

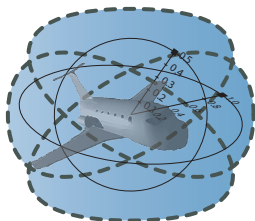
Proving Hybrid Systems

André Platzer

`aplatzer@cs.cmu.edu`

Computer Science Department

Carnegie Mellon University, Pittsburgh, PA





- 1 CPS are Multi-Dynamical Systems
 - Hybrid Systems
 - Hybrid Games
- 2 Dynamic Logic of Dynamical Systems
 - Syntax
 - Semantics
 - Example: Car Control Design
- 3 Proofs for CPS
 - Compositional Proof Calculus
 - Example: Safe Car Control
- 4 Theory of CPS
 - Soundness and Completeness
 - Differential Invariants
 - Example: Elementary Differential Invariants
 - Differential Axioms
- 5 Applications
- 6 Summary



- 1 CPS are Multi-Dynamical Systems
 - Hybrid Systems
 - Hybrid Games
- 2 Dynamic Logic of Dynamical Systems
 - Syntax
 - Semantics
 - Example: Car Control Design
- 3 Proofs for CPS
 - Compositional Proof Calculus
 - Example: Safe Car Control
- 4 Theory of CPS
 - Soundness and Completeness
 - Differential Invariants
 - Example: Elementary Differential Invariants
 - Differential Axioms
- 5 Applications
- 6 Summary

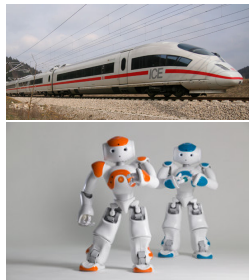
A CPSs Promise Transformative Impact!

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.

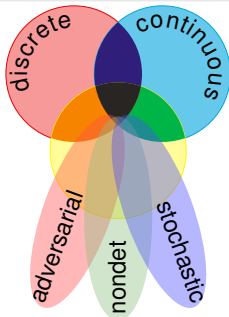
How can we provide people with cyber-physical systems they can bet their lives on?
— Jeannette Wing



CPSs are Multi-Dynamical Systems

CPS Dynamics

CPS are characterized by multiple facets of dynamical systems.



CPS Compositions

CPS combine multiple simple dynamical effects.

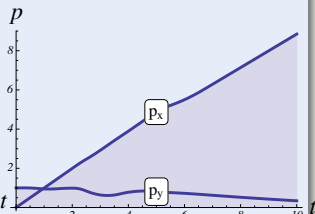
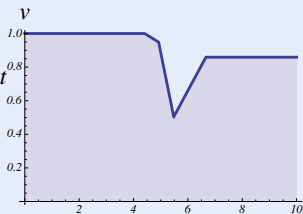
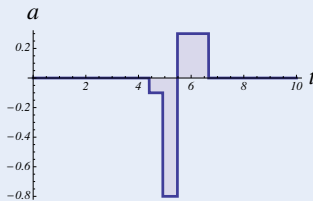
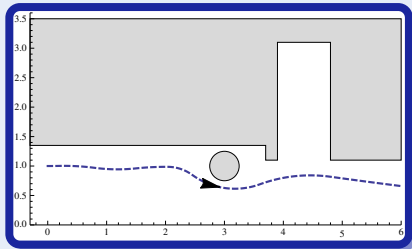
Tame Parts

Exploiting compositionality tames CPS complexity.

Challenge (Hybrid Systems)

Fixed rule describing state evolution with both

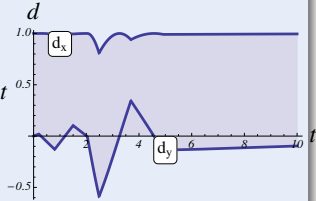
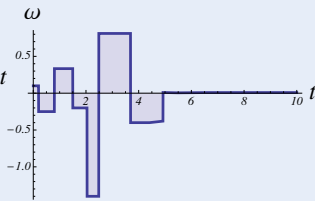
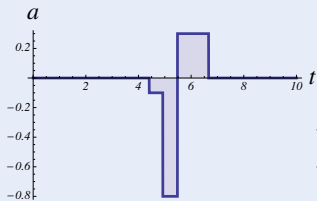
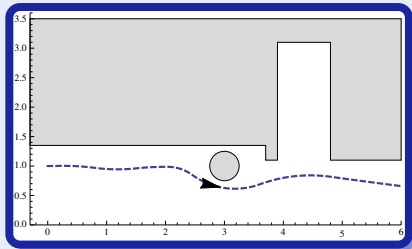
- Discrete dynamics (control decisions)
- Continuous dynamics (differential equations)



Challenge (Hybrid Systems)

Fixed rule describing state evolution with both

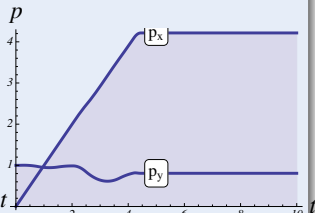
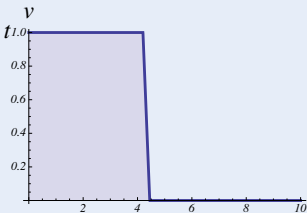
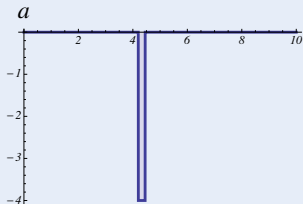
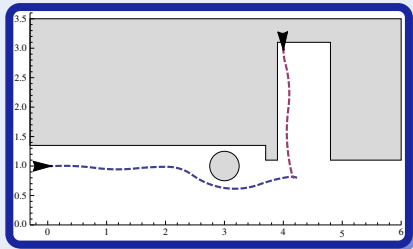
- Discrete dynamics (control decisions)
- Continuous dynamics (differential equations)



Challenge (Hybrid Systems)

Fixed rule describing state evolution with both

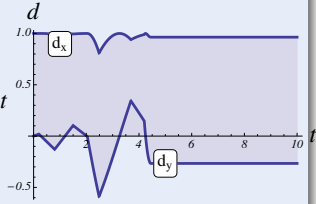
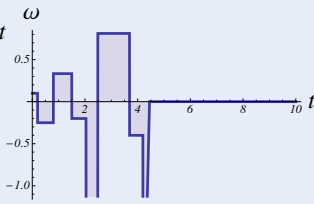
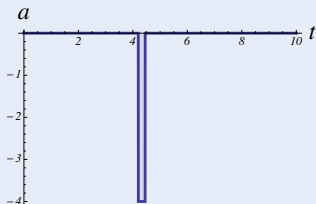
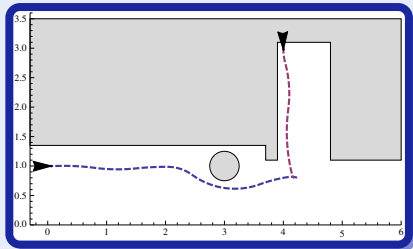
- Discrete dynamics (control decisions)
- Continuous dynamics (differential equations)



Challenge (Hybrid Systems)

Fixed rule describing state evolution with both

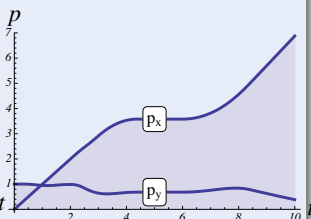
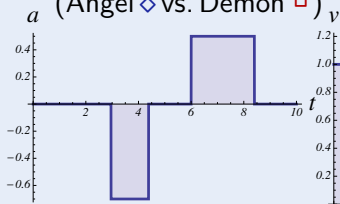
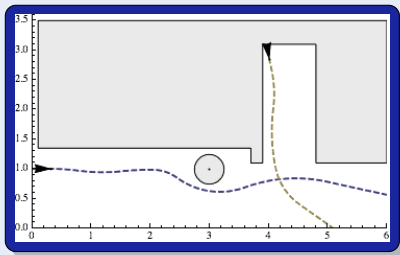
- Discrete dynamics (control decisions)
- Continuous dynamics (differential equations)



Challenge (Hybrid Games)

Game rules describing play choices with

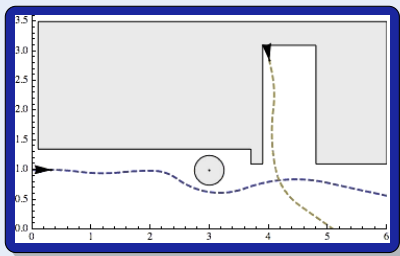
- Discrete dynamics (control decisions)
- Continuous dynamics (differential equations)
- Adversarial dynamics (Angel \diamond vs. Demon \square)



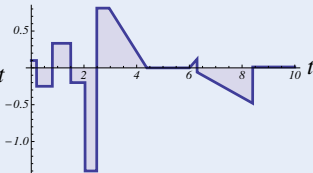
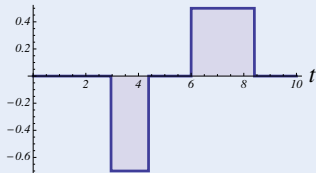
Challenge (Hybrid Games)

Game rules describing play choices with

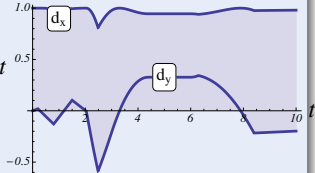
- Discrete dynamics (control decisions)
- Continuous dynamics (differential equations)
- Adversarial dynamics (Angel \diamond vs. Demon \square)



a (Angel \diamond vs. Demon \square) ω



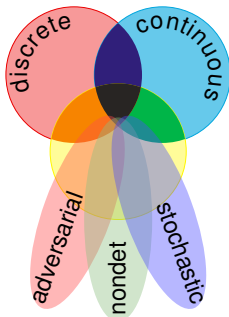
d



CPSs are Multi-Dynamical Systems

hybrid systems

HS = discrete + ODE

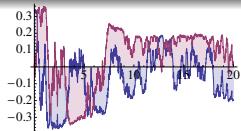


hybrid games

HG = HS + adversary

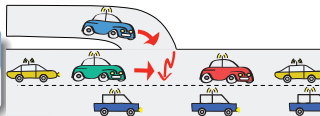
stochastic hybrid sys.

SHS = HS + stochastic



distributed hybrid sys.

DHS = HS + distributed

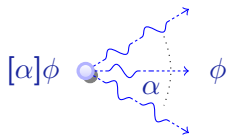




Dynamic Logics for Dynamical Systems

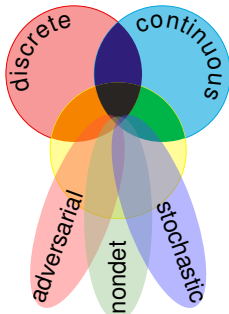
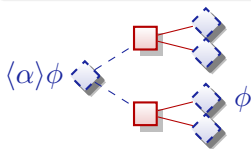
differential dynamic logic

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



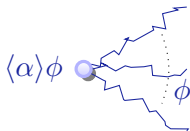
differential game logic

$$dGL = GL + HG$$



stochastic differential DL

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



quantified differential DL

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



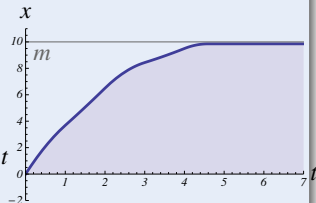
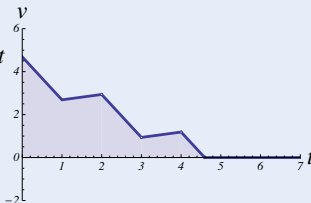
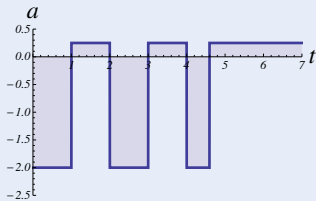
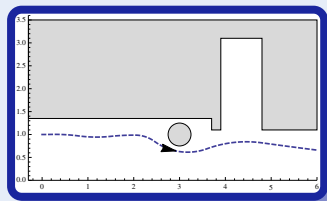
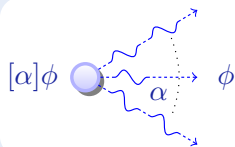
- 1 CPS are Multi-Dynamical Systems
 - Hybrid Systems
 - Hybrid Games
- 2 Dynamic Logic of Dynamical Systems
 - Syntax
 - Semantics
 - Example: Car Control Design
- 3 Proofs for CPS
 - Compositional Proof Calculus
 - Example: Safe Car Control
- 4 Theory of CPS
 - Soundness and Completeness
 - Differential Invariants
 - Example: Elementary Differential Invariants
 - Differential Axioms
- 5 Applications
- 6 Summary



- 1 CPS are Multi-Dynamical Systems
 - Hybrid Systems
 - Hybrid Games
- 2 Dynamic Logic of Dynamical Systems
 - Syntax
 - Semantics
 - Example: Car Control Design
- 3 Proofs for CPS
 - Compositional Proof Calculus
 - Example: Safe Car Control
- 4 Theory of CPS
 - Soundness and Completeness
 - Differential Invariants
 - Example: Elementary Differential Invariants
 - Differential Axioms
- 5 Applications
- 6 Summary

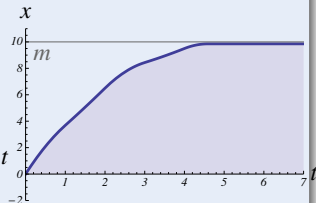
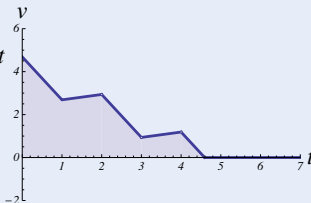
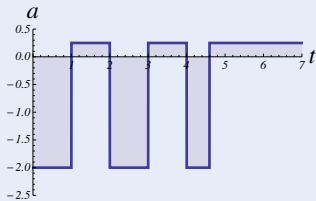
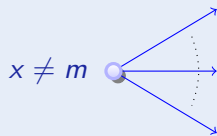
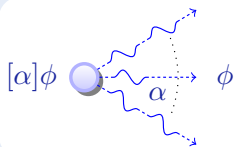
Concept (Differential Dynamic Logic)

(JAR'08, LICS'12)



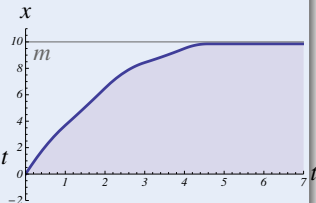
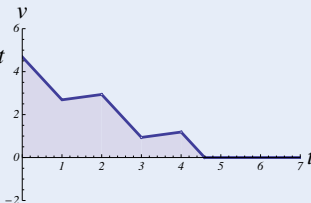
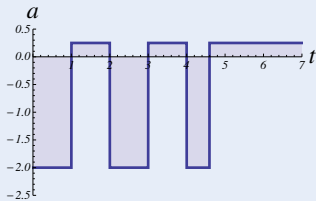
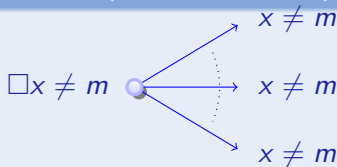
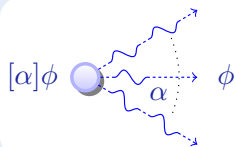
Concept (Differential Dynamic Logic)

(JAR'08, LICS'12)



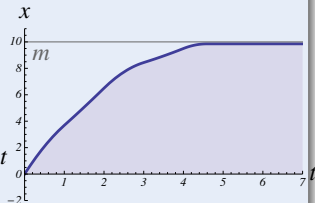
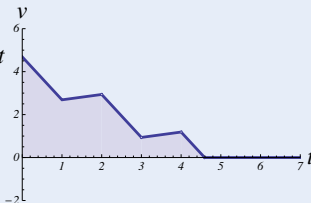
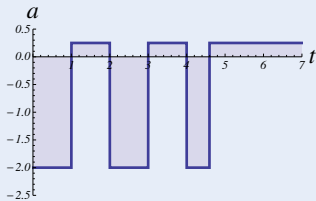
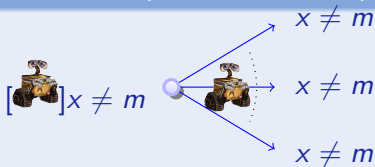
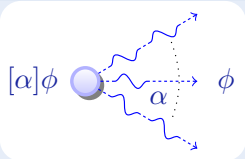
Concept (Differential Dynamic Logic)

(JAR'08, LICS'12)



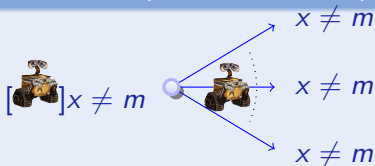
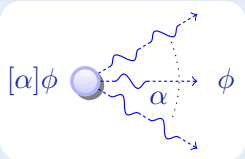
Concept (Differential Dynamic Logic)

(JAR'08, LICS'12)



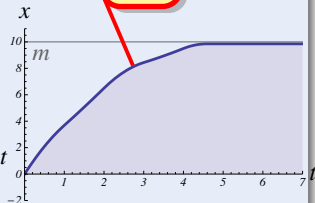
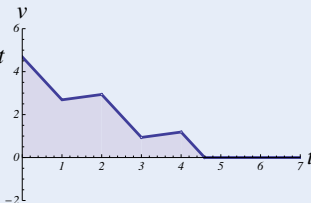
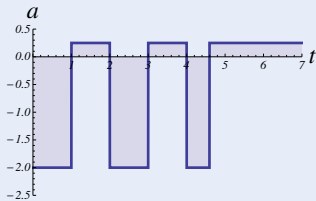
Concept (Differential Dynamic Logic)

(JAR'08, LICS'12)



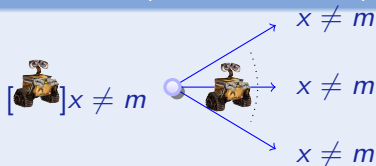
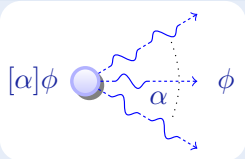
$$x' = v, v' = a$$

ODE



Concept (Differential Dynamic Logic)

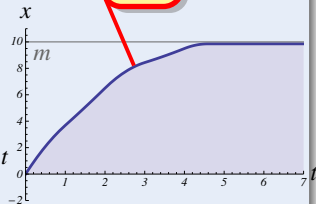
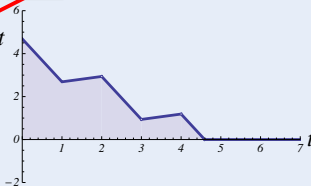
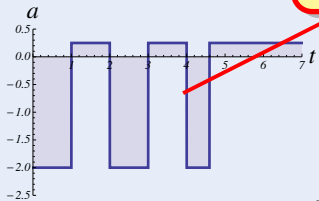
(JAR'08, LICS'12)



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

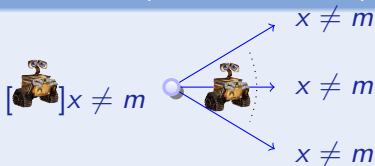
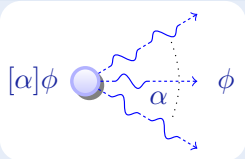
assign

ODE



Concept (Differential Dynamic Logic)

(JAR'08, LICS'12)

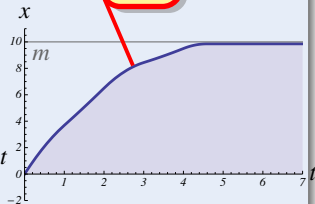
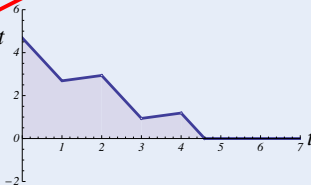
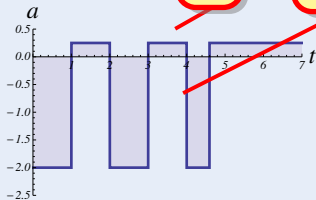


$$(\text{if}(\text{SB}(x, m)) a := -b) \quad x' = v, v' = a$$

test

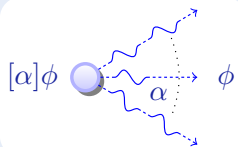
assign

ODE



Concept (Differential Dynamic Logic)

(JAR'08, LICS'12)



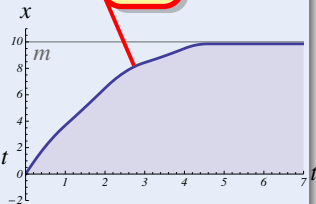
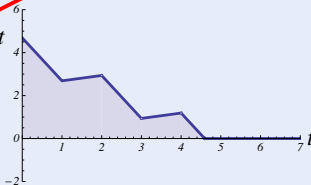
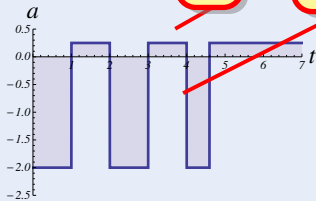
seq.
compose

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

test

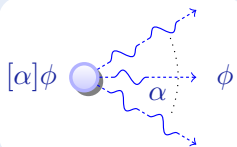
assign

ODE



Concept (Differential Dynamic Logic)

(JAR'08, LICS'12)



seq.
compose

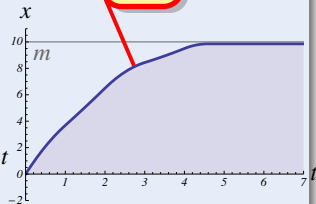
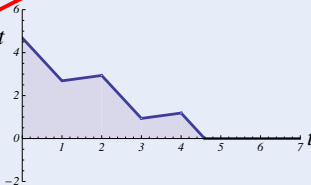
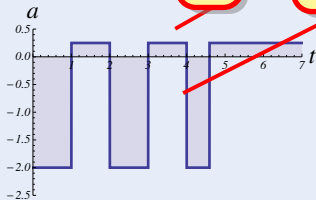
nondet.
repeat

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

test

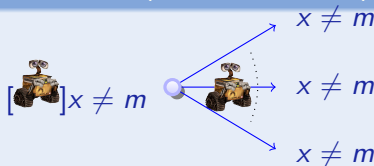
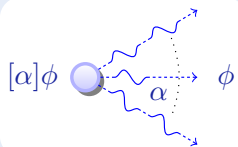
assign

ODE



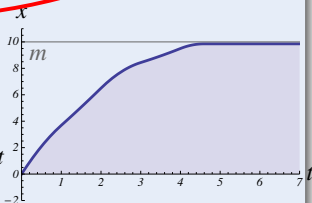
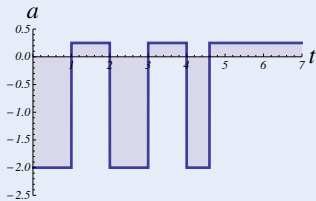
Concept (Differential Dynamic Logic)

(JAR'08, LICS'12)



$$\left[\left(\text{if}(\text{SB}(x, m)) \ a := -b \ ; \ x' = v, v' = a \right)^* \right] x \neq m$$

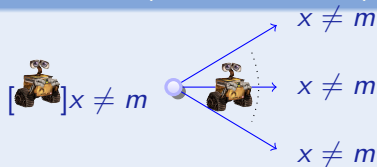
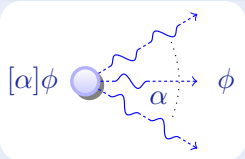
post



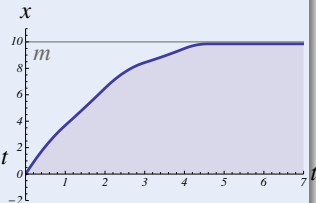
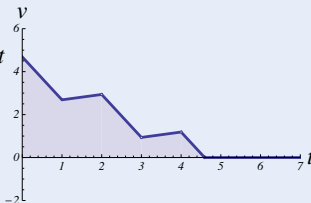
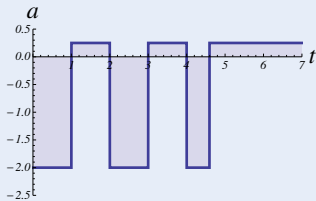
all runs

Concept (Differential Dynamic Logic)

(JAR'08, LICS'12)

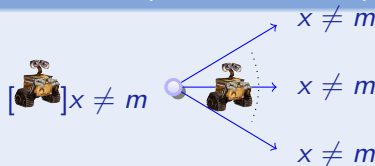
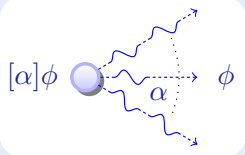


$$\underbrace{x \neq m \wedge b > 0}_{\text{init}} \rightarrow \left[\left(\text{if}(\text{SB}(x, m)) \ a := -b \ ; \ x' = v, v' = a \right)^* \right] \underbrace{x \neq m}_{\text{post}}$$



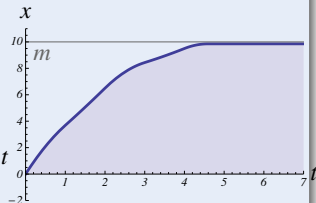
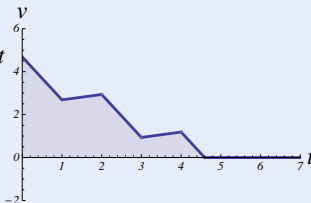
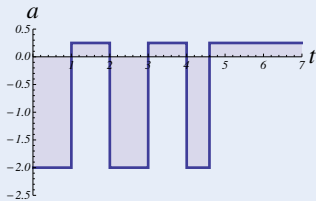
Concept (Differential Dynamic Logic)

(JAR'08, LICS'12)



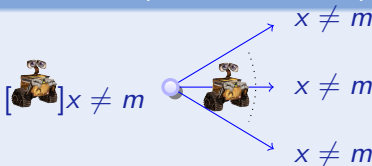
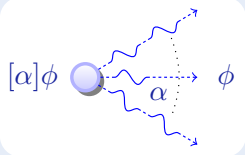
nondet.
choice

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



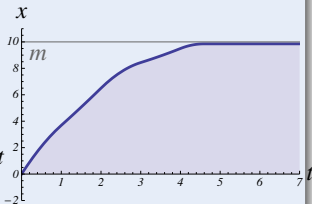
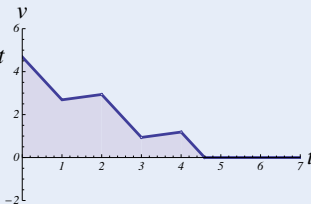
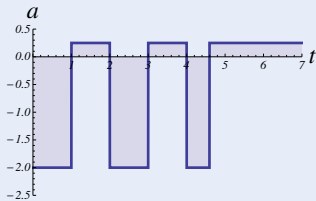
Concept (Differential Dynamic Logic)

(JAR'08, LICS'12)

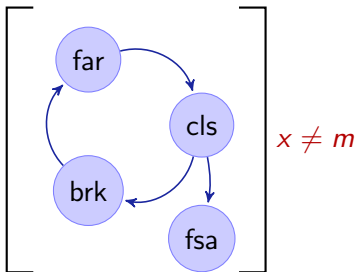


test nondet. choice

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



Want: Compositional verification



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

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

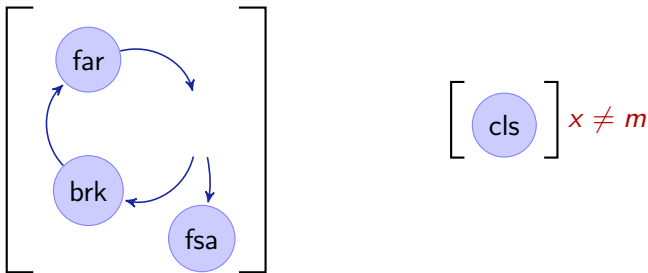
$$\text{cls} \equiv x' = v, v' = \dots \& \dots$$

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



Hybrid Programs vs. Hybrid Automata

Want: Compositional verification



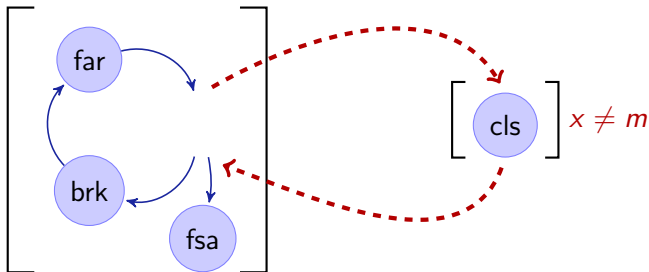
$$\text{far} \equiv x' = v, v' = A \& \neg \text{SB}(x, m)$$

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

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

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

Want: Compositional verification



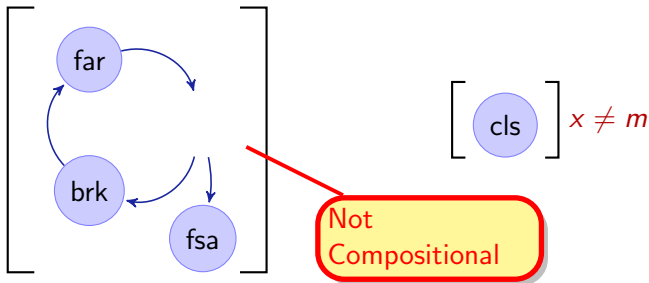
$$\text{far} \equiv x' = v, v' = A \& \neg \text{SB}(x, m)$$

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

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

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

Want: Compositional verification



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

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

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

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



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

Discrete Assign

Test Condition

Differential Equation

Nondet. Choice

Seq. Compose

Nondet. Repeat

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

Definition (Hybrid program semantics)

($\llbracket \cdot \rrbracket : \text{HP} \rightarrow \wp(\mathcal{S} \times \mathcal{S})$)

$$\llbracket x := f(x) \rrbracket = \{(v, w) : w = v \text{ except } \llbracket x \rrbracket w = \llbracket f(x) \rrbracket v\}$$

$$\llbracket ?Q \rrbracket = \{(v, v) : v \in \llbracket Q \rrbracket\}$$

$$\llbracket x' = f(x) \rrbracket = \{(\varphi(0), \varphi(r)) : \varphi \models x' = f(x) \text{ for some duration } r\}$$

$$\llbracket a \cup b \rrbracket = \llbracket a \rrbracket \cup \llbracket b \rrbracket$$

$$\llbracket a; b \rrbracket = \llbracket a \rrbracket \circ \llbracket b \rrbracket$$

$$\llbracket a^* \rrbracket = \bigcup_{n \in \mathbb{N}} \llbracket a^n \rrbracket$$

Definition (dL semantics)

($\llbracket \cdot \rrbracket : \text{Fml} \rightarrow \wp(\mathcal{S})$)

$$\llbracket e_1 \geq e_2 \rrbracket = \{v : \llbracket e_1 \rrbracket v \geq \llbracket e_2 \rrbracket v\}$$

$$\llbracket \neg P \rrbracket = (\llbracket P \rrbracket)^c$$

$$\llbracket P \wedge Q \rrbracket = \llbracket P \rrbracket \cap \llbracket Q \rrbracket$$

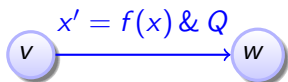
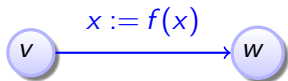
$$\llbracket \langle a \rangle P \rrbracket = \llbracket a \rrbracket \circ \llbracket P \rrbracket = \{v : w \in \llbracket P \rrbracket \text{ for some } w (v, w) \in \llbracket a \rrbracket\}$$

$$\llbracket [a] P \rrbracket = \llbracket \neg \langle a \rangle \neg P \rrbracket = \{v : w \in \llbracket P \rrbracket \text{ for all } w (v, w) \in \llbracket a \rrbracket\}$$

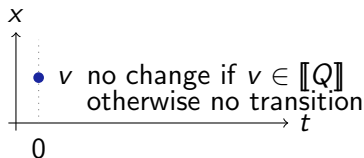
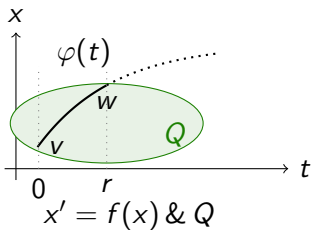
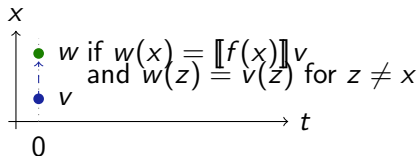
$$\llbracket \exists x P \rrbracket = \{v : v_x^r \in \llbracket P \rrbracket \text{ for some } r \in \mathbb{R}\}$$



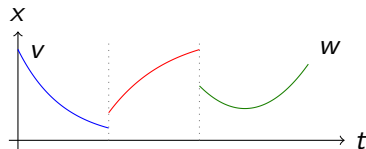
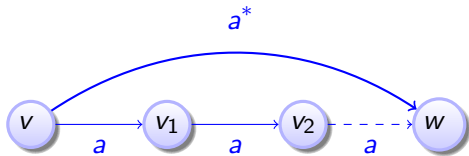
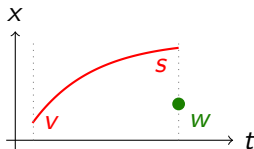
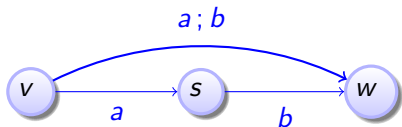
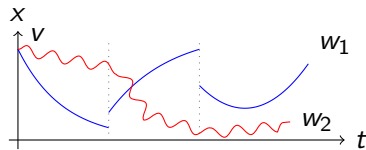
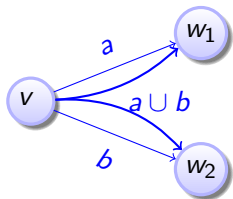
Differential Dynamic Logic dL: Transition Semantics

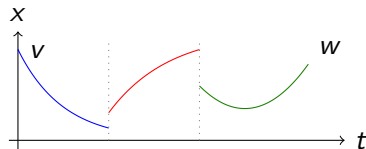
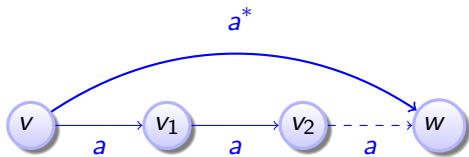
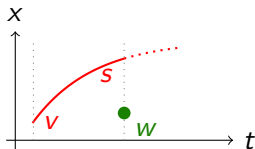
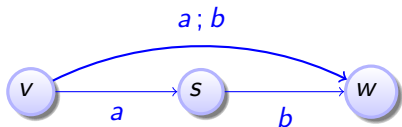
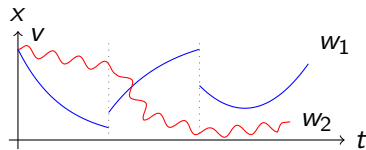
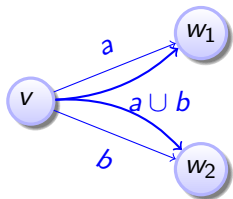


if $v \in \llbracket Q \rrbracket$

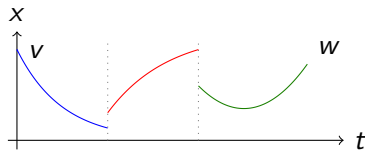
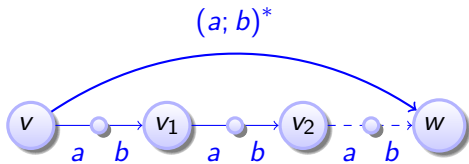
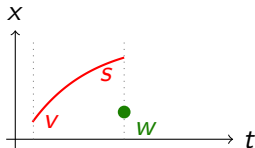
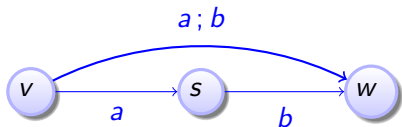
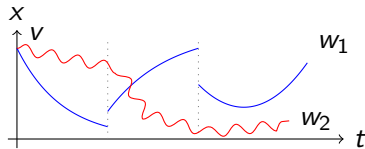
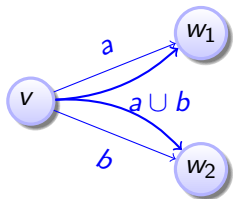


\mathcal{A} Differential Dynamic Logic $d\mathcal{L}$: Transition Semantics

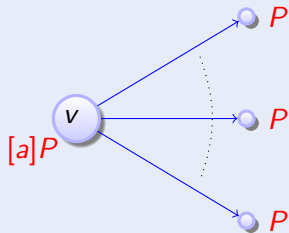




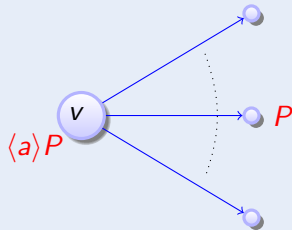
\mathcal{A} Differential Dynamic Logic $d\mathcal{L}$: Transition Semantics



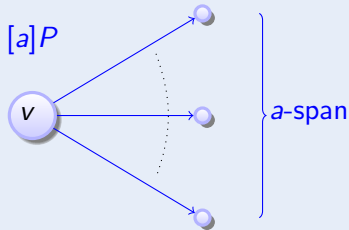
Definition ($d\mathcal{L}$ Formulas)



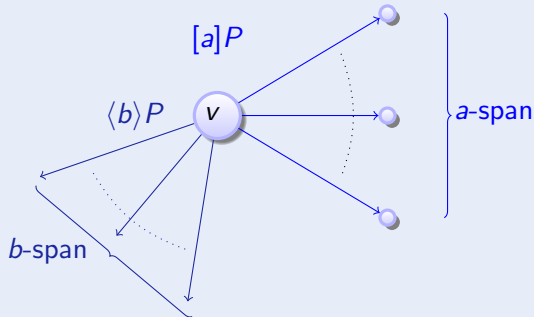
Definition ($d\mathcal{L}$ Formulas)



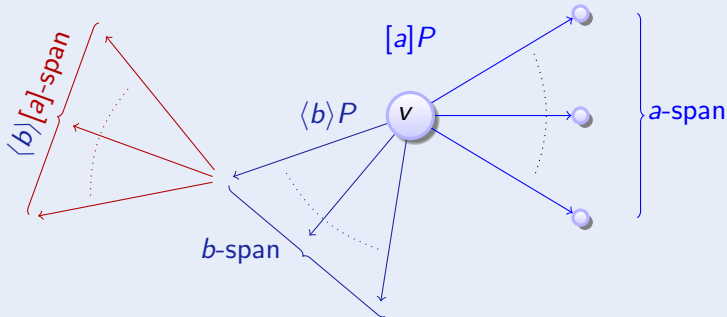
Definition ($d\mathcal{L}$ Formulas)



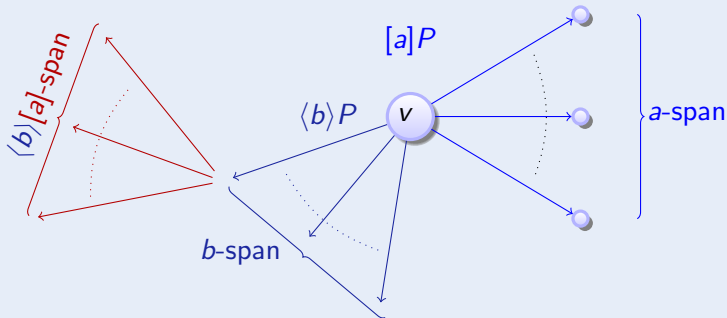
Definition ($d\mathcal{L}$ Formulas)



Definition ($d\mathcal{L}$ Formulas)



Definition ($d\mathcal{L}$ Formulas)



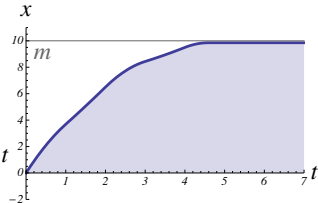
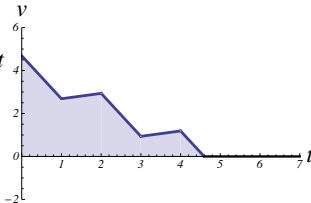
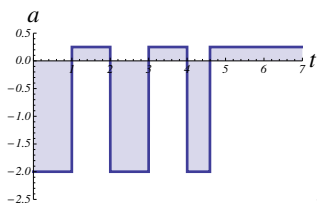
compositional semantics \Rightarrow compositional proofs!

Accelerate condition $?H$



Example (Single car car_s)

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



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

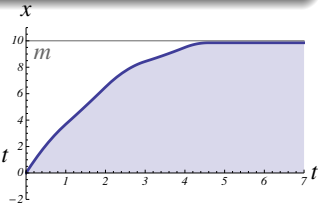
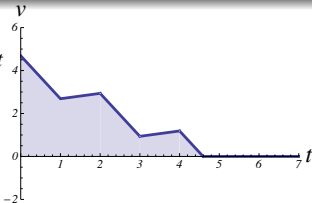
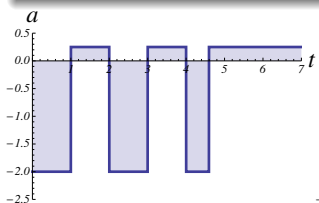


Example (Single car car_ε time-triggered)

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

Example (▶ Safely stays before traffic light m)

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



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

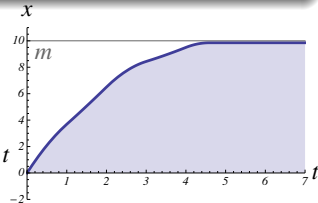
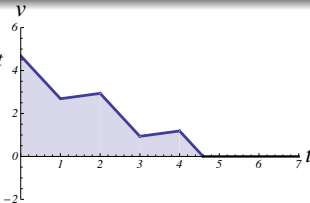
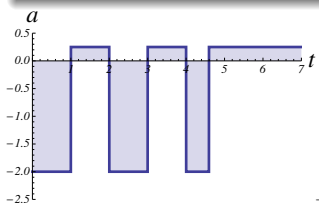


Example (Single car car_ε time-triggered)

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

Example (▶ Live, can move everywhere)

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





- 1 CPS are Multi-Dynamical Systems
 - Hybrid Systems
 - Hybrid Games
- 2 Dynamic Logic of Dynamical Systems
 - Syntax
 - Semantics
 - Example: Car Control Design
- 3 **Proofs for CPS**
 - **Compositional Proof Calculus**
 - **Example: Safe Car Control**
- 4 Theory of CPS
 - Soundness and Completeness
 - Differential Invariants
 - Example: Elementary Differential Invariants
 - Differential Axioms
- 5 Applications
- 6 Summary

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

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

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

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

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

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

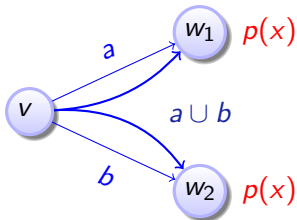
$$I \quad [a^*](p(x) \rightarrow [a]p(x)) \rightarrow (p(x) \rightarrow [a^*]p(x))$$

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

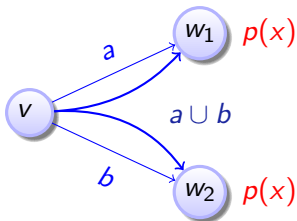
$$DS \quad [x' = f]p(x) \leftrightarrow \forall t \geq 0 [x := x + ft]p(x)$$

compositional semantics \Rightarrow compositional rules!

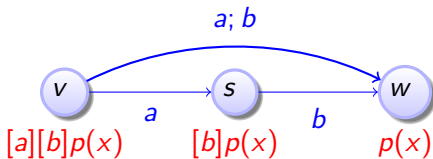
$$\frac{[a]p(x) \wedge [b]p(x)}{[a \cup b]p(x)}$$



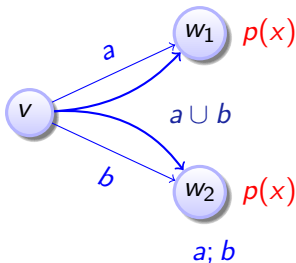
$$\frac{[a]p(x) \wedge [b]p(x)}{[a \cup b]p(x)}$$



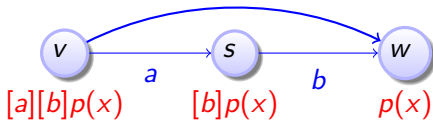
$$\frac{[a][b]p(x)}{[a; b]p(x)}$$



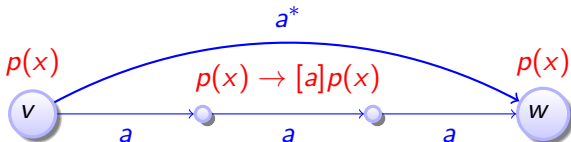
$$\frac{[a]p(x) \wedge [b]p(x)}{[a \cup b]p(x)}$$



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



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



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



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

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



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

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



$$\begin{array}{l} \frac{[1] \quad J(x, v) \rightarrow [x' = v, v' = -b] J(x, v)}{[:=] \quad J(x, v) \rightarrow [a := -b][x' = v, v' = a] J(x, v)} \\ [;] \quad J(x, v) \rightarrow [a := -b; (x' = v, v' = a)] J(x, v) \end{array}$$

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



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

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



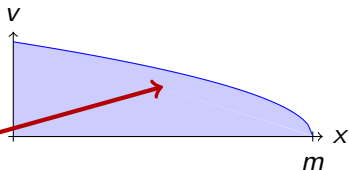
$$\begin{array}{l} \text{QE} \frac{J(x, v) \rightarrow \forall t \geq 0 (-\frac{b}{2}t^2 + vt + x \leq m)}{[\text{:=}] \frac{J(x, v) \rightarrow \forall t \geq 0 [x := -\frac{b}{2}t^2 + vt + x] J(x, v)}{[\text{'}] \frac{J(x, v) \rightarrow [x' = v, v' = -b] J(x, v)}{[\text{:=}] \frac{J(x, v) \rightarrow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

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



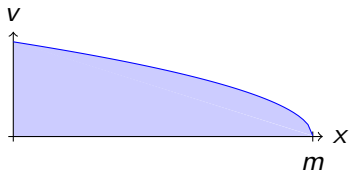
$$\begin{array}{l}
 J(x, v) \rightarrow v^2 \leq 2b(m - x) \\
 \text{QE} \frac{J(x, v) \rightarrow \forall t \geq 0 (-\frac{b}{2}t^2 + vt + x \leq m)}{J(x, v) \rightarrow \forall t \geq 0 [x := -\frac{b}{2}t^2 + vt + x]J(x, v)} \\
 \text{[:=]} \frac{J(x, v) \rightarrow \forall t \geq 0 [x := -\frac{b}{2}t^2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

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



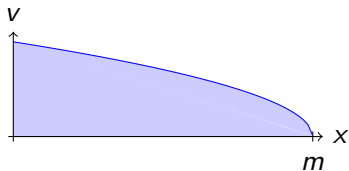
$$\begin{array}{l}
 J(x, v) \rightarrow v^2 \leq 2b(m - x) \\
 \hline
 \text{QE } J(x, v) \rightarrow \forall t \geq 0 \left(-\frac{b}{2}t^2 + vt + x \leq m \right) \\
 \hline
 [:=] J(x, v) \rightarrow \forall t \geq 0 [x := -\frac{b}{2}t^2 + vt + x] J(x, v) \\
 \hline
 ['] J(x, v) \rightarrow [x' =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

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



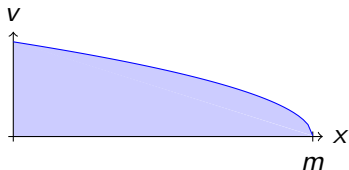
$$[i] \frac{}{J(x, v) \rightarrow [?\neg SB; a := A; (x' = v, v' = a, t' = 1 \ \& \ t \leq \epsilon)] J(x, v)}$$

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



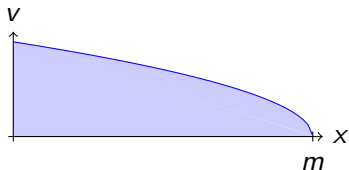
$$\frac{[?] \overline{J(x, v) \rightarrow [?\neg\text{SB}][a := A; (x' = v, v' = a, t' = 1 \& t \leq \varepsilon)]J(x, v)}}{[i] \overline{J(x, v) \rightarrow [?\neg\text{SB}; a := A; (x' = v, v' = a, t' = 1 \& t \leq \varepsilon)]J(x, v)}}$$

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



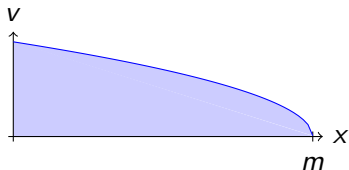
- $$\begin{array}{l} \text{[i]} \frac{J(x, v) \rightarrow \neg \text{SB} \rightarrow [a := A; (x' = v, v' = a, t' = 1 \& t \leq \varepsilon)] J(x, v)}{J(x, v) \rightarrow [\text{?}\neg \text{SB}][a := A; (x' = v, v' = a, t' = 1 \& t \leq \varepsilon)] J(x, v)} \\ \text{[?]} \frac{J(x, v) \rightarrow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

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



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

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

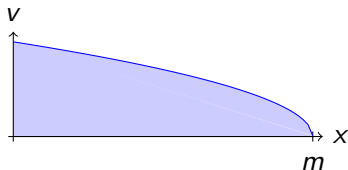


$$\frac{[?] \quad J(x, v) \rightarrow \neg \text{SB} \rightarrow [x' = v, v' = A, t' = 1 \ \& \ t \leq \varepsilon] J(x, v)}{[? =] \quad J(x, v) \rightarrow \neg \text{SB} \rightarrow [a := A][x' = v, v' = a, t' = 1 \ \& \ t \leq \varepsilon] J(x, v)}$$

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

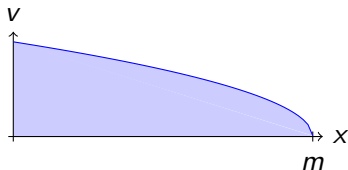
$$\frac{[?] \quad J(x, v) \rightarrow [? \neg \text{SB}; a := A; (x' = v, v' = a, t' = 1 \ \& \ t \leq \varepsilon)] J(x, v)}{[?] \quad J(x, v) \rightarrow [? \neg \text{SB}; a := A; (x' = v, v' = a, t' = 1 \ \& \ t \leq \varepsilon)] J(x, v)}$$

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



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

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



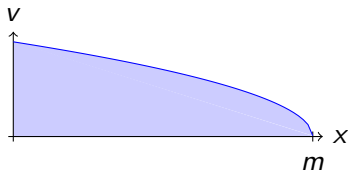
$$\frac{J(x, v) \rightarrow \neg \text{SB} \rightarrow \forall t \geq 0 (t \leq \varepsilon \rightarrow J(\frac{A}{2}t^2 + vt + x, At + v))}{\begin{array}{l} \text{[:=]} \\ \text{[?]} \end{array}} J(x, v) \rightarrow \neg \text{SB} \rightarrow \forall t \geq 0 (t \leq \varepsilon \rightarrow [x := \frac{A}{2}t^2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

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

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

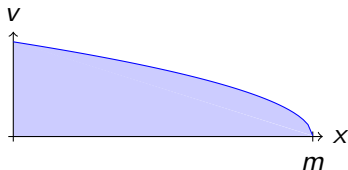
$$\text{[?]} J(x, v) \rightarrow [\text{?} \neg \text{SB}; a := A; (x' = v, v' = a, t' = 1 \ \& \ t \leq \varepsilon)] J(x, v)$$

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



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

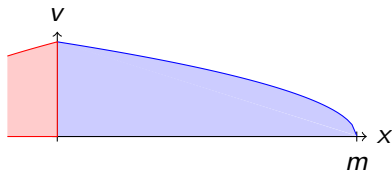
$$J(x, v) \equiv v^2 \leq 2b(m - x)$$



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

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

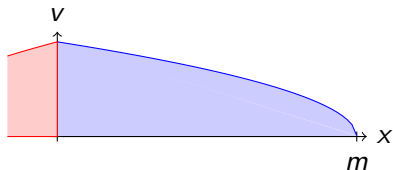
$$\text{SB} \equiv 2b(m - x) < v^2 + (A + b)(A\varepsilon^2 + 2\varepsilon v)$$



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

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

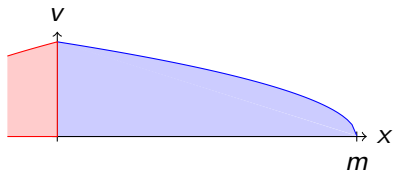
$$SB \equiv 2b(m - x) < v^2 + (A + b)(A\varepsilon^2 + 2\varepsilon v)$$



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

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

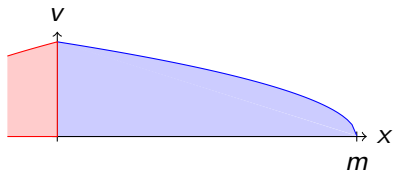
$$SB \equiv 2b(m - x) < v^2 + (A + b)(A\varepsilon^2 + 2\varepsilon v)$$



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

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

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

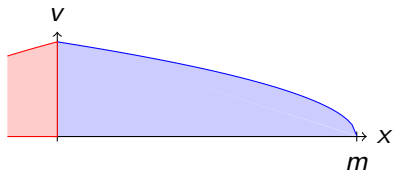


$$\frac{[U] J(x, v) \rightarrow [a := -b \cup ?\neg SB; a := A][x'' = a, t' = 1 \ \& \ t \leq \varepsilon] J(x, v)}{[i] J(x, v) \rightarrow [(a := -b \cup ?\neg SB; a := A); x'' = a, t' = 1 \ \& \ t \leq \varepsilon] J(x, v)}$$

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

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

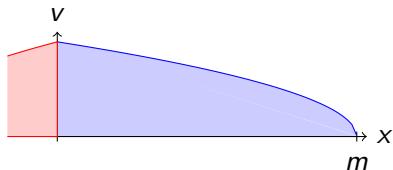
$$SB \equiv 2b(m - x) < v^2 + (A + b)(A\varepsilon^2 + 2\varepsilon v)$$



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

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

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



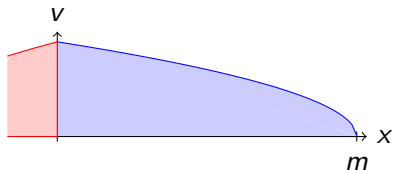
previous proofs for braking and acceleration

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

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

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

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



previous proofs for braking and acceleration

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

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

- 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



- 1 CPS are Multi-Dynamical Systems
 - Hybrid Systems
 - Hybrid Games
- 2 Dynamic Logic of Dynamical Systems
 - Syntax
 - Semantics
 - Example: Car Control Design
- 3 Proofs for CPS
 - Compositional Proof Calculus
 - Example: Safe Car Control
- 4 Theory of CPS
 - Soundness and Completeness
 - Differential Invariants
 - Example: Elementary Differential Invariants
 - Differential Axioms
- 5 Applications
- 6 Summary



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



Complete Proof Theory of Hybrid Systems

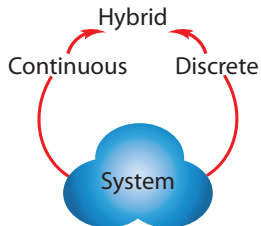
Theorem (Sound & Complete) (J.Autom.Reas. 2008, LICS'12)

*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





Complete Proof Theory of Hybrid Systems

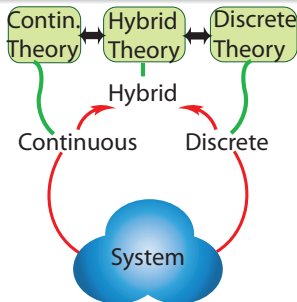
Theorem (Sound & Complete) (J.Autom.Reas. 2008, LICS'12)

*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

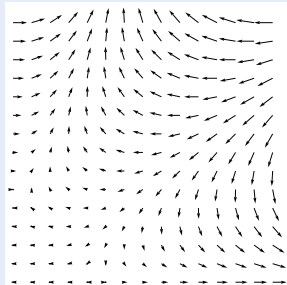


JAutomReas'08,LICS'12

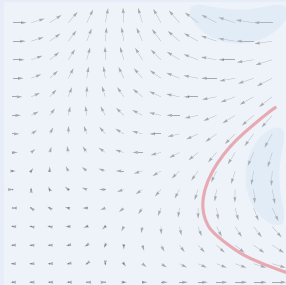


Differential Invariants for Differential Equations

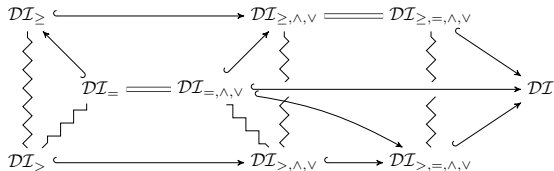
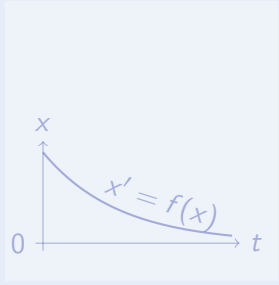
Differential Invariant



Differential Cut



Differential Ghost



Logic

Provability
theory

Math

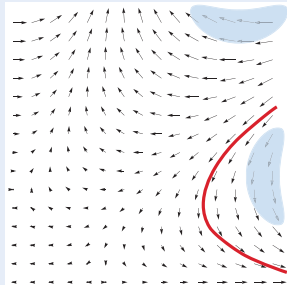
Character-
istic PDE

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

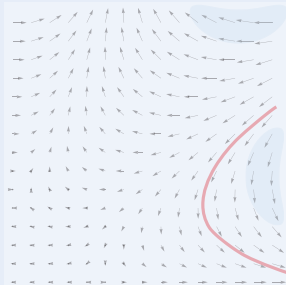


Differential Invariants for Differential Equations

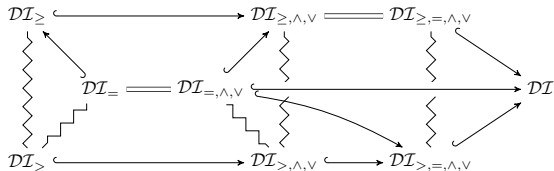
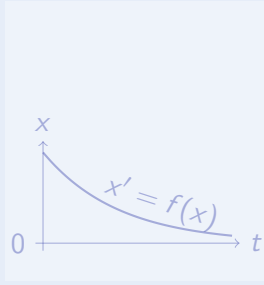
Differential Invariant



Differential Cut



Differential Ghost



Logic

Provability
theory

Math

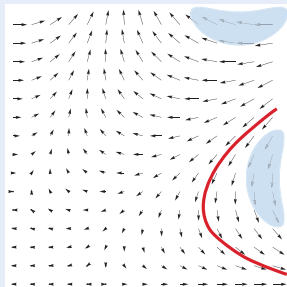
Character-
istic PDE

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

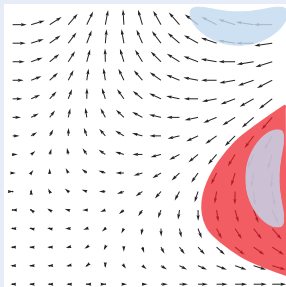


Differential Invariants for Differential Equations

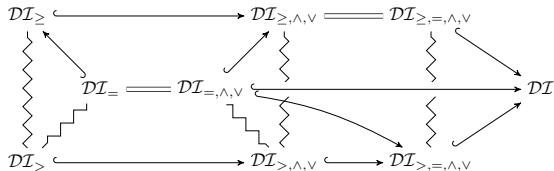
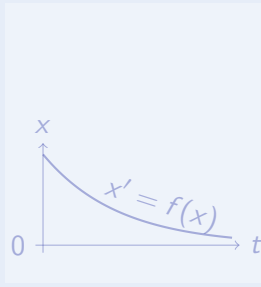
Differential Invariant



Differential Cut



Differential Ghost



Logic

Provability
theory

Math

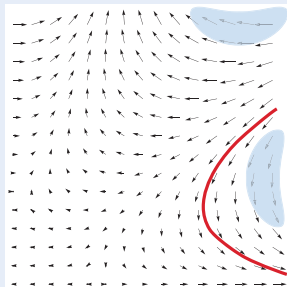
Character-
istic PDE

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

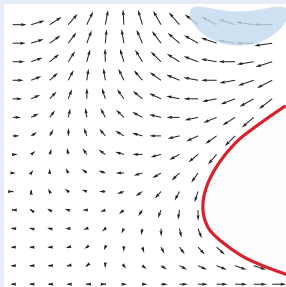


Differential Invariants for Differential Equations

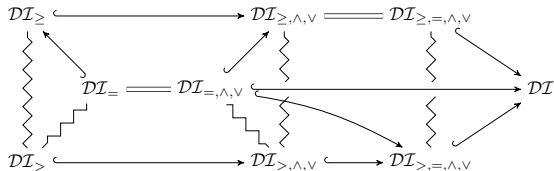
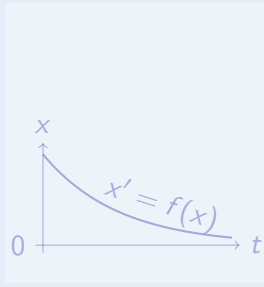
Differential Invariant



Differential Cut



Differential Ghost



Logic

Provability
theory

Math

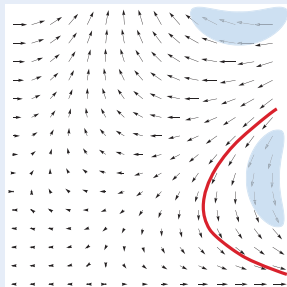
Character-
istic PDE

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

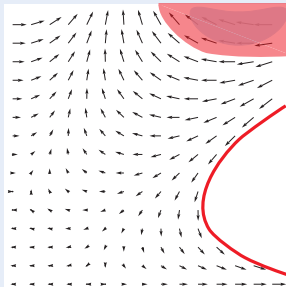


Differential Invariants for Differential Equations

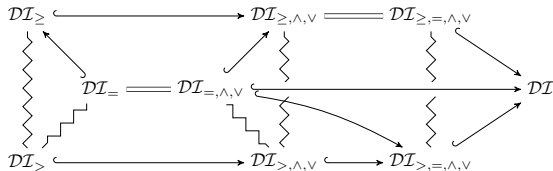
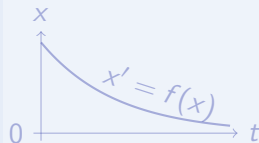
Differential Invariant



Differential Cut



Differential Ghost



Logic

Provability
theory

Math

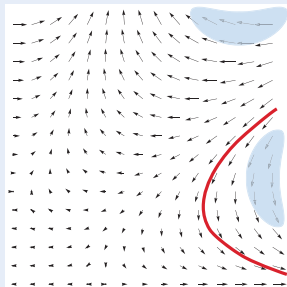
Character-
istic PDE

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

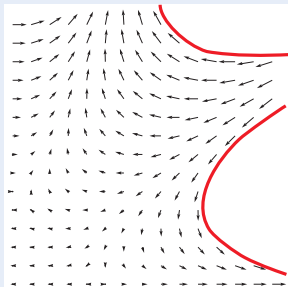


Differential Invariants for Differential Equations

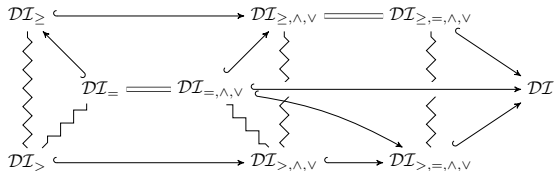
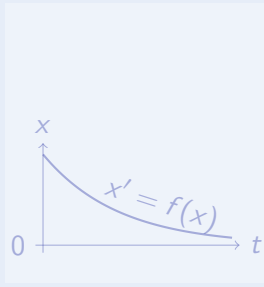
Differential Invariant



Differential Cut



Differential Ghost



Logic

Provability
theory

Math

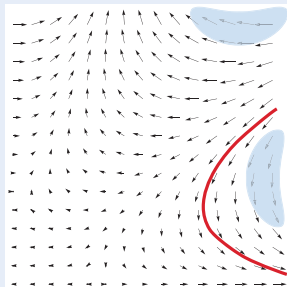
Character-
istic PDE

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

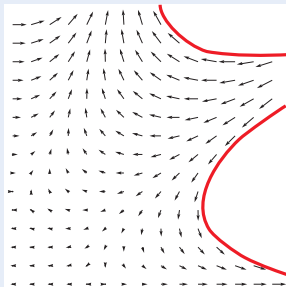


Differential Invariants for Differential Equations

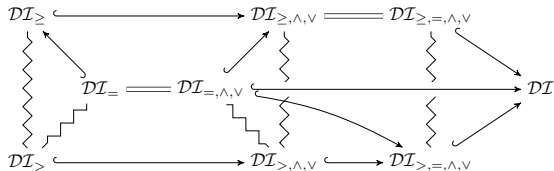
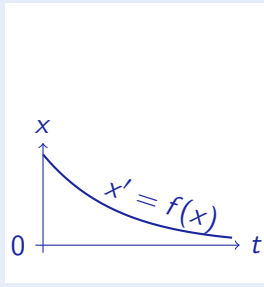
Differential Invariant



Differential Cut



Differential Ghost



Logic

Provability
theory

Math

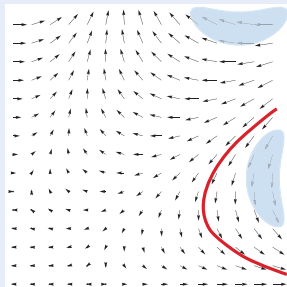
Character-
istic PDE

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

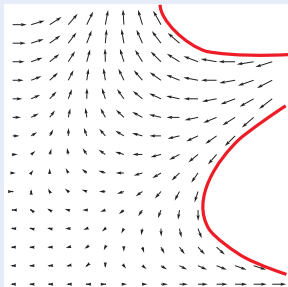


Differential Invariants for Differential Equations

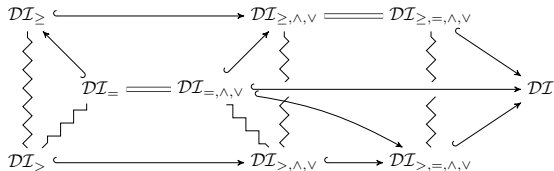
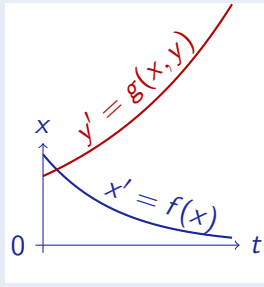
Differential Invariant



Differential Cut



Differential Ghost



Logic

Provability
theory

Math

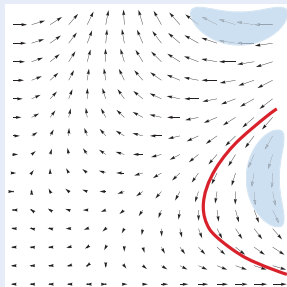
Character-
istic PDE

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

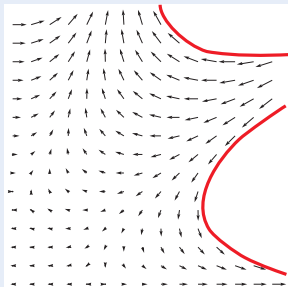


Differential Invariants for Differential Equations

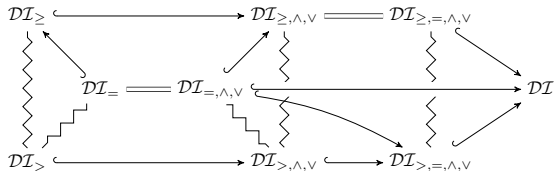
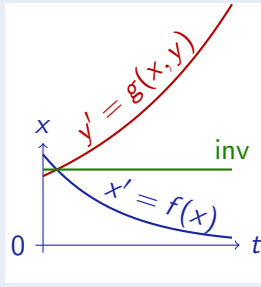
Differential Invariant



Differential Cut



Differential Ghost



Logic

Provability
theory

Math

Character-
istic PDE

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

Differential Invariant

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

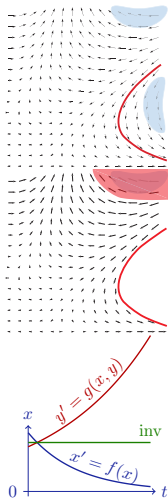
Differential Cut

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

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

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

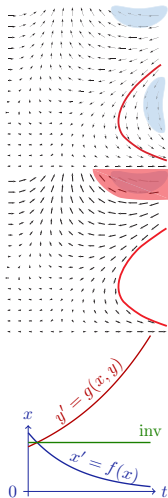
Differential Cut

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

Differential Ghost

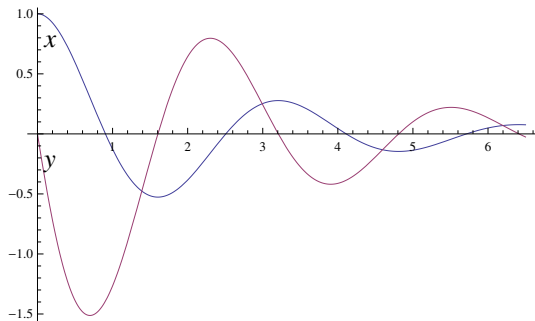
$$\frac{F \leftrightarrow \exists y G \quad G \rightarrow [x' = f(x), y' = g(x, y) \ \& \ H]G}{F \rightarrow [x' = f(x) \ \& \ H]F}$$

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





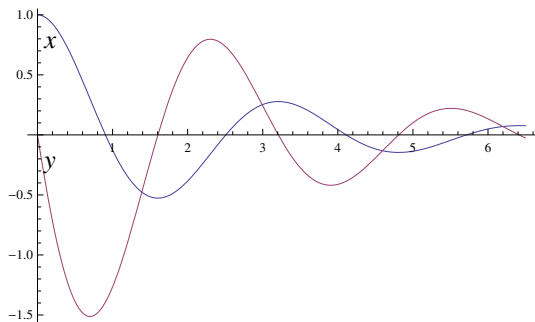
$$\omega^2 x^2 + y^2 \leq c^2 \rightarrow [x' = y, y' = -\omega^2 x - 2d\omega y \ \& \ (\omega \geq 0 \wedge d \geq 0)] \omega^2 x^2 + y^2 \leq c^2$$





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

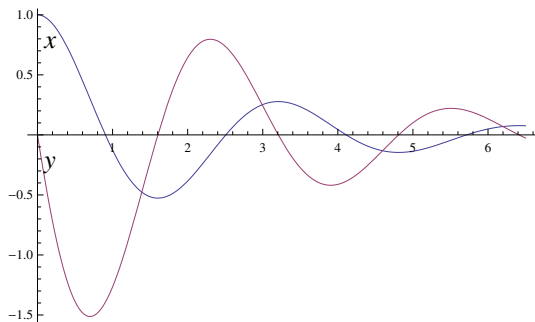
$$\omega^2 x^2 + y^2 \leq c^2 \rightarrow [x' = y, y' = -\omega^2 x - 2d\omega y \ \& \ (\omega \geq 0 \wedge d \geq 0)] \omega^2 x^2 + y^2 \leq c^2$$



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

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

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

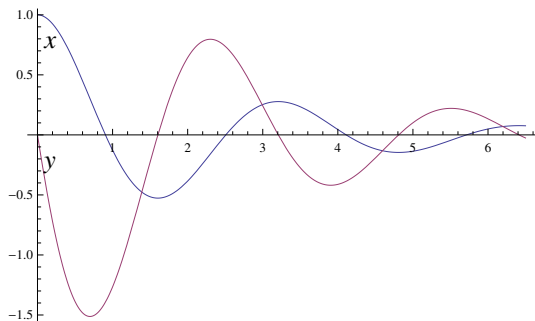


*

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

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

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

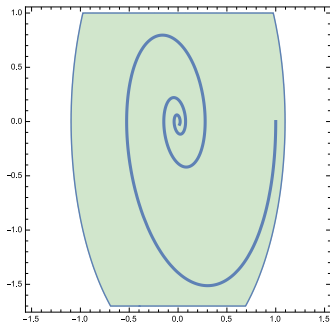
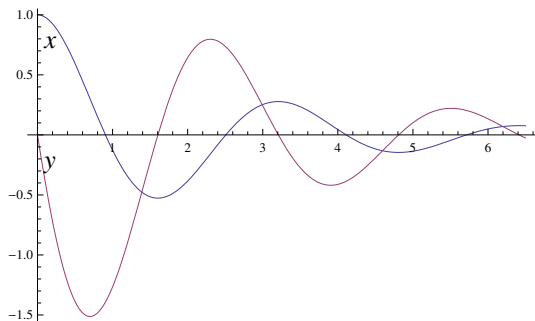


*

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

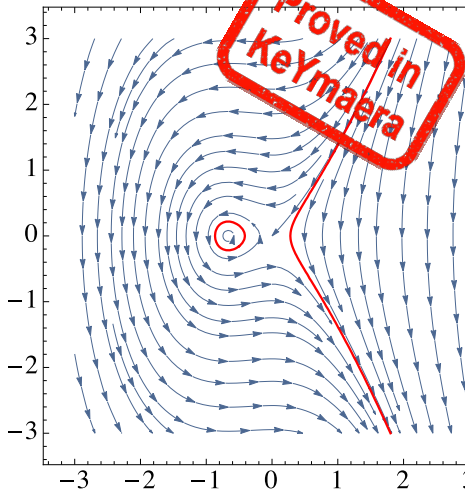
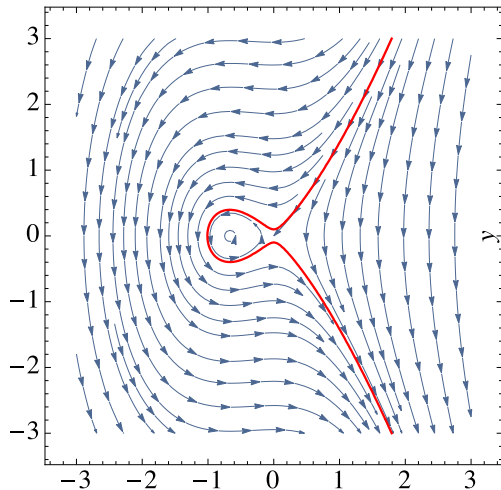
$$\omega \geq 0 \wedge d \geq 0 \rightarrow [x' := y][y' := -\omega^2 x - 2d\omega y] 2\omega^2 x x' + 2y y' \leq 0$$

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





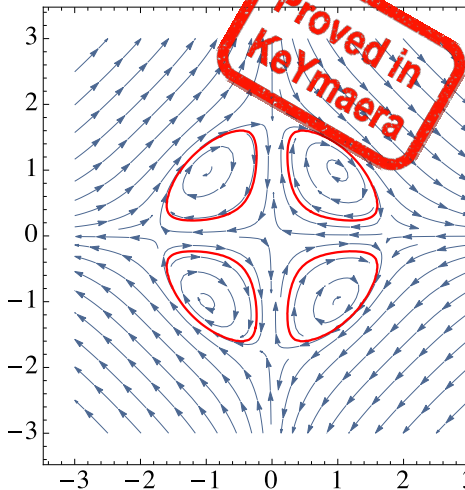
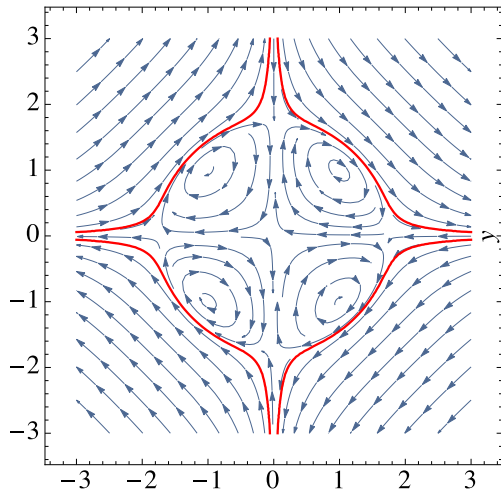
Differential Invariants for Differential Equations



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

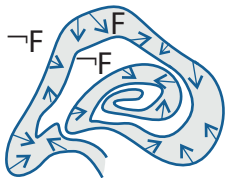


Differential Invariants for Differential Equations

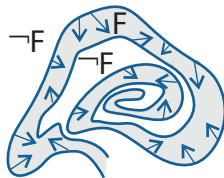


Proved in
KeYmaera

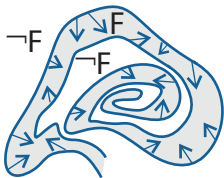
$$[x' = 2x^4y + 4x^2y^3 - 6x^2y, y' = -4x^3y^2 - 2xy^4 + 6xy^2] x^4y^2 + x^2y^4 - 3x^2y^2 \leq c$$



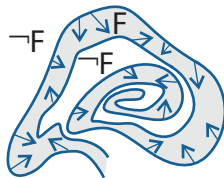
$$\frac{H \rightarrow [x' := f(x)]F'}{F \rightarrow [x' = f(x) \ \& \ H]F}$$



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



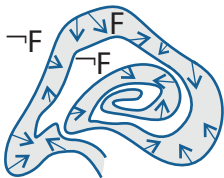
$$\frac{H \rightarrow [x' := f(x)]F'}{F \rightarrow [x' = f(x) \ \& \ H]F}$$



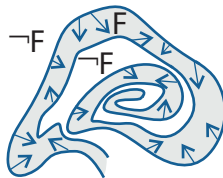
$$\frac{F \wedge H \rightarrow [x' := f(x)]F'}{F \rightarrow [x' = \theta \ \& \ H]F}$$

Example (Restrictions)

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



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

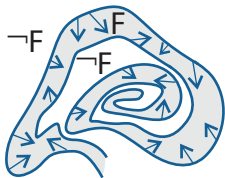


$$\frac{F \wedge H \rightarrow [x' := f(x)]F'}{F \rightarrow [x' = \theta \& H]F}$$

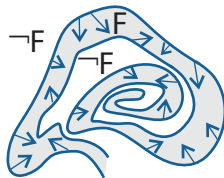
Example (Restrictions)

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

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



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



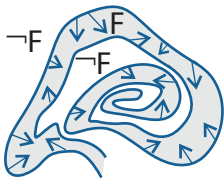
$$\frac{F \wedge H \rightarrow [x' := f(x)]F'}{F \rightarrow [x' = \theta \& H]F}$$

Example (Restrictions)

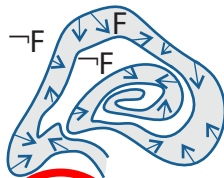
$$d^2 - 2d + 1 = 0 \rightarrow 2de - 2e = 0$$

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

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



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



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

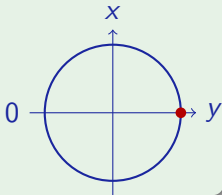
Example (Restrictions are unsound!)

(unsound)

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

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

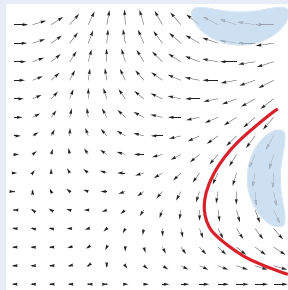
$$d^2 - 2d + 1 = 0 \rightarrow [d' = e, e' = -d]d^2 - 2d + 1 = 0$$



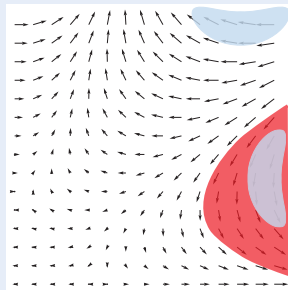


Differential Invariants for Differential Equations

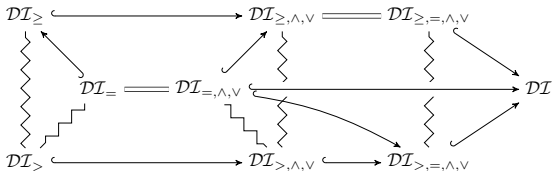
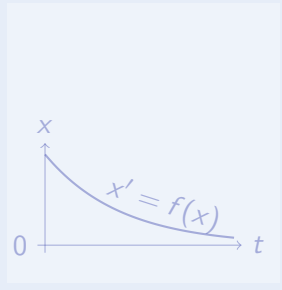
Differential Invariant



Differential Cut



Differential Ghost



Logic
Provability
theory

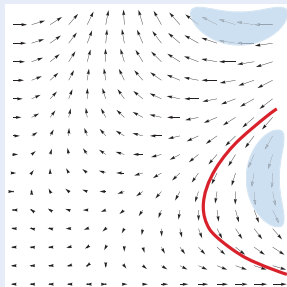
Math
Character-
istic PDE

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

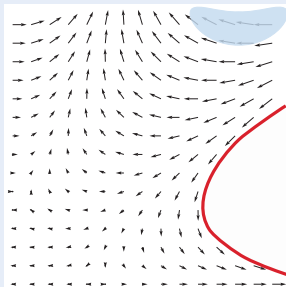


Differential Invariants for Differential Equations

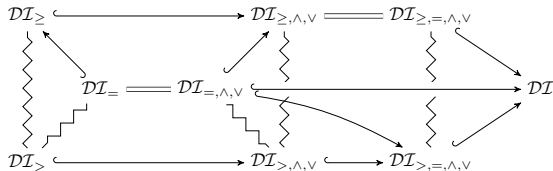
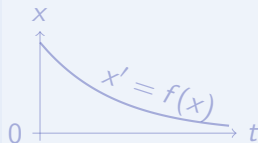
Differential Invariant



Differential Cut



Differential Ghost



Logic

Provability
theory

Math

Character-
istic PDE

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



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

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

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

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

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

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

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

$$\text{QE } 5y^4 y^2 \geq 0$$

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

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

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

*

$$\text{QE } 5y^4 y^2 \geq 0$$

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

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

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

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

*

$$\text{QE} \quad \frac{5y^4 y^2 \geq 0}{\text{DI}}$$

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

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

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

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

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

*

$$\text{QE} \quad 5y^4y^2 \geq 0$$

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

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

$$\text{QE} \quad y^5 \geq 0 \rightarrow 2x^2((x-2)^4 + y^5) \geq 0$$

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

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

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

*

$$\text{QE} \quad 5y^4y^2 \geq 0$$

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

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

*

$$\text{QE} \quad y^5 \geq 0 \rightarrow 2x^2((x-2)^4 + y^5) \geq 0$$

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

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

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

*

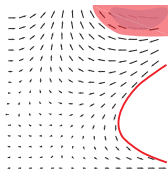
$$\text{QE} \quad 5y^4y^2 \geq 0$$

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

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

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)

$$\frac{A \rightarrow B \vee C \quad A \wedge C \rightarrow B}{A \rightarrow B} \quad \textit{cut can be eliminated}$$

Theorem (No Differential Cut Elimination)

(LMCS 2012)

Deductive power with differential cut exceeds deductive power without.

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

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

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

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

$$\text{DI } [x' = f(x) \ \& \ q(x)]p(x) \leftarrow (q(x) \rightarrow p(x) \wedge [x' = f(x) \ \& \ q(x)](p(x)))'$$

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

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

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

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

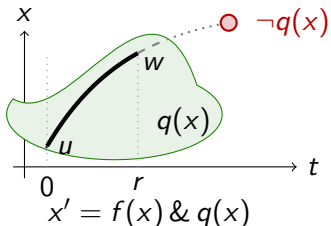
$$\cdot (f(\bar{x}) \cdot g(\bar{x}))' = (f(\bar{x}))' \cdot g(\bar{x}) + f(\bar{x}) \cdot (g(\bar{x}))'$$

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

Axiom (Differential Weakening)

(CADE'15)

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



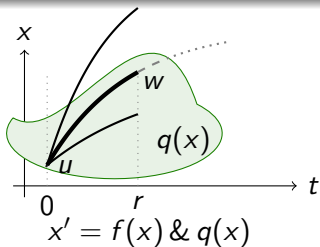
Differential equations cannot leave their evolution domains. Implies:

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

Axiom (Differential Cut)

(CADE'15)

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



DC is a cut for differential equations.

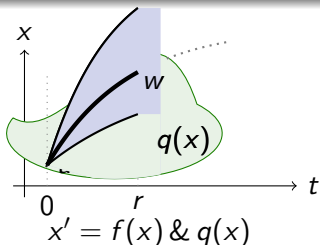
DC is a differential modal modus ponens K.

Can't leave $r(x)$, then might as well restrict state space to $r(x)$.

Axiom (Differential Cut)

(CADE'15)

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



DC is a cut for differential equations.

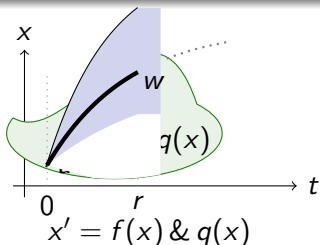
DC is a differential modal modus ponens K.

Can't leave $r(x)$, then might as well restrict state space to $r(x)$.

Axiom (Differential Cut)

(CADE'15)

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



DC is a cut for differential equations.

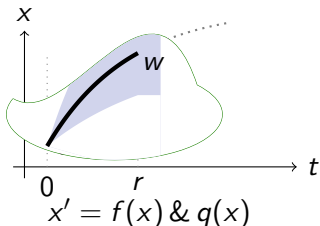
DC is a differential modal modus ponens K.

Can't leave $r(x)$, then might as well restrict state space to $r(x)$.

Axiom (Differential Cut)

(CADE'15)

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



DC is a cut for differential equations.

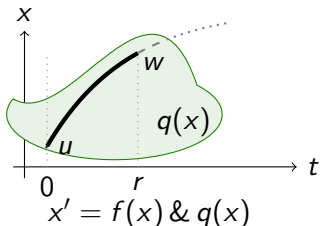
DC is a differential modal modus ponens K.

Can't leave $r(x)$, then might as well restrict state space to $r(x)$.

Axiom (Differential Cut)

(CADE'15)

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



DC is a cut for differential equations.

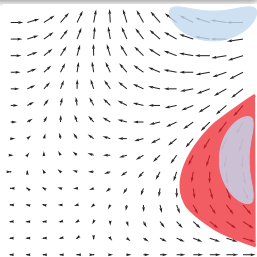
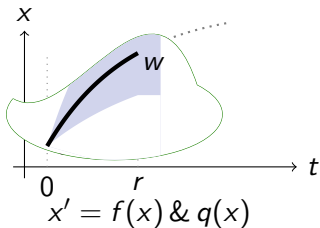
DC is a differential modal modus ponens K.

Can't leave $r(x)$, then might as well restrict state space to $r(x)$.

Axiom (Differential Cut)

(CADE'15)

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



DC is a cut for differential equations.

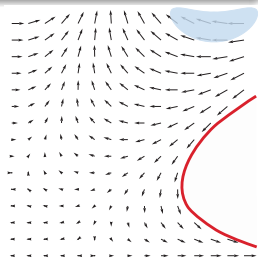
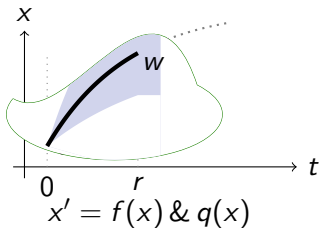
DC is a differential modal modus ponens K.

Can't leave $r(x)$, then might as well restrict state space to $r(x)$.

Axiom (Differential Cut)

(CADE'15)

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



DC is a cut for differential equations.

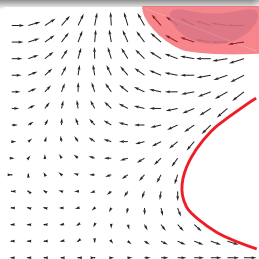
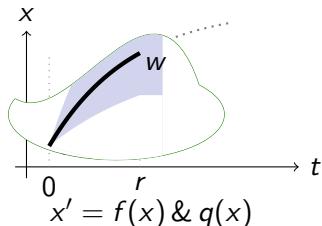
DC is a differential modal modus ponens K.

Can't leave $r(x)$, then might as well restrict state space to $r(x)$.

Axiom (Differential Cut)

(CADE'15)

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



DC is a cut for differential equations.

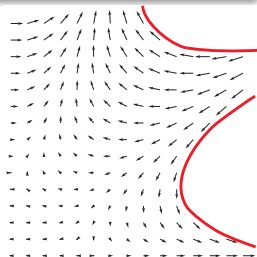
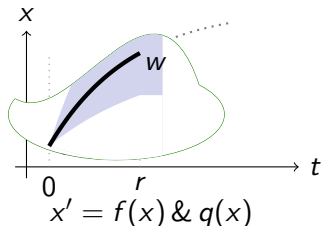
DC is a differential modal modus ponens K.

Can't leave $r(x)$, then might as well restrict state space to $r(x)$.

Axiom (Differential Cut)

(CADE'15)

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



DC is a cut for differential equations.

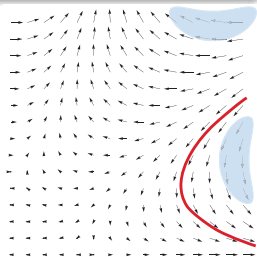
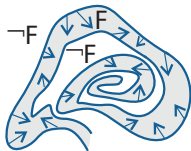
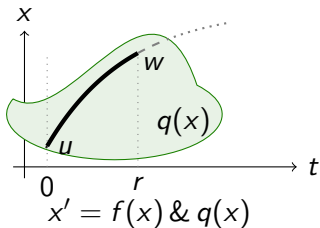
DC is a differential modal modus ponens K.

Can't leave $r(x)$, then might as well restrict state space to $r(x)$.

Axiom (Differential Invariant)

(CADE'15)

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



Differential invariant: $p(x)$ true now and its differential $(p(x))'$ true always

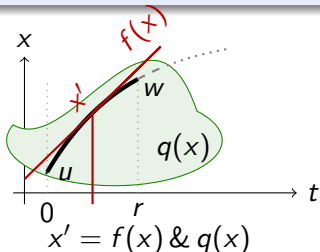
What's the differential of a formula???

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

Axiom (Differential Effect)

(CADE'15)

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



Effect of differential equation on differential symbol x'

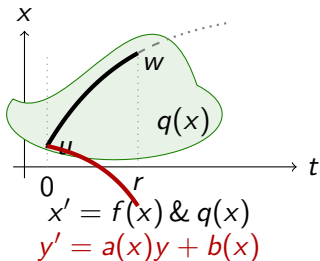
$[x' := f(x)]$ instantly mimics continuous effect $[x' = f(x)]$ on x'

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

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

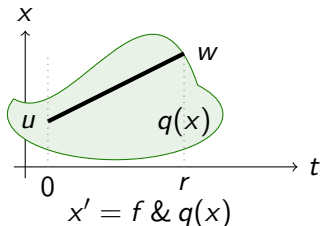
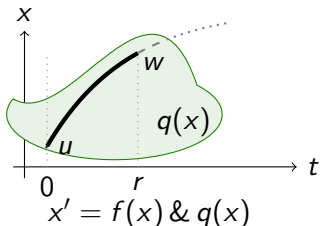
Can cause new invariants

“Dark matter” counterweight to balance conserved quantities

Axiom (Differential Solution)

(CADE'15)

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



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 **.'** differential computations are axiomatic (**US**)

$$\begin{array}{c}
 \text{US} \frac{*}{(f(\bar{x}) \cdot g(\bar{x}))' = (f(\bar{x}))' \cdot g(\bar{x}) + f(\bar{x}) \cdot (g(\bar{x}))'} \\
 \text{US} \frac{*}{(x \cdot x)' = (x)' \cdot x + x \cdot (x)'} \\
 \text{CE} \frac{*}{x^3 \cdot x + x \cdot x^3 \geq 0} \\
 \text{[':=]} \frac{[x' := x^3] x' \cdot x + x \cdot x' \geq 0}{[x' := x^3] x' \cdot x + x \cdot x' \geq 0} \\
 \text{G} \frac{[x' := x^3] x' \cdot x + x \cdot x' \geq 0}{[x' := x^3] x' \cdot x + x \cdot x' \geq 0} \\
 \text{CE} \frac{[x' := x^3] x' \cdot x + x \cdot x' \geq 0}{[x' := x^3] (x \cdot x)' \leftrightarrow x' \cdot x + x \cdot x' \geq 0} \\
 \text{DE} \frac{[x' := x^3] (x \cdot x)' \leftrightarrow x' \cdot x + x \cdot x' \geq 0}{[x' := x^3] (x \cdot x \geq 1)' \leftrightarrow x' \cdot x + x \cdot x' \geq 0} \\
 \text{DI} \frac{[x' := x^3] (x \cdot x \geq 1)' \leftrightarrow x' \cdot x + x \cdot x' \geq 0}{x \cdot x \geq 1 \rightarrow [x' := x^3] x \cdot x \geq 1}
 \end{array}$$



$$\llbracket (\theta)' \rrbracket u = ???$$

$$\llbracket (x^2)' \rrbracket u$$



$$\llbracket (\theta)' \rrbracket u = ???$$

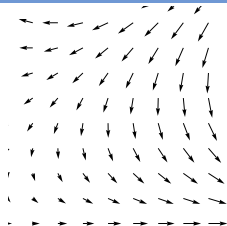
$$\llbracket (x^2)' \rrbracket u = \llbracket 2x \rrbracket u ?$$



$$\llbracket (\theta)' \rrbracket u = ???$$

$$\llbracket (x^2)' \rrbracket u = \llbracket 2x \rrbracket u ?$$

depends on the differential equation ...

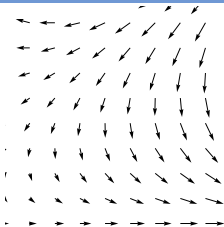


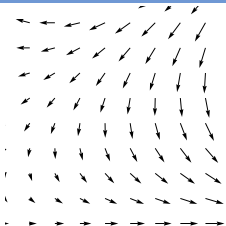
$$\llbracket (\theta)' \rrbracket u = ???$$

$$\llbracket (x^2)' \rrbracket u = \llbracket 2x \rrbracket u ?$$

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?

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

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

depends on state u

tangent space basis

cotangent space basis

depends on $u(x'_i) = dx^i$

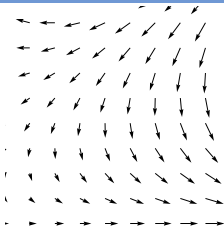


$$[(\theta)']u = ???$$

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

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 $\frac{dx}{dt}$ if that existed

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

Lemma (Differential lemma)

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

$$\text{Syntactic} \rightarrow \llbracket (\eta)' \rrbracket \varphi(\zeta) = \frac{d \llbracket \eta \rrbracket \varphi(t)}{dt}(\zeta) \leftarrow \text{Analytic}$$

Lemma (Differential assignment)

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

Lemma (Derivations)

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

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

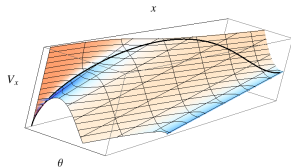
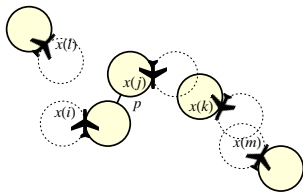
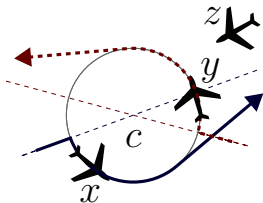
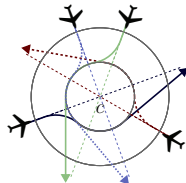
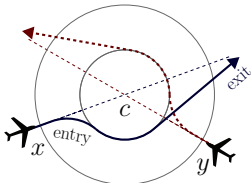
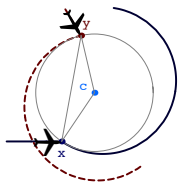
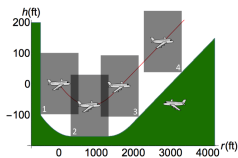
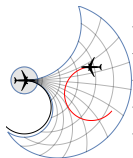
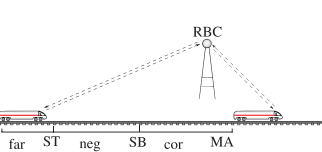
$$[y := \theta][y' := 1]((f(\theta))' = (f(y))' \cdot (\theta)') \quad \text{for } y, y' \notin \theta$$

$$(f)' = 0$$

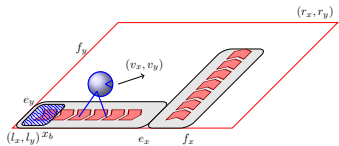
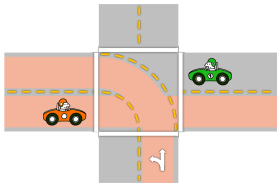
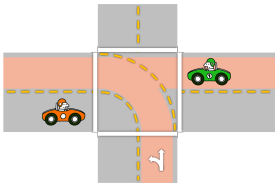
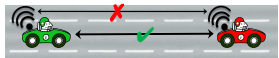
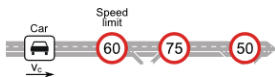
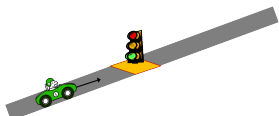
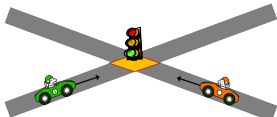
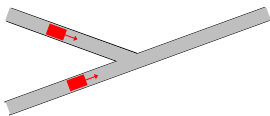
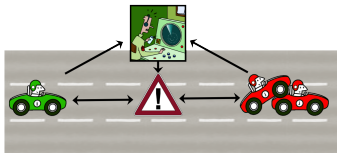
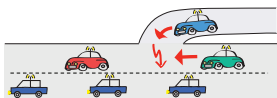
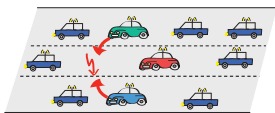
for arity 0 functions/numbers f



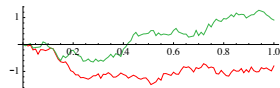
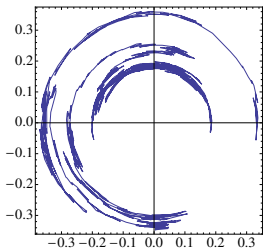
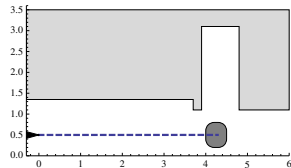
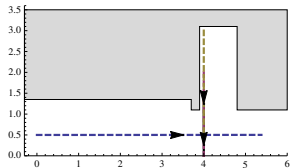
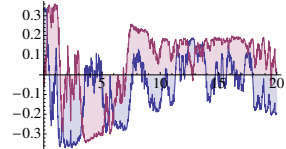
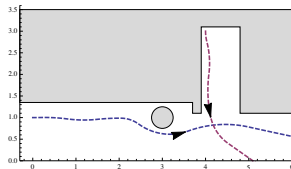
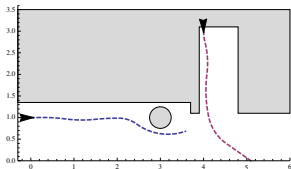
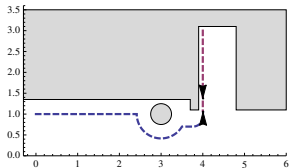
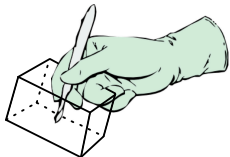
- 1 CPS are Multi-Dynamical Systems
 - Hybrid Systems
 - Hybrid Games
- 2 Dynamic Logic of Dynamical Systems
 - Syntax
 - Semantics
 - Example: Car Control Design
- 3 Proofs for CPS
 - Compositional Proof Calculus
 - Example: Safe Car Control
- 4 Theory of CPS
 - Soundness and Completeness
 - Differential Invariants
 - Example: Elementary Differential Invariants
 - Differential Axioms
- 5 Applications
- 6 Summary



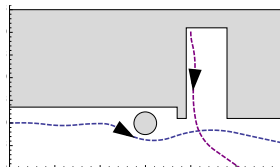
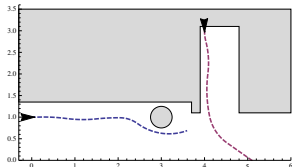
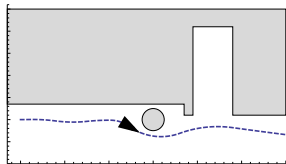
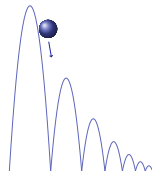
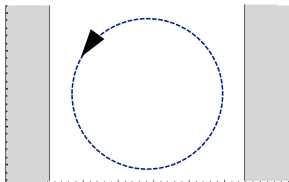
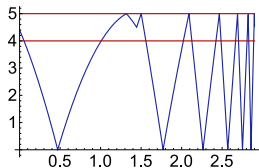
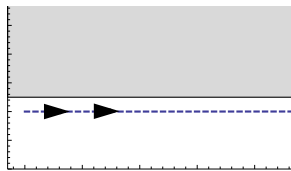
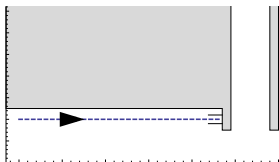
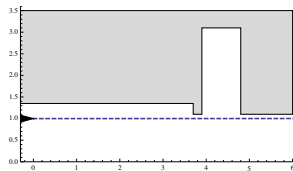
ICFEM'09, JAIS'14, TACAS'15, CAV'08, FM'09, HSCC'11, HSCC'13, TACAS'14



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



HSCC'13, RSS'13, CADE'12



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



- 1 CPS are Multi-Dynamical Systems
 - Hybrid Systems
 - Hybrid Games
- 2 Dynamic Logic of Dynamical Systems
 - Syntax
 - Semantics
 - Example: Car Control Design
- 3 Proofs for CPS
 - Compositional Proof Calculus
 - Example: Safe Car Control
- 4 Theory of CPS
 - Soundness and Completeness
 - Differential Invariants
 - Example: Elementary Differential Invariants
 - Differential Axioms
- 5 Applications
- 6 Summary



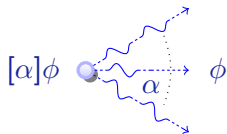
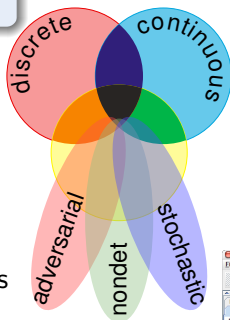
KeYmaera X Kernel: Qualifies as a Microkernel

	\approx 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

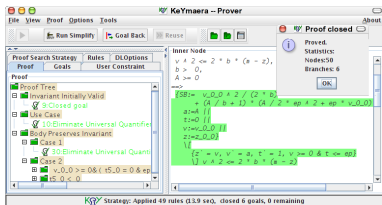
differential dynamic logic

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



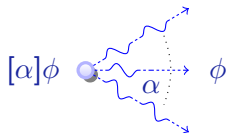
- Multi-dynamical systems
- Combine simple dynamics
- Tame complexity
- Logic & proofs for CPS
- Theory of CPS
- Applications

KeYmaera Prover

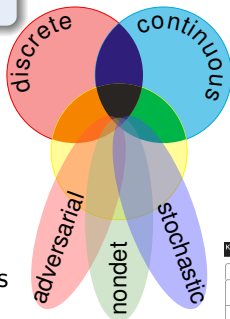


differential dynamic logic

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



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



KeYmaera X

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



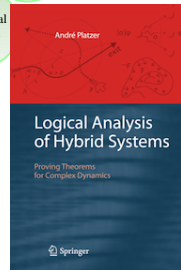
JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

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





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

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

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

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

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

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

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

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

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

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

$$(\forall) \frac{p(x)}{\forall x p(x)}$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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



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:](http://www.cs.cmu.edu/~aplatzer/course/fcps14/fcps14.pdf)

[//www.cs.cmu.edu/~aplatzer/course/fcps14/fcps14.pdf](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](https://doi.org/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](https://doi.org/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](https://doi.org/10.1145/2817824).



André Platzer.

The complete proof theory of hybrid systems.

In *LICS* [17], pages 541–550.

[doi:10.1109/LICS.2012.64](https://doi.org/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](https://doi.org/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](https://doi.org/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](https://doi.org/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](https://doi.org/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](https://doi.org/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](https://doi.org/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.



7 Differential Radical Invariants

- Differential Radical Invariants

8 ACAS X

Theorem (Differential radical invariant characterization)

$$h = 0 \rightarrow \bigwedge_{i=0}^{N-1} (h^{(i)})_{x'}^p = 0$$

$$\frac{}{h = 0 \rightarrow [x' = p]h = 0}$$

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

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

Corollary (Algebraic Invariants Decidable)

Algebraic invariants of algebraic differential equations are decidable.

Study (6th Order Longitudinal Flight Equations)

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

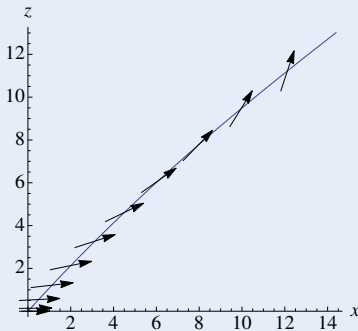
$$w' = \frac{Z}{m} + g \cos(\theta) + qu \quad \text{vertical velocity}$$

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

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

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

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



X : thrust along u

Z : thrust along w

g : gravity

m : mass

M : thrust moment for w

I_{yy} : inertia second diagonal

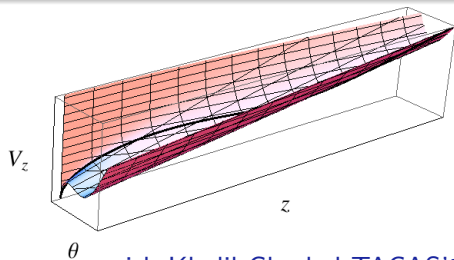
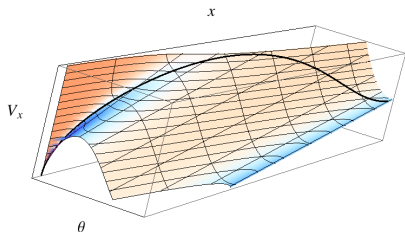
with Khalil Ghorbal TACAS'14

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



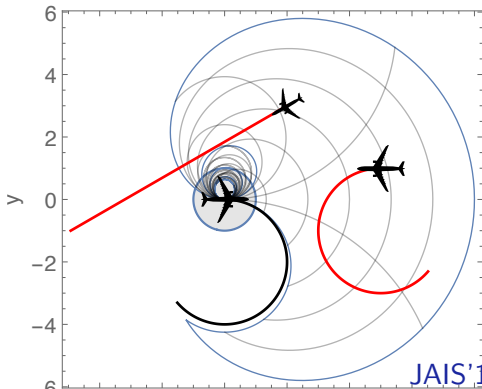
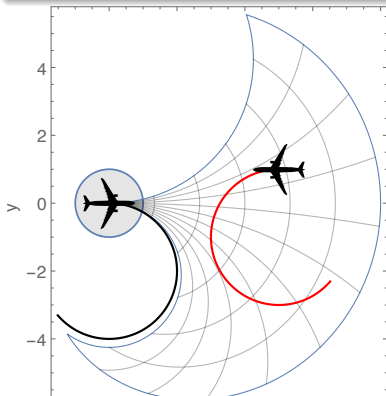
Case Study: Dubins Dynamics of 2 Airplanes



Result (DRI Automatically Generates Invariants)

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

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



J AIS'14

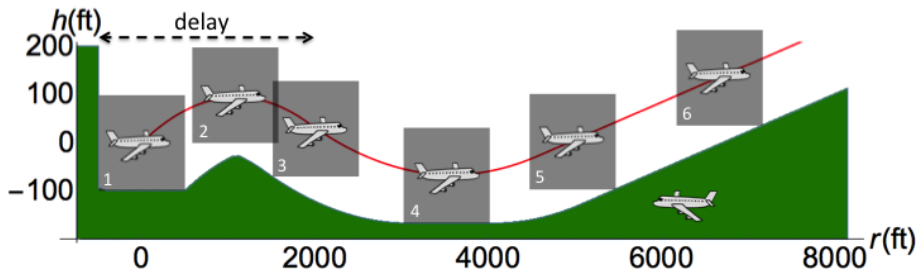


7 Differential Radical Invariants

- Differential Radical Invariants

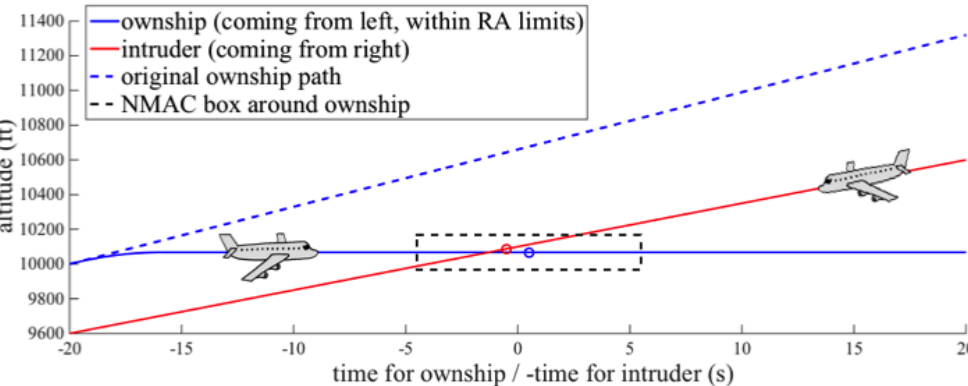
8 ACAS X

- 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

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