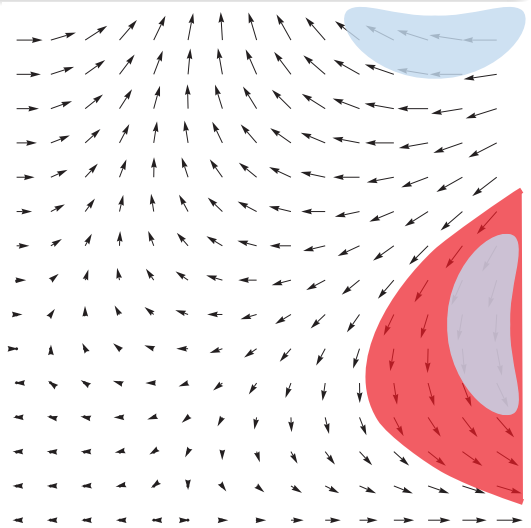


DC is a cut for differential equations.
DC is a differential modal modus ponens K.
Can't leave $r(x)$, then might as well restrict state space to $r(x)$.

Axiom (Differential Cut) (CADE'15)

$$\text{(DC)}\quad \big([x' = f(x)\,\&\,q(x)]p(x) \leftrightarrow [x' = f(x)\,\&\,q(x)\wedge r(x)]p(x)\big) \leftarrow [x' = f(x)\,\&\,q(x)]r(x)$$



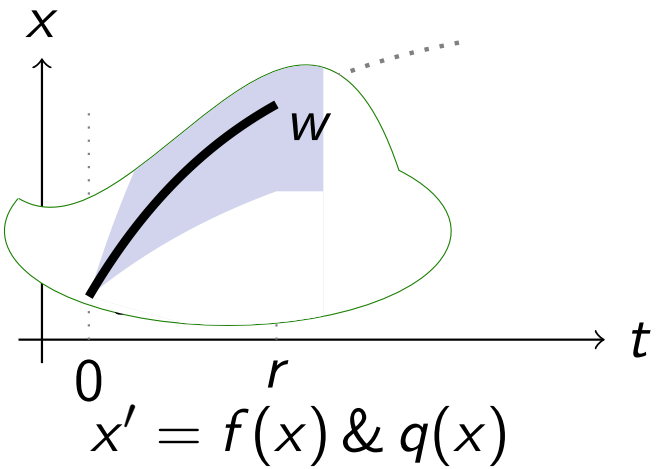


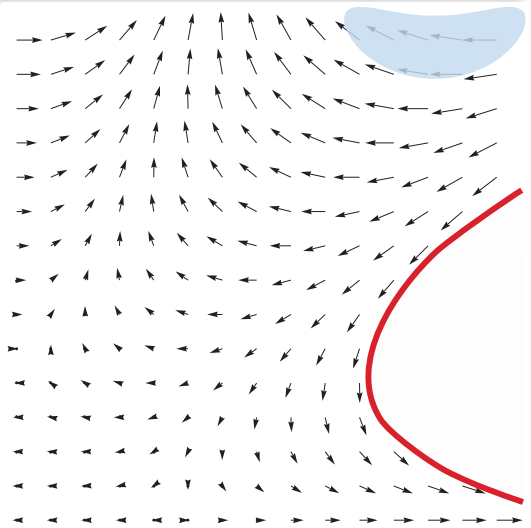
DC is a cut for differential equations.
DC is a differential modal modus ponens K.
Can't leave $r(x)$, then might as well restrict state space to $r(x)$.

Differential Equation Axioms

Axiom (Differential Cut) (CADE'15)

$$\text{(DC)}\quad \big([x' = f(x)\,\&\,q(x)]p(x) \leftrightarrow [x' = f(x)\,\&\,q(x)\wedge r(x)]p(x)\big) \leftarrow [x' = f(x)\,\&\,q(x)]r(x)$$



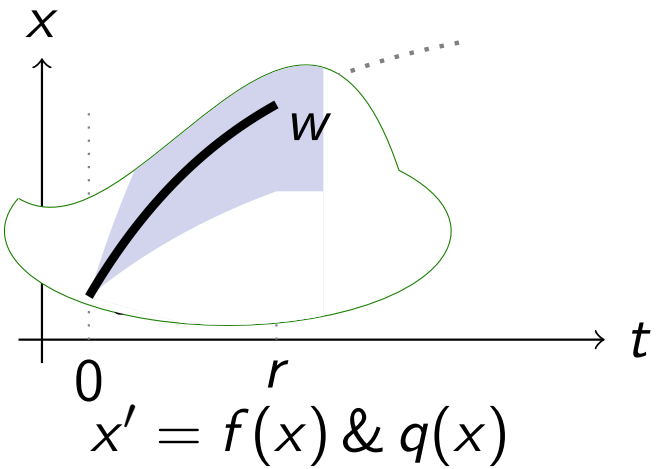


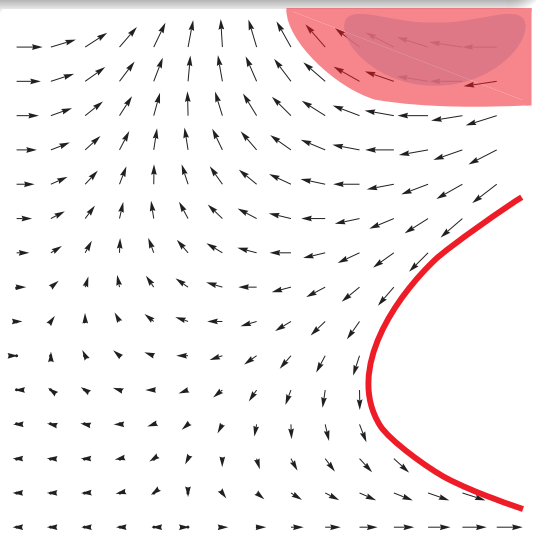
DC is a cut for differential equations.
DC is a differential modal modus ponens K.
Can't leave $r(x)$, then might as well restrict state space to $r(x)$.

Differential Equation Axioms

Axiom (Differential Cut) (CADE'15)

$$\text{(DC)}\quad \big([x' = f(x)\,\&\,q(x)]p(x) \leftrightarrow [x' = f(x)\,\&\,q(x)\wedge r(x)]p(x)\big) \leftarrow [x' = f(x)\,\&\,q(x)]r(x)$$



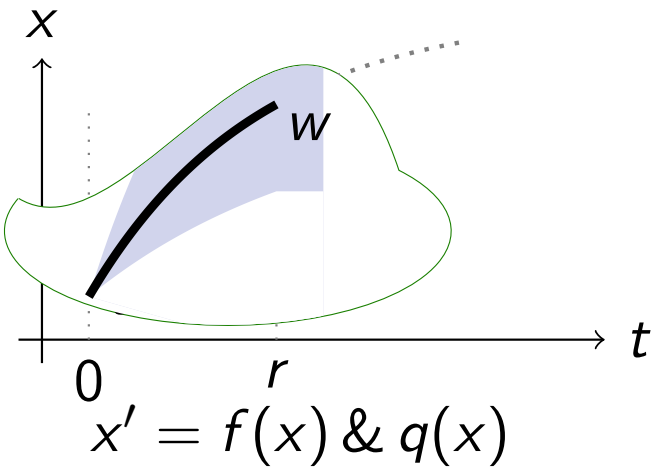


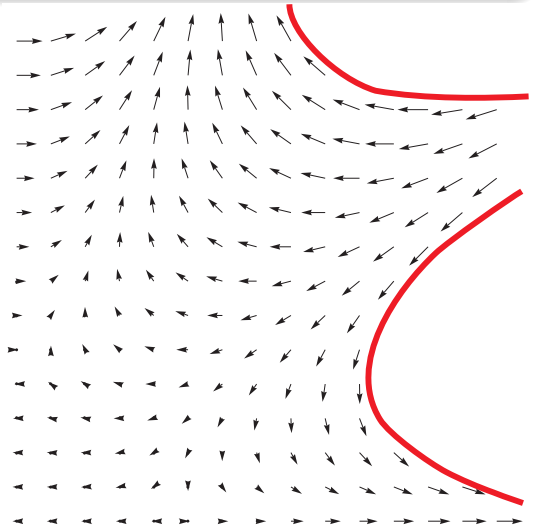
DC is a cut for differential equations.
DC is a differential modal modus ponens K.
Can't leave $r(x)$, then might as well restrict state space to $r(x)$.

Differential Equation Axioms

Axiom (Differential Cut) (CADE'15)

$$\text{(DC)}\quad \big([x' = f(x)\,\&\,q(x)]p(x) \leftrightarrow [x' = f(x)\,\&\,q(x)\wedge r(x)]p(x)\big) \leftarrow [x' = f(x)\,\&\,q(x)]r(x)$$

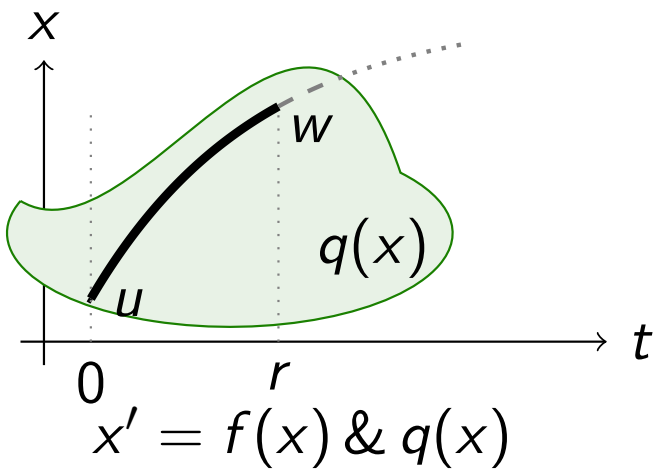


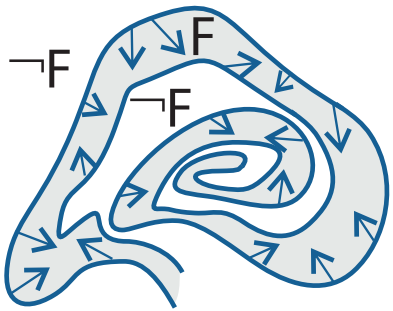


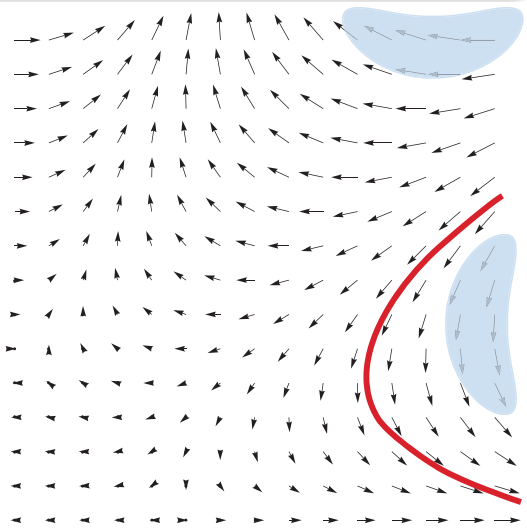
DC is a cut for differential equations.
DC is a differential modal modus ponens K.
Can't leave $r(x)$, then might as well restrict state space to $r(x)$.

Axiom (Differential Invariant) (CADE'15)

(DI) $[x' = f(x)\,\&\,q(x)]p(x) \leftarrow \big(q(x) \rightarrow p(x) \wedge [x' = f(x)\,\&\,q(x)](p(x))'\big)$



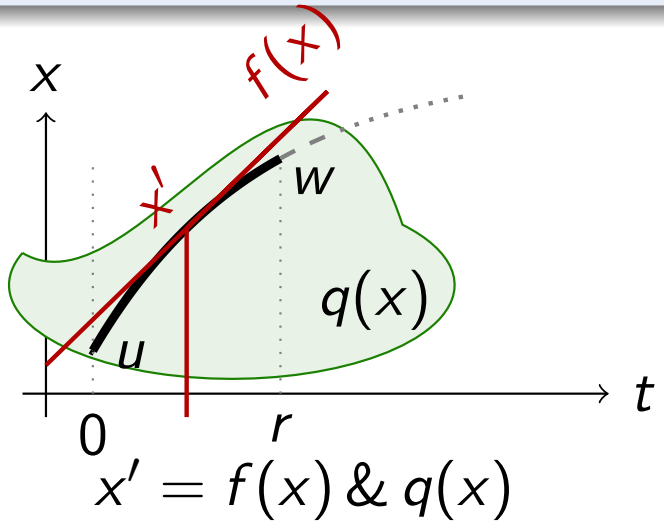




Differential invariant: $p(x)$ true now and its differential $(p(x))'$ true always
What's the differential of a formula???
What's the meaning of a differential term . . . in a state???

Axiom (Differential Effect) (CADE'15)

$$\text{(DE)}\quad [x' = f(x)\,\&\,q(x)]p(x,x') \leftrightarrow [x' = f(x)\,\&\,q(x)][x' := f(x)]p(x,x')$$



Effect of differential equation on differential symbol x'

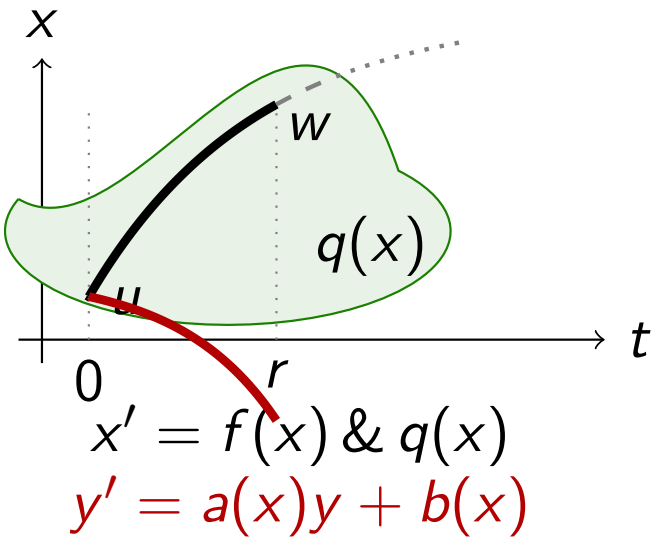
$[x' := f(x)]$ instantly mimics continuous effect $[x' = f(x)]$ on x'

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

Differential Equation Axioms

Axiom (Differential Ghost) (CADE'15)

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

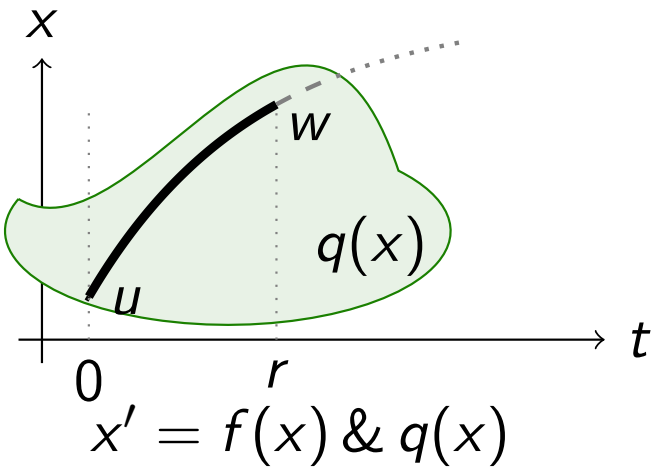


Differential ghost/auxiliaries: extra differential equations that exist
Can cause new invariants
"Dark matter" counterweight to balance conserved quantities

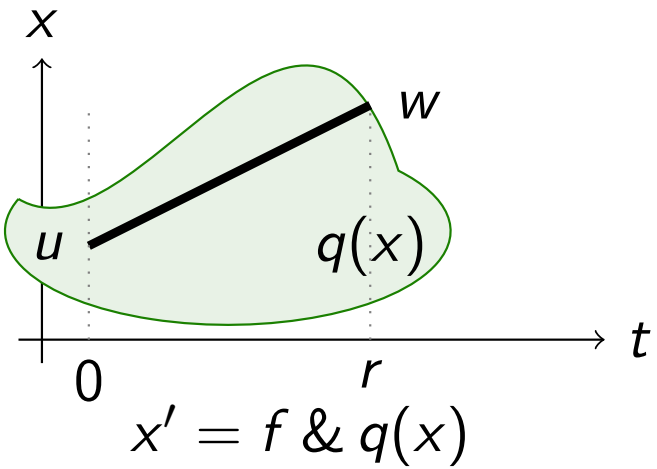
Differential Equation Axioms

Axiom (Differential Solution) (CADE'15)

(DS) $[x' = f \,\&\, q(x)]p(x) \leftrightarrow \forall t{\geq}0 \left((\forall 0{\leq}s{\leq}t\, q(x{+}fs)) \rightarrow [x := x + ft]p(x)\right)$



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



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

Differential solutions: solve differential equations with DG,DC and inverse companions

1. DI proves a property of an ODE inductively by its differentials
2. DE exports vector field, possibly after DW exports evolution domain
3. CE+CQ reason efficiently in Equivalence or eQuational context
4. G isolates postcondition
5. $[':=]$ differential substitution uses vector field
6. $\cdot'$ differential computations are axiomatic (US)

$$\text{DI}\,\frac{\text{DE}\,\frac{\text{CE}\,\frac{\text{G}\,\frac{[':=]\,\frac{\text{QE}\,\frac{*}{x^3\cdot x + x\cdot x^3 \geq 0}}{[x' := x^3]x'\cdot x + x\cdot x' \geq 0}}{[x' = x^3][x' := x^3]x'\cdot x + x\cdot x' \geq 0}}{[x' = x^3][x' := x^3](x\cdot x \geq 1)'}}{[x' = x^3](x\cdot x \geq 1)'}}{x\cdot x \geq 1 \rightarrow [x' = x^3]x\cdot x \geq 1}$$

$$\text{CQ}\,\frac{\text{US}\,\frac{\cdot'\,\frac{*}{(f(\bar{x})\cdot g(\bar{x}))' = (f(\bar{x}))'\cdot g(\bar{x}) + f(\bar{x})\cdot(g(\bar{x}))'}}{(x\cdot x)' = (x)'\cdot x + x\cdot(x)'}}{(x\cdot x)' = x'\cdot x + x\cdot x'}$$

$$\frac{(x\cdot x)' \geq 0 \leftrightarrow x'\cdot x + x\cdot x' \geq 0}{(x\cdot x \geq 1)' \leftrightarrow x'\cdot x + x\cdot x' \geq 0}$$

$$[\![(\theta)']\!]u = \text{???}$$

$$[\![(x^2)']\!]u$$

The Meaning of Primes

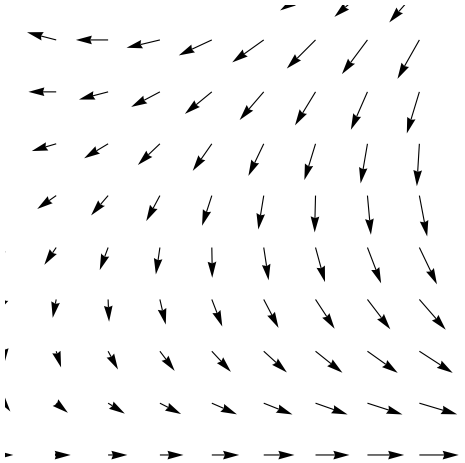
$$[\![(\theta)']\!]u = \ ???$$
$$[\![(x^2)']\!]u = [\![2x]\!]u \ ?$$

The Meaning of Primes

$$[\![(\theta)']\!]u = \text{ ???}$$

$$[\![(x^2)']\!]u = [\![2x]\!]u \text{ ?}$$

depends on the differential equation ...



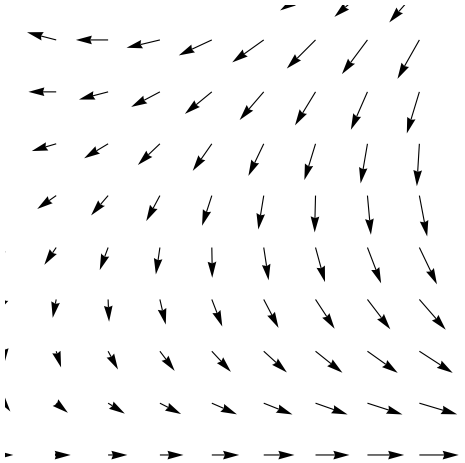
The Meaning of Primes

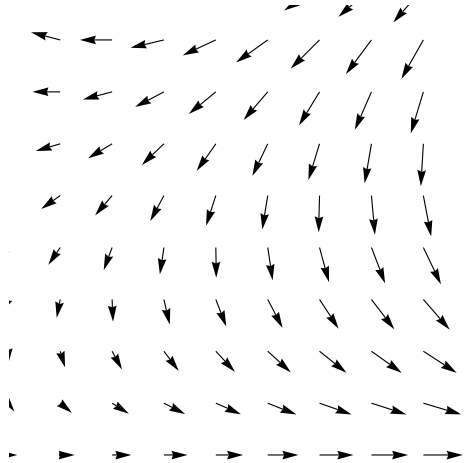
$[\![(\theta)']\!]u = \;???$

$[\![(x^2)']\!]u = [\![2x]\!]u\;?$

depends on the differential equation ...

well-defined locally in an isolated state at all?





$[\![(\theta)']\!]u = \;???$

$[\![(x^2)']\!]u = [\![2x]\!]u\;?$

depends on the differential equation ...

well-defined locally in an isolated state at all?

$$[\![(\theta)']\!]u = \sum_x u(x')\frac{\partial [\![\theta]\!]^I}{\partial x}(u) = \sum_x u(x')\frac{\partial [\![\theta]\!]u_x^X}{\partial X}$$

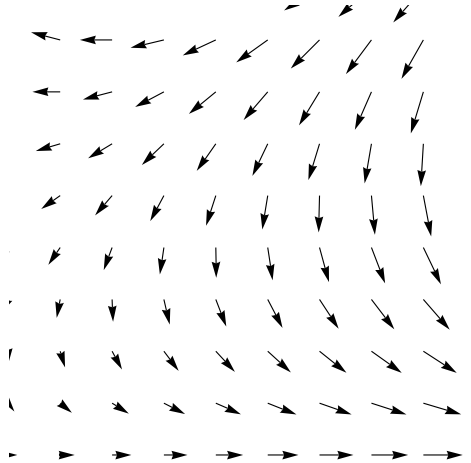
$$[\![(\theta)']\!] = d[\![\theta]\!] = \sum_{i=1}^{n} \frac{\partial [\![\theta]\!]}{\partial x^i} dx^i$$

depends on state u

tangent space basis

cotangent space basis

depends on $u(x_i') = dx^i$



$[\![(\theta)']\!]u = \;???$

$[\![(x^2)']\!]u = [\![2x]\!]u\;?$

depends on the differential equation . . .

well-defined locally in an isolated state at all?

$$[\![(\theta)']\!]u = \sum_x u(x')\frac{\partial [\![\theta]\!]'}{\partial x}(u) = \sum_x u(x')\frac{\partial [\![\theta]\!] u_x^X}{\partial X}$$

$$[\![(\theta)']\!] = d[\![\theta]\!] = \sum_{i=1}^{n} \frac{\partial [\![\theta]\!]}{\partial x^i} dx^i$$

$u(x')$ is the local shadow of $\frac{\mathrm{d}x}{\mathrm{d}t}$ if that existed

$(\theta)'$ represents how θ changes locally, depending on x'

Differential Substitution Lemmas

Lemma (Differential lemma)

If $\varphi \models x' = f(x) \land Q$ *for duration* $r > 0$, *then for all* $0 \leq \zeta \leq r$:

Syntactic $[\![(\eta)']\!]\varphi(\zeta) = \dfrac{\mathrm{d}[\![\eta]\!]\varphi(t)}{\mathrm{d}t}(\zeta)$ Analytic

Lemma (Differential assignment)

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

Lemma (Derivations)

$$(\theta + \eta)' = (\theta)' + (\eta)'$$

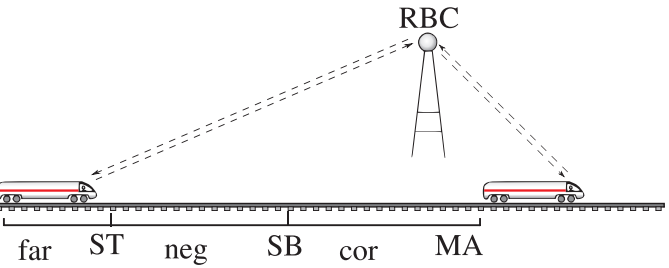
$$(\theta \cdot \eta)' = (\theta)' \cdot \eta + \theta \cdot (\eta)'$$

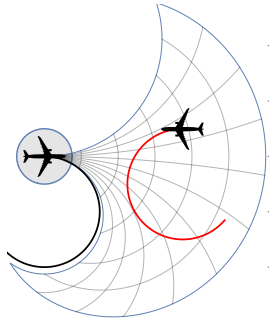
$$[y := \theta][y' := 1]((f(\theta))' = (f(y))' \cdot (\theta)') \quad \text{for } y, y' \notin \theta$$

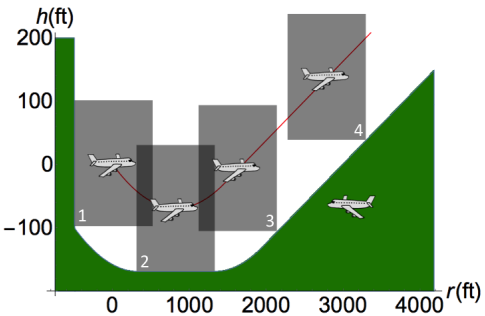
$$(f)' = 0 \quad \text{for arity 0 functions/numbers } f$$

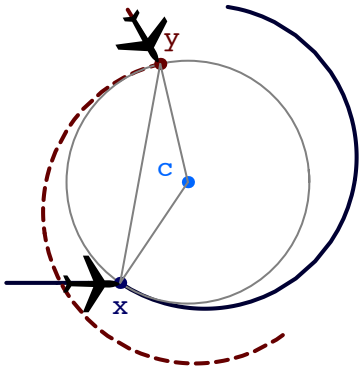
Outline

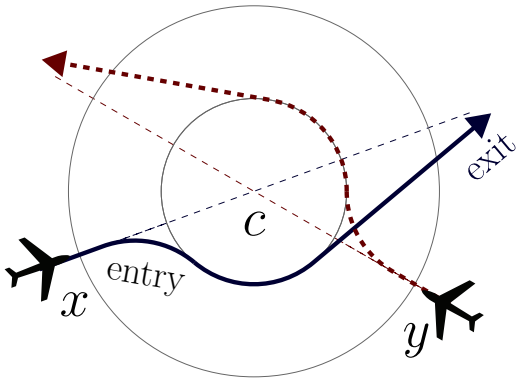
Verified CPS Applications

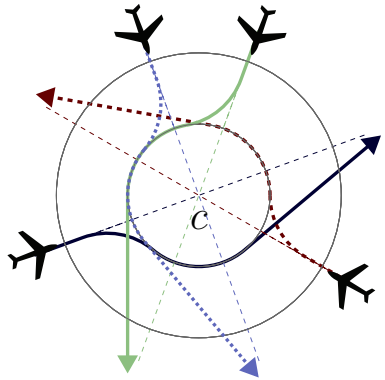


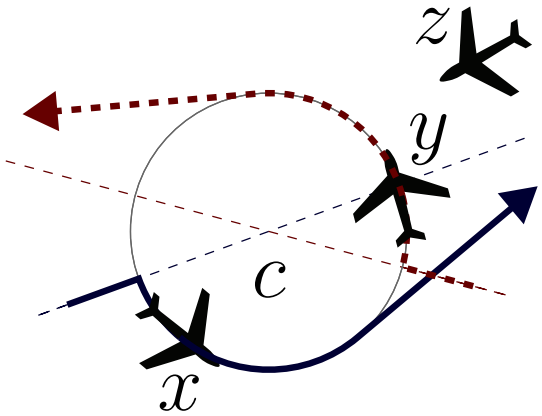


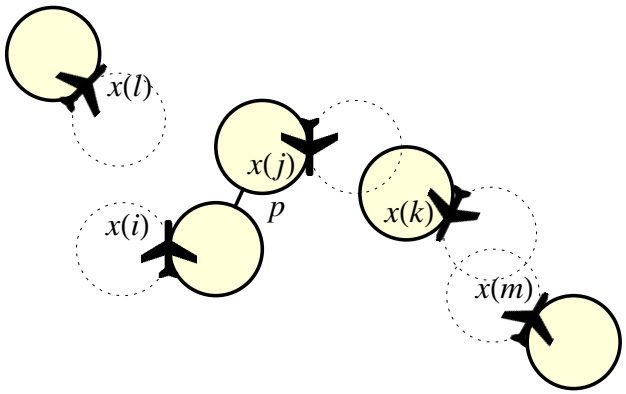


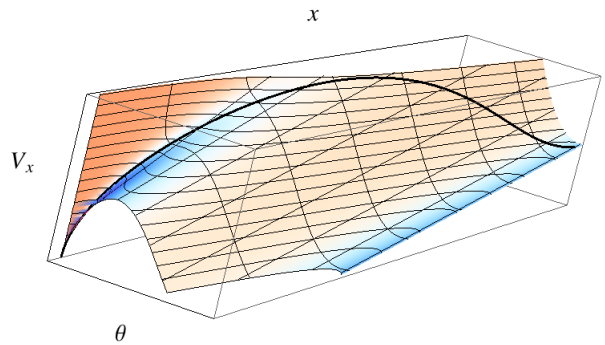






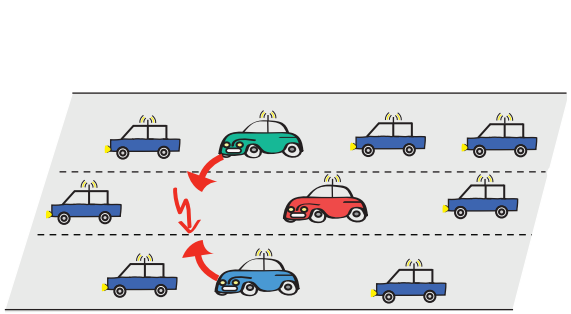


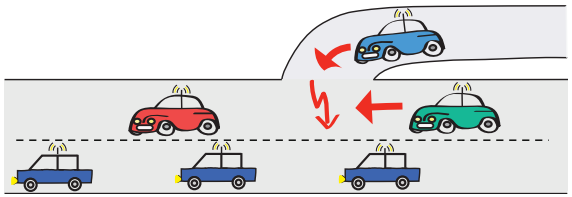


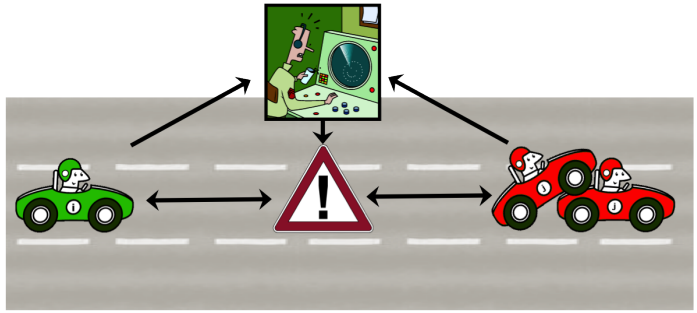


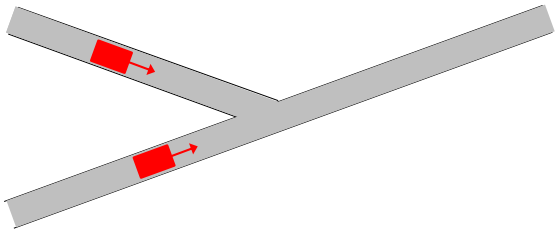
ICFEM'09,JAIS'14,TACAS'15,CAV'08,FM'09,HSCC'11,HSCC'13, TACAS'14

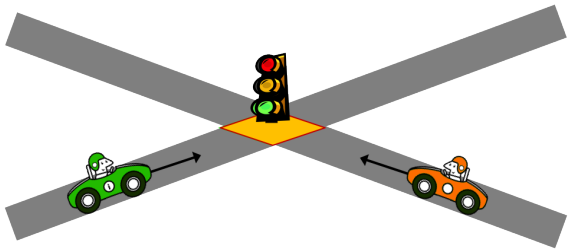
Verified CPS Applications

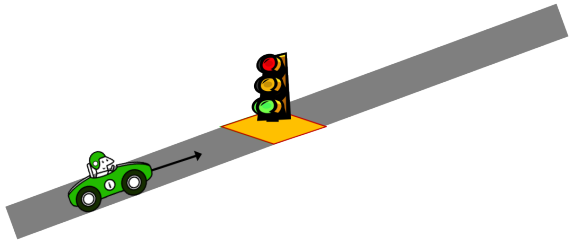


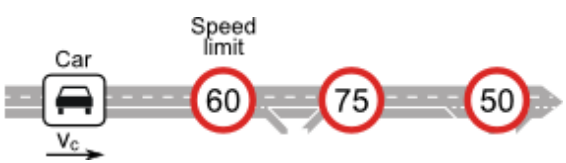


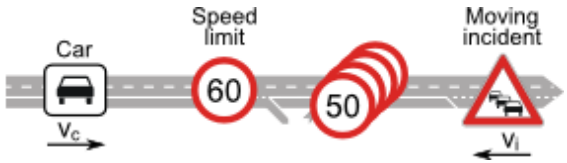


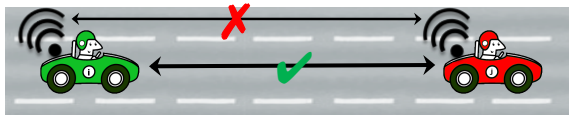


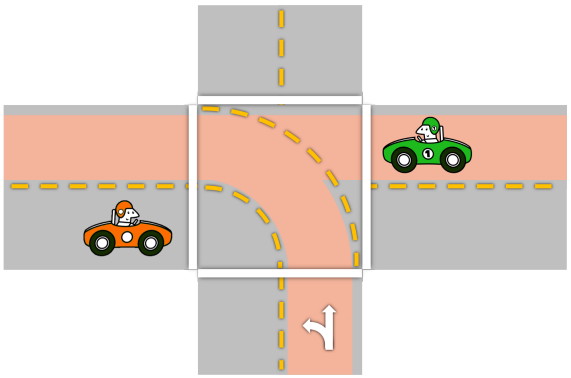


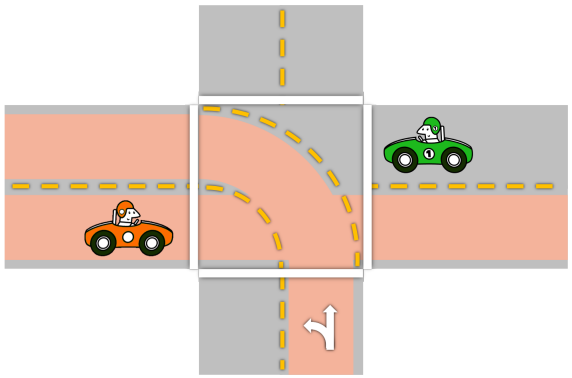


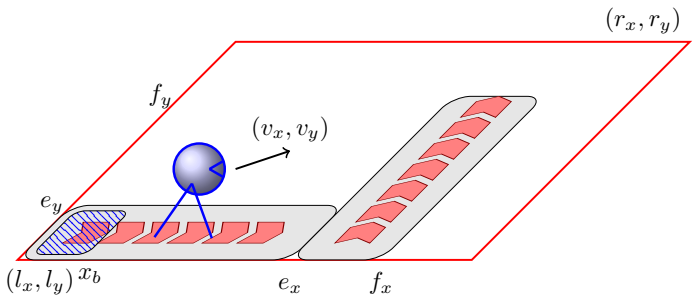






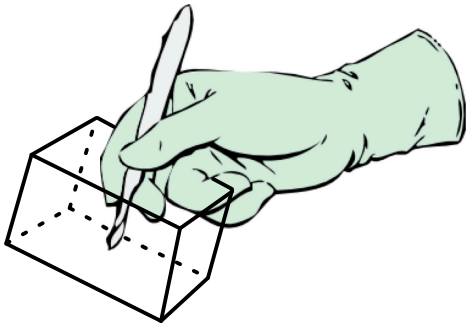


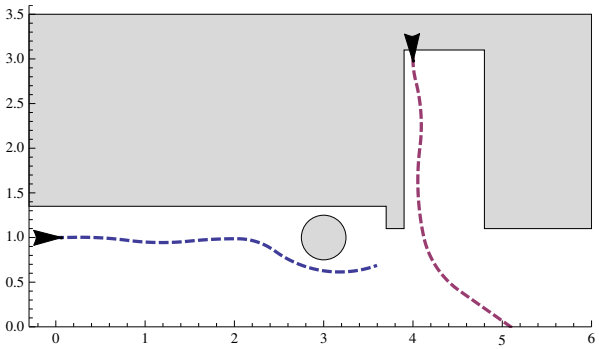


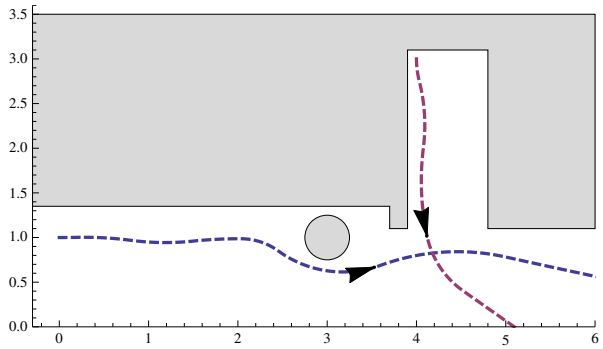


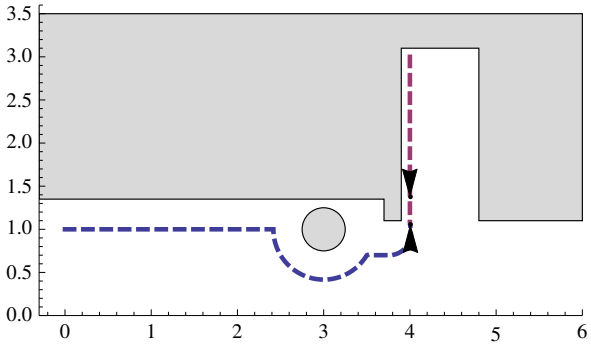
FM'11,LMCS'12,ICCPS'12,ITSC'11,ITSC'13,IJCAR'12

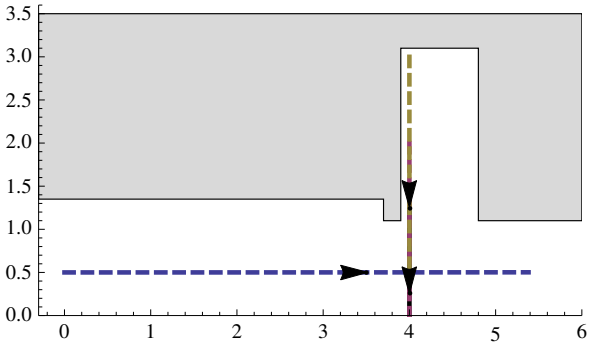
Verified CPS Applications

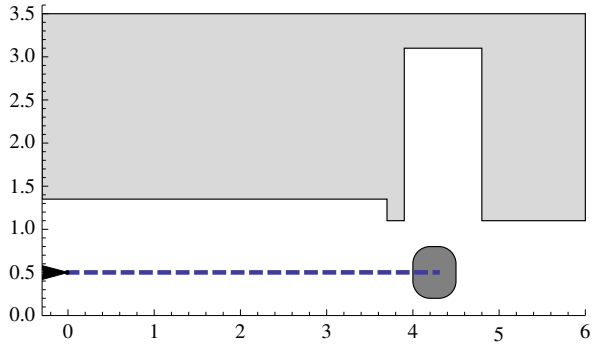


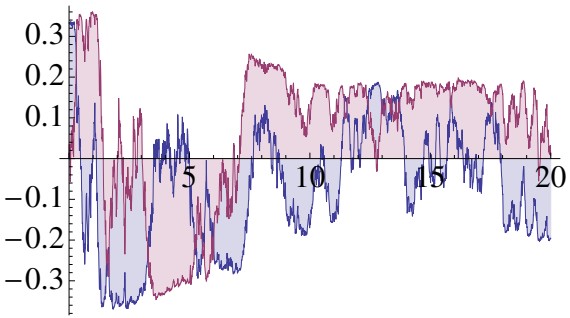


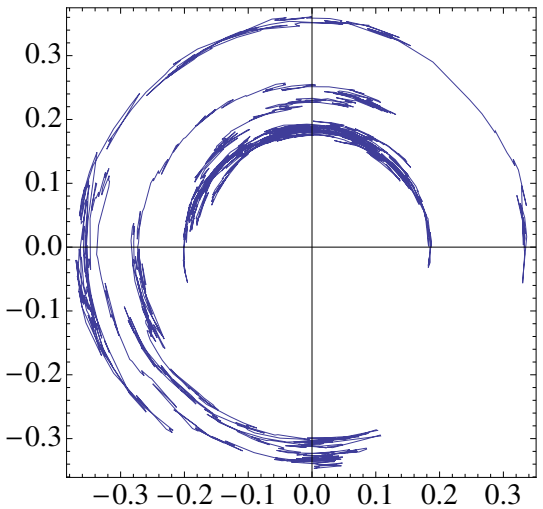


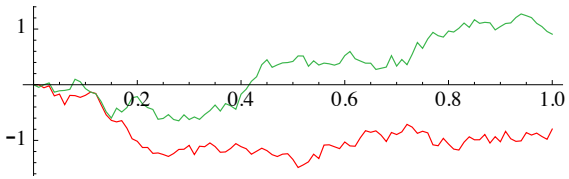






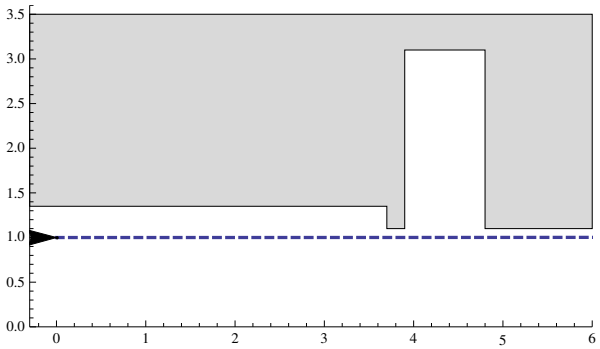
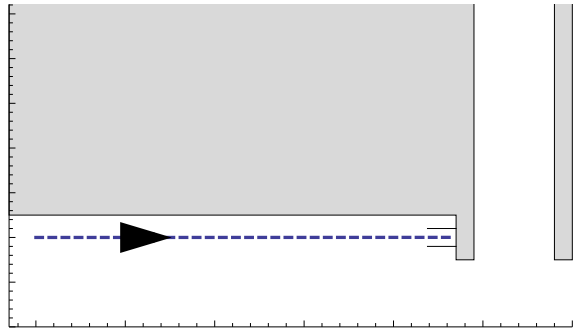
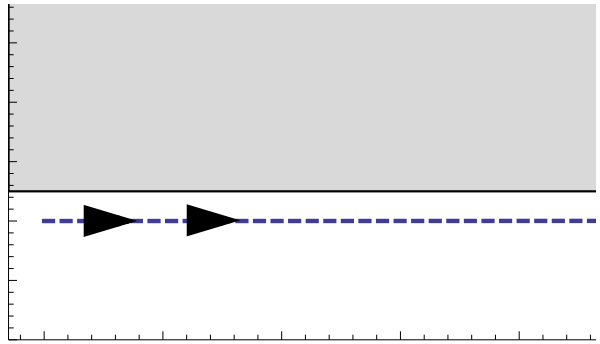
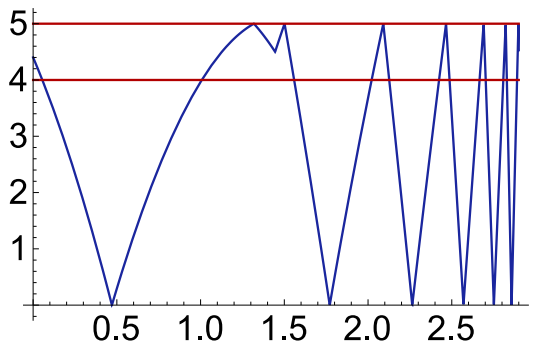
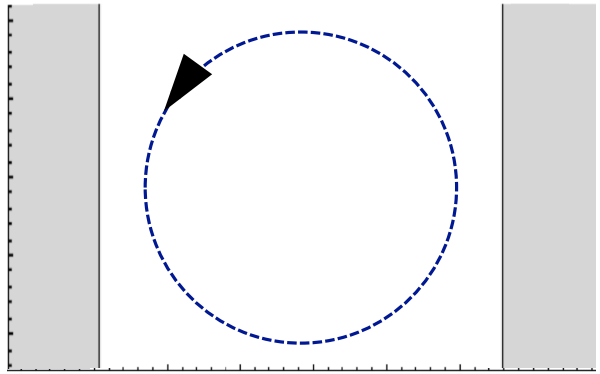
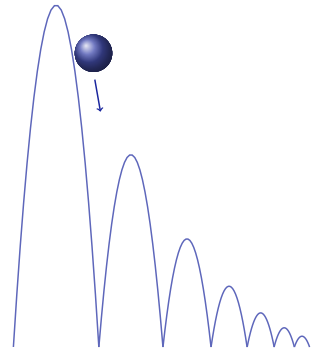
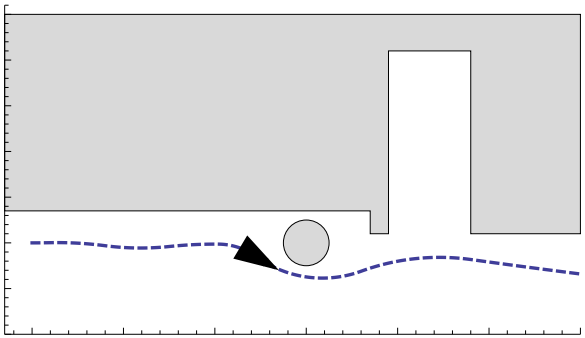
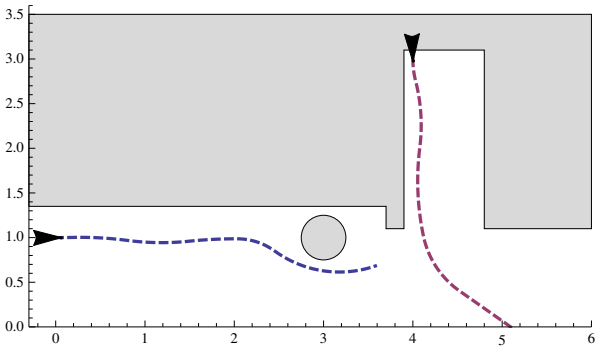
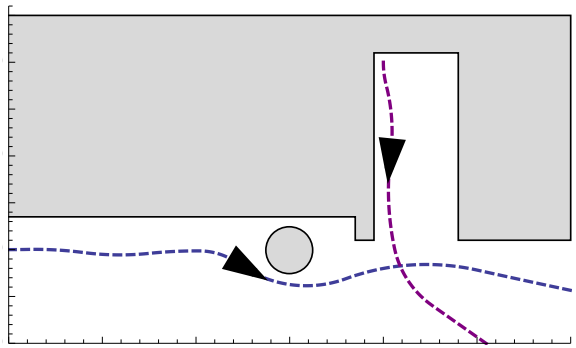






HSCC'13,RSS'13,CADE'12

Verified CPS Applications By Undergrads

15-424/624 *Foundations of Cyber-Physical Systems* students

Outline

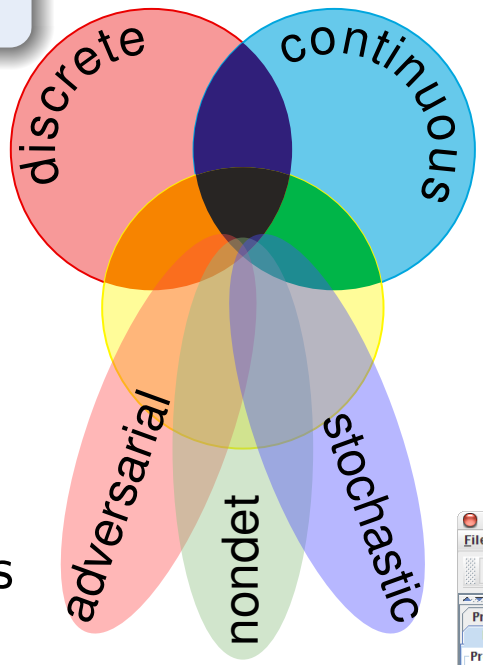
KeYmaera X Kernel: Qualifies as a Microkernel

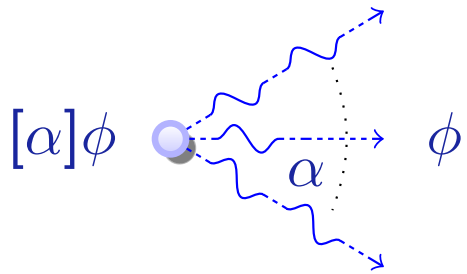
	≈LOC	
KeYmaera X	1 682	
KeYmaera	65 989	
KeY	51 328	
HOL Light	396	
Isabelle/Pure	8 113	
Nuprl	15 000	+ 50 000
Coq	20 000	
HSolver	20 000	
Flow*	25 000	
PHAVer	30 000	
dReal	50 000	+ millions
SpaceEx	100 000	
HyCreate2	6 081	+ user model analysis

Disclaimer: These self-reported estimates of the soundness-critical lines of code + rules are to be taken with a grain of salt. Different languages, capabilities, styles

differential dynamic logic

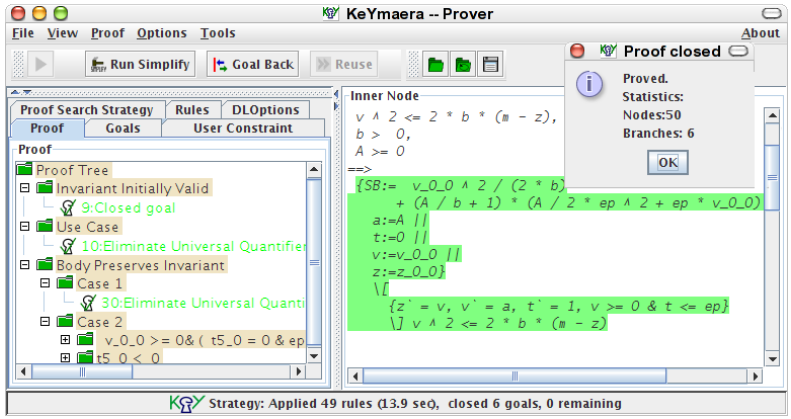
$$\mathrm{d}\mathcal{L} = \mathrm{DL} + \mathrm{HP}$$





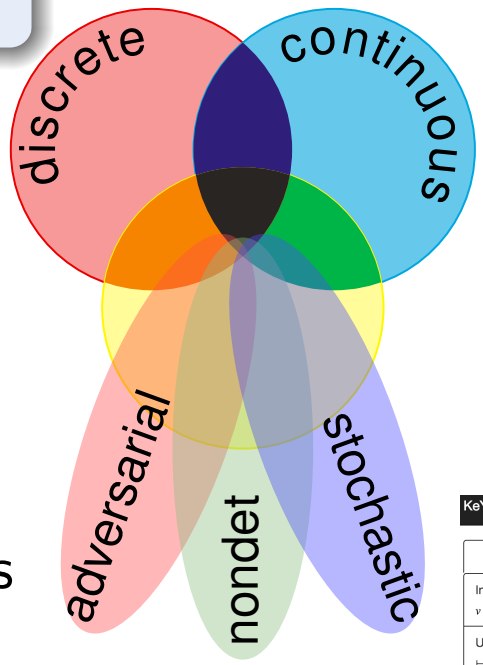
- Multi-dynamical systems
- Combine simple dynamics
- Tame complexity
- Logic & proofs for CPS
- Theory of CPS
- Applications

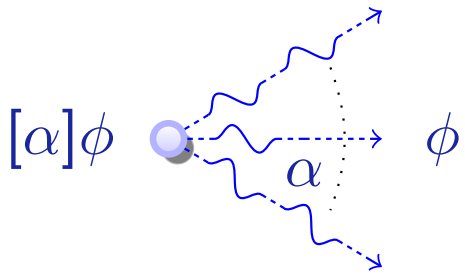
KeYmaera Prover



differential dynamic logic

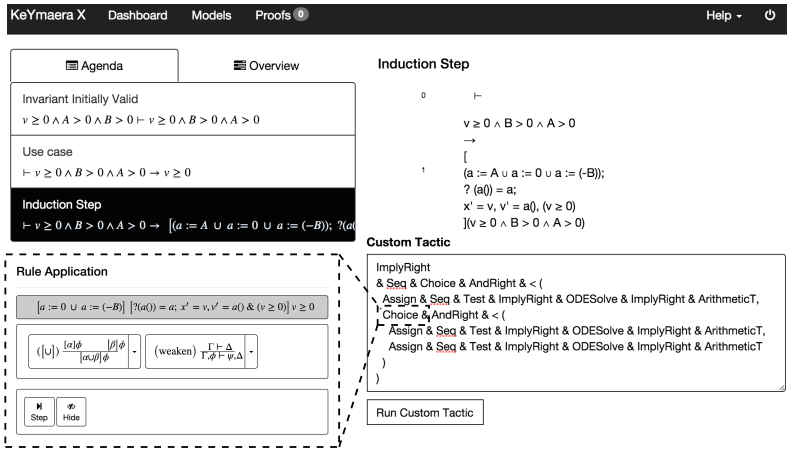
$$\mathrm{d}\mathcal{L} = \mathrm{DL} + \mathrm{HP}$$





- Multi-dynamical systems
- Combine simple dynamics
- Tame complexity
- Logic & proofs for CPS
- Theory of CPS
- Applications

KeYmaera X



Acknowledgments

Students and postdocs of the Logical Systems Lab at Carnegie Mellon
Nathan Fulton, David Henriques, Sarah Loos, João Martins, Erik Zawadzki
Khalil Ghorbal, Jean-Baptiste Jeannin, Stefan Mitsch

BOSCH
Invented for life

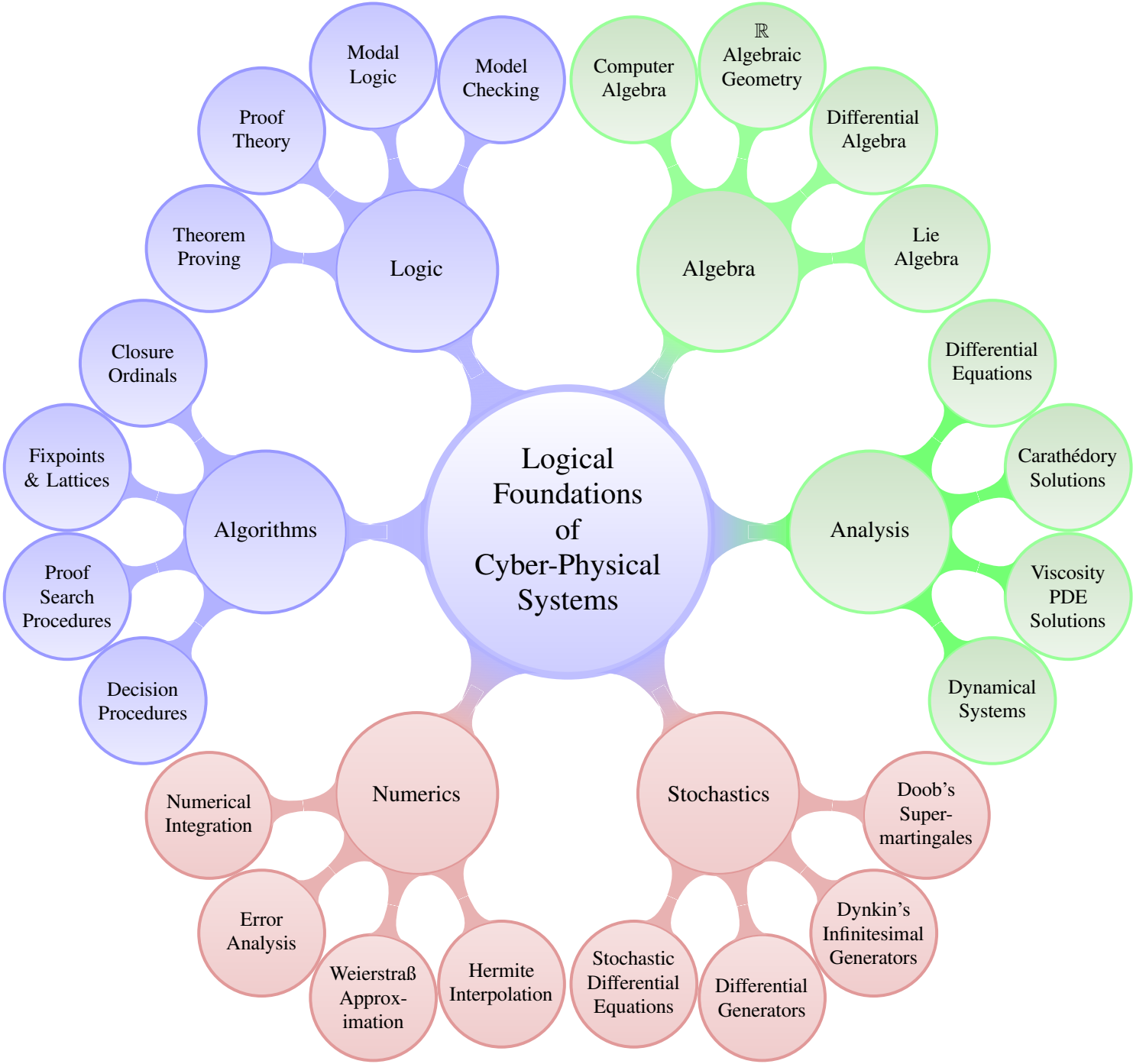
TOYOTA
TOYOTA TECHNICAL CENTER

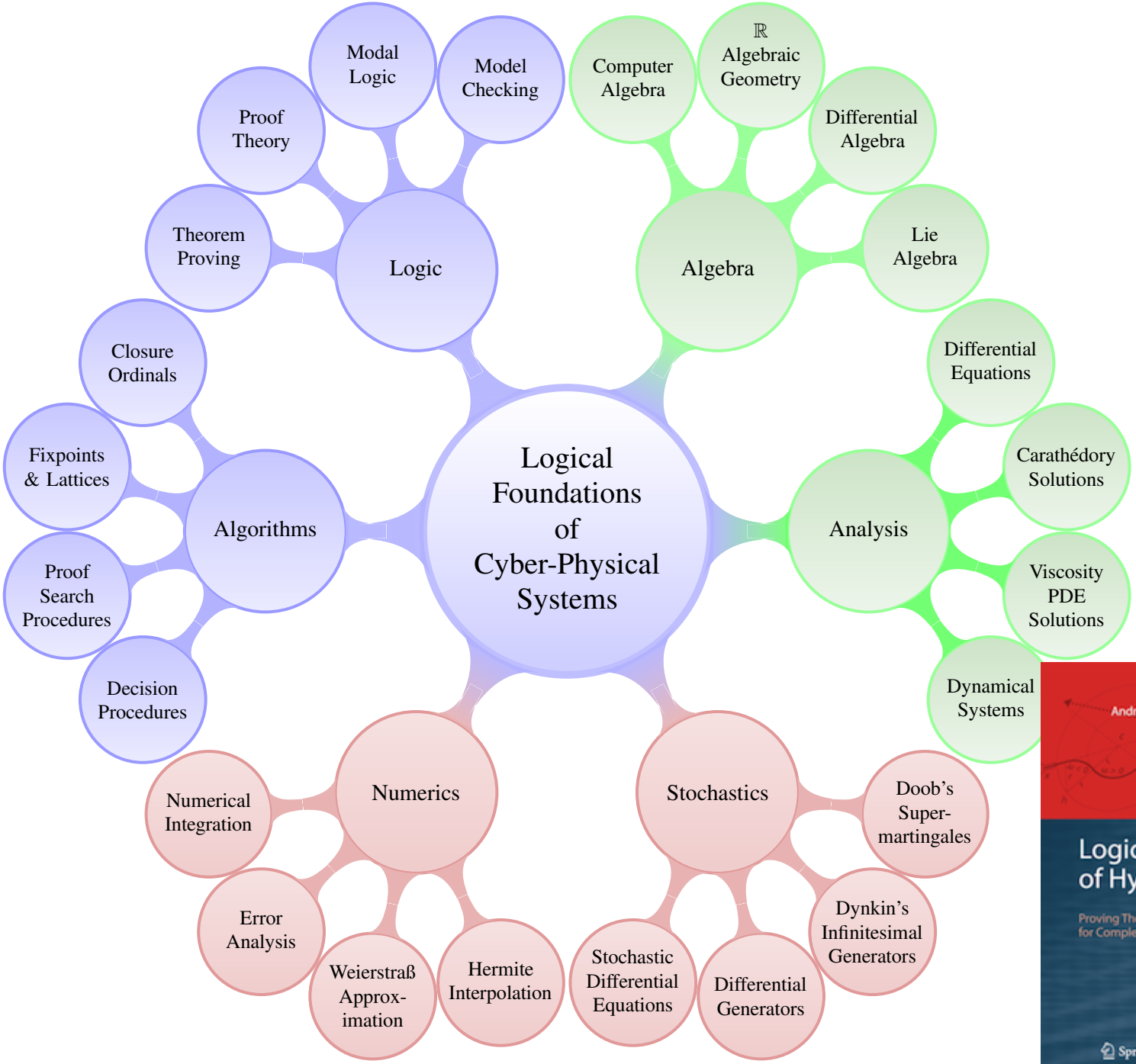
JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

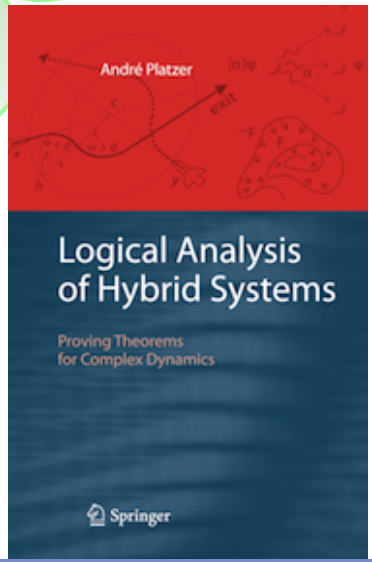
How to trust a computer to control physics

Recipe

1. CPS promise a transformative impact
2. CPS have to be safe to make the world a better place
3. Safety needs a safety analysis
4. Analytic tools for CPS have to be sound
5. Sound analysis needs sound and strong foundations
6. Foundations themselves have to be challenged, e.g., by applications
7. Logic has a lot to offer for CPS
8. CPS bring excitement and new challenges to logic


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
Carathédory Solutions
Viscosity PDE Solutions
Dynamical Systems
Algorithms
Closure Ordinals
Fixpoints & Lattices
Proof Search Procedures
Decision Procedures
Numerics
Numerical Integration
Error Analysis
Weierstraß Approx-imation
Hermite Interpolation
Stochastics
Doob's Super-martingales
Dynkin's Infinitesimal Generators
Stochastic Differential Equations
Differential Generators


Logical Foundations of Cyber-Physical Systems
Logic
Modal Logic
Model Checking
Proof Theory
Theorem Proving
Algebra
Computer Algebra
$\mathbb{R}$ Algebraic Geometry
Differential Algebra
Lie Algebra
Analysis
Differential Equations
Carathédory Solutions
Viscosity PDE Solutions
Dynamical Systems
Algorithms
Closure Ordinals
Fixpoints & Lattices
Proof Search Procedures
Decision Procedures
Numerics
Numerical Integration
Error Analysis
Weierstraß Approx-imation
Hermite Interpolation
Stochastics
Doob's Super-martingales
Dynkin's Infinitesimal Generators
Stochastic Differential Equations
Differential Generators


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

$([:=])\quad [x := f]p(x) \leftrightarrow p(f)$

$([?])\quad [?q]p \leftrightarrow (q \rightarrow p)$

$([\cup])\quad [a \cup b]p(\bar{x}) \leftrightarrow [a]p(\bar{x}) \wedge [b]p(\bar{x})$

$([;])\quad [a; b]p(\bar{x}) \leftrightarrow [a][b]p(\bar{x})$

$([^*])\quad [a^*]p(\bar{x}) \leftrightarrow p(\bar{x}) \wedge [a][a^*]p(\bar{x})$

$(K)\quad [a](p(\bar{x}) \rightarrow q(\bar{x})) \rightarrow ([a]p(\bar{x}) \rightarrow [a]q(\bar{x}))$

$(I)\quad [a^*](p(\bar{x}) \rightarrow [a]p(\bar{x})) \rightarrow (p(\bar{x}) \rightarrow [a^*]p(\bar{x}))$

$(V)\quad p \rightarrow [a]p$

$(DS)\quad [x' = f]p(x) \leftrightarrow \forall t \geq 0\, [x := x + ft]p(x)$

LICS'12,CADE'15

$$\text{(G)}\quad \frac{p(\bar{x})}{[a]p(\bar{x})}$$

$$\text{(}\forall\text{)}\quad \frac{p(x)}{\forall x\, p(x)}$$

$$\text{(MP)}\quad \frac{p \rightarrow q \quad p}{q}$$

$$\text{(CT)}\quad \frac{f(\bar{x}) = g(\bar{x})}{c(f(\bar{x})) = c(g(\bar{x}))}$$

$$\text{(CQ)}\quad \frac{f(\bar{x}) = g(\bar{x})}{p(f(\bar{x})) \leftrightarrow p(g(\bar{x}))}$$

$$\text{(CE)}\quad \frac{p(\bar{x}) \leftrightarrow q(\bar{x})}{C(p(\bar{x})) \leftrightarrow C(q(\bar{x}))}$$

LICS'12,CADE'15

Differential Equation Axioms & Differential Axioms

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

(DC) $\big([x' = f(x) \,\&\, q(x)]p(x) \leftrightarrow [x' = f(x) \,\&\, q(x) \wedge r(x)]p(x)\big)$
$\leftarrow [x' = f(x) \,\&\, q(x)]r(x)$

(DE) $[x' = f(x) \,\&\, q(x)]p(x, x') \leftrightarrow [x' = f(x) \,\&\, q(x)][x' := f(x)]p(x, x')$

(DI) $[x' = f(x) \,\&\, q(x)]p(x) \leftarrow \big(q(x) \rightarrow p(x) \wedge [x' = f(x) \,\&\, q(x)](p(x))'\big)$

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

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

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

$(+')$ $(f(\bar{x}) + g(\bar{x}))' = (f(\bar{x}))' + (g(\bar{x}))'$

$(\cdot')$ $(f(\bar{x}) \cdot g(\bar{x}))' = (f(\bar{x}))' \cdot g(\bar{x}) + f(\bar{x}) \cdot (g(\bar{x}))'$

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

CADE'15


André Platzer.
Logics of dynamical systems.
In LICS [17], pages 13–24.
doi:10.1109/LICS.2012.13.


André Platzer.
Foundations of cyber-physical systems.
Lecture Notes 15-424/624, Carnegie Mellon University, 2014.
URL: http://www.cs.cmu.edu/~aplatzer/course/fcps14/fcps14.pdf.


André Platzer.
Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics.
Springer, Heidelberg, 2010.
doi:10.1007/978-3-642-14509-4.


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 uniform substitution calculus for differential dynamic logic.
In Amy Felty and Aart Middeldorp, editors, *CADE*, volume 9195 of *LNCS*, pages 467–481. Springer, 2015.
doi:10.1007/978-3-319-21401-6_32.


André Platzer.
Differential game logic.
ACM Trans. Comput. Log., 2015.
To appear. Preprint at arXiv 1408.1980.
doi:10.1145/2817824.


André Platzer.
The complete proof theory of hybrid systems.
In LICS [17], 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):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 431–445. Springer, 2011.
doi:10.1007/978-3-642-22438-6_34.


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.
In Aarti Gupta and Sharad Malik, editors, *CAV*, volume 5123 of *LNCS*, pages 176–189. Springer, 2008.

doi:10.1007/978-3-540-70545-1_17.


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):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. Springer, 2012.
doi:10.1007/978-3-642-32347-8_3.


Khalil Ghorbal, Andrew Sogokon, and André Platzer.

Invariance of conjunctions of polynomial equalities for algebraic differential equations.
In Markus Müller-Olm and Helmut Seidl, editors, *SAS*, volume 8723 of *LNCS*, pages 151–167. Springer, 2014.
doi:10.1007/978-3-319-10936-7_10.

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. Springer, 2014.
doi:10.1007/978-3-642-54862-8_19.

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

Outline

Theorem (Differential radical invariant characterization)

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

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

$$(h^{(N)})^p_{x'} = \sum_{i=0}^{N-1} g_i (h^{(i)})^p_{x'} \quad (g_i \in \mathbb{R}[x])$$

Corollary (Algebraic Invariants Decidable)

Algebraic invariants of algebraic differential equations are decidable.

with Khalil Ghorbal TACAS'14

Study (6th Order Longitudinal Flight Equations)

$$u' = \frac{X}{m} - g\sin(\theta) - qw \quad \text{axial velocity}$$

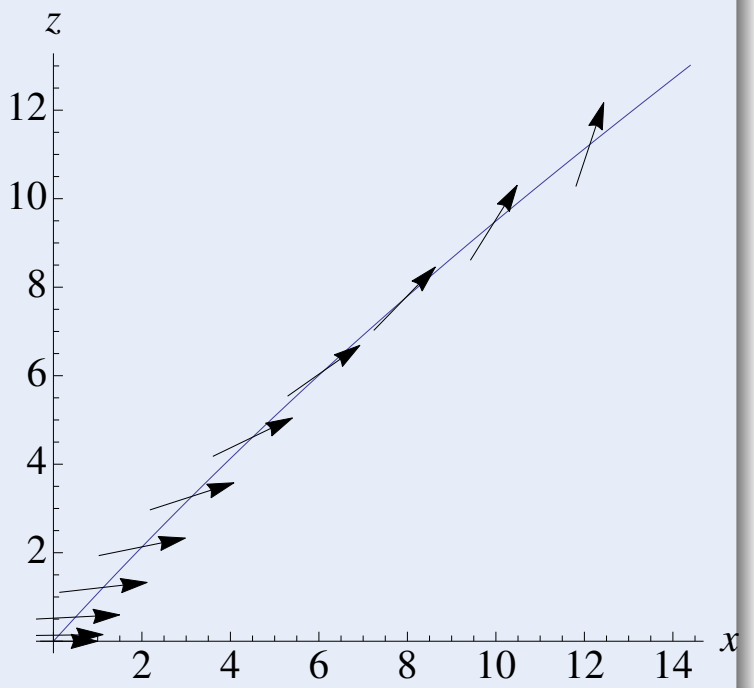
$$w' = \frac{Z}{m} + g\cos(\theta) + qu \quad \text{vertical velocity}$$

$$x' = \cos(\theta)u + \sin(\theta)w \quad \text{range}$$

$$z' = -\sin(\theta)u + \cos(\theta)w \quad \text{altitude}$$

$$\theta' = q \quad \text{pitch angle}$$

$$q' = \frac{M}{I_{yy}} \quad \text{pitch rate}$$



X : thrust along u Z : thrust along w M : thrust moment for w

g : gravity m : mass I_{yy} : inertia second diagonal

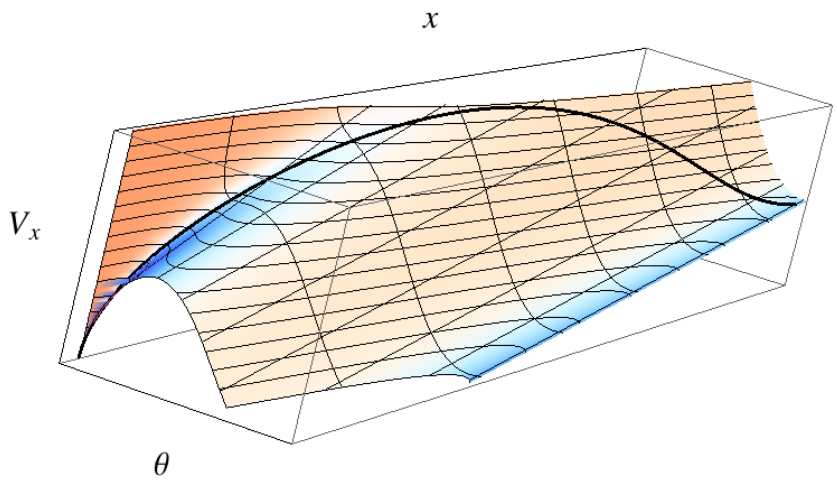
with Khalil Ghorbal TACAS'14

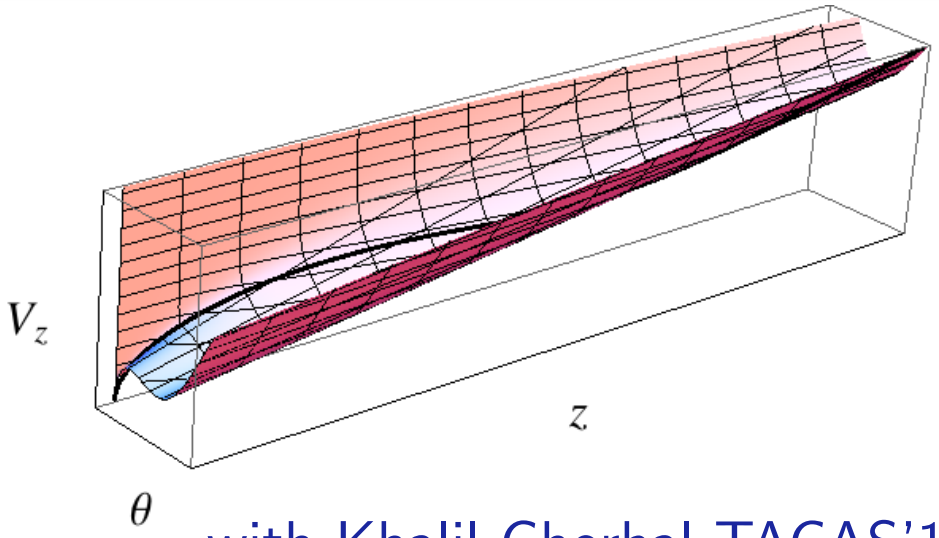
Result (DRI Automatically Generates Invariant Functions)

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

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

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



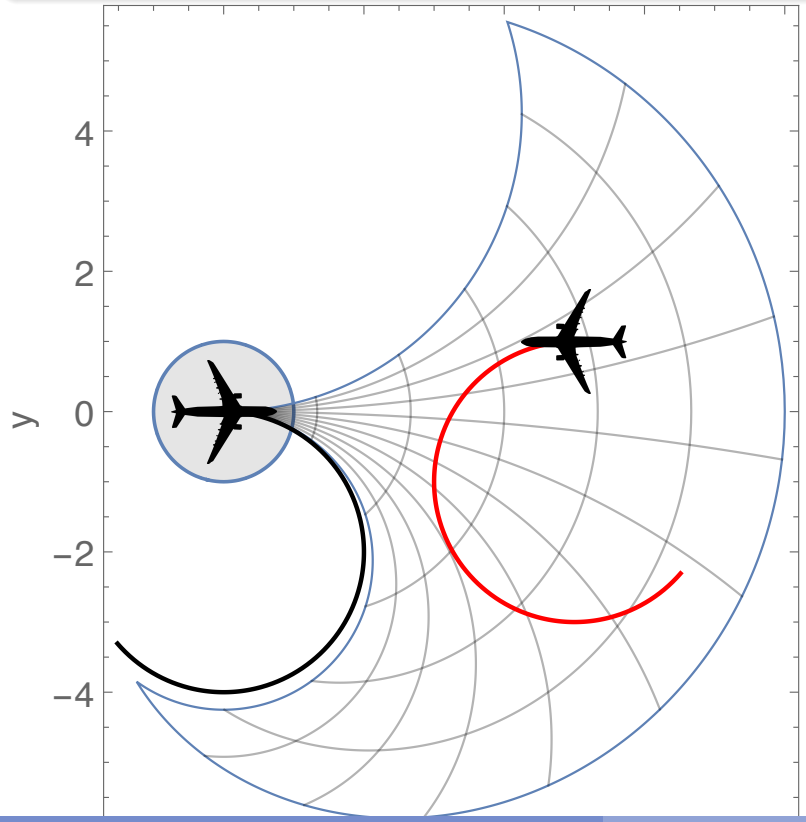


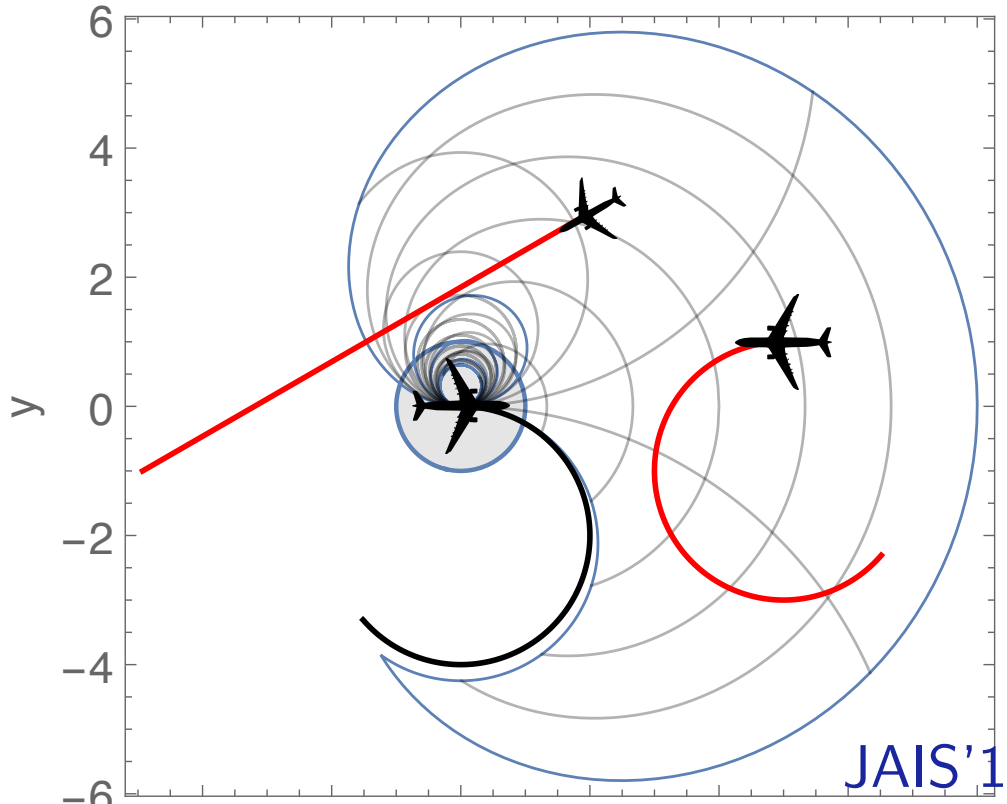
with Khalil Ghorbal TACAS'14

Result (DRI Automatically Generates Invariants)

$$\omega_1 = 0 \wedge \omega_2 = 0 \rightarrow v_2 \sin\vartheta x = (v_2 \cos\vartheta - v_1) y > p(v_1 + v_2)$$

$$\omega_1 \neq 0 \vee \omega_2 \neq 0 \rightarrow -\omega_1\omega_2(x^2 + y^2) + 2v_2\omega_1 \sin\vartheta x + 2(v_1\omega_2 - v_2\omega_1 \cos\vartheta) y + 2v_1 v_2 \cos\vartheta > 2v_1 v_2 + 2p(v_2|\omega_1| + v_1|\omega_2|) + p^2|\omega_1\omega_2|$$



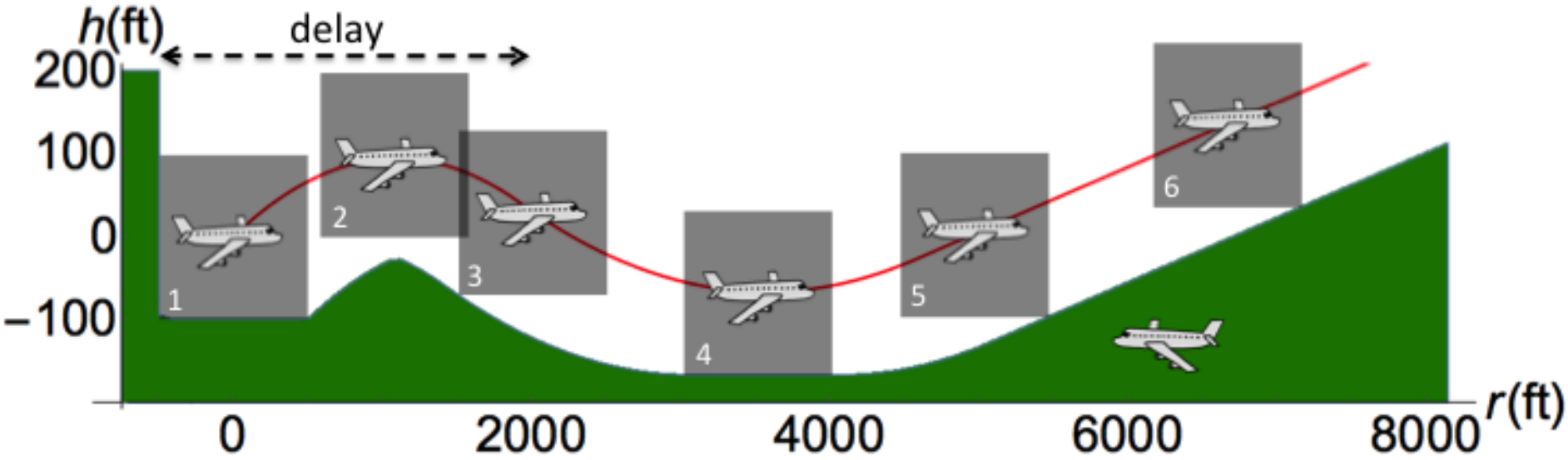


JAIS'14

Outline

Airborne Collision Avoidance System ACAS X: Verify

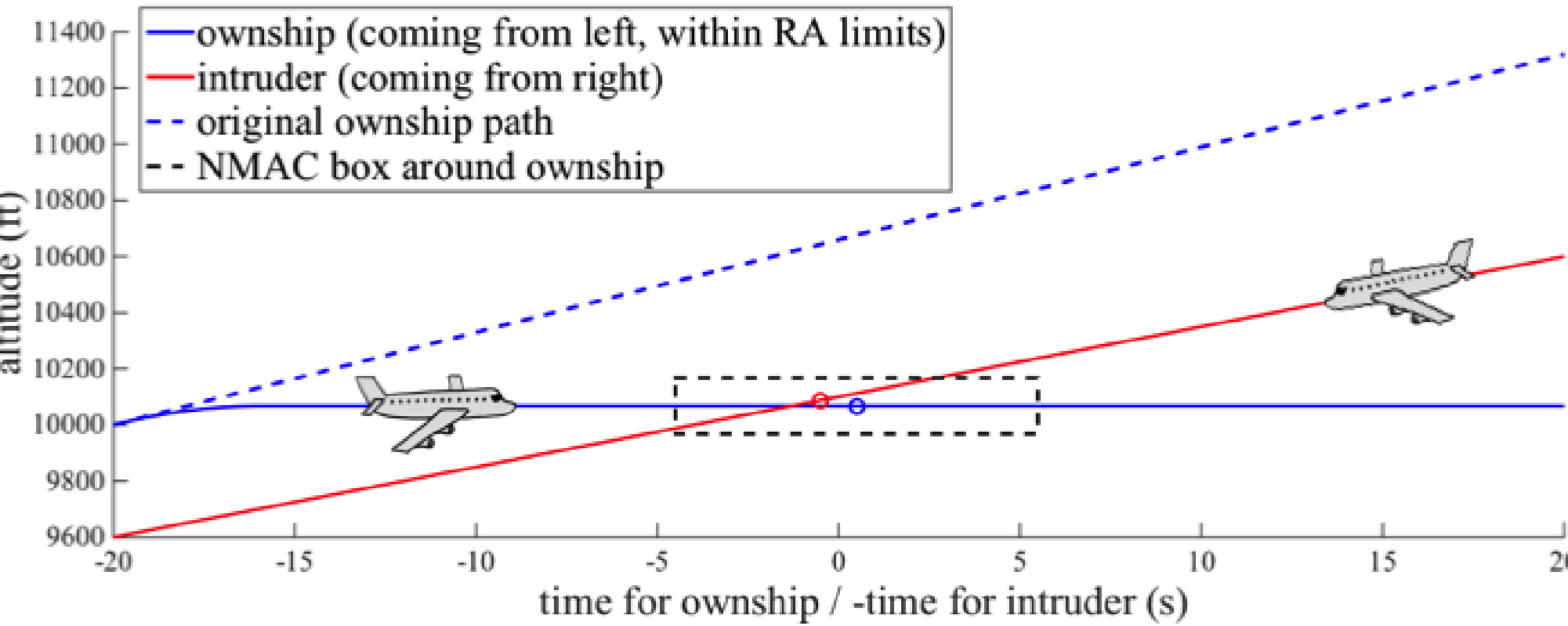
- Developed by the FAA to replace current TCAS in aircraft
- Approximately optimizes Markov Decision Process on a grid
- Advisory from lookup tables with numerous 5D interpolation regions



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

TACAS'15

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

TACAS'15