

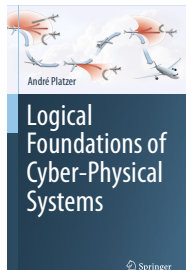
Logical Foundations of Cyber-Physical Systems

André Platzer

Karlsruhe Institute of Technology

Computer Science Department
Carnegie Mellon University

<http://lfcps.org/>



- 1 CPS are Multi-Dynamical Systems
- 2 CPS Programs
 - Syntax
 - Semantics
 - Examples
- 3 Differential Dynamic Logic
 - Syntax
 - Semantics
 - Example: Car Control Design
- 4 Dynamic Axioms for Dynamical Systems
 - Axiomatics
 - dL Proofs in KeYmaera X
- 5 Differential Invariants for Differential Equations
 - Axiomatics
 - Examples
- 6 Summary

- 1 CPS are Multi-Dynamical Systems
- 2 CPS Programs
 - Syntax
 - Semantics
 - Examples
- 3 Differential Dynamic Logic
 - Syntax
 - Semantics
 - Example: Car Control Design
- 4 Dynamic Axioms for Dynamical Systems
 - Axiomatics
 - dL Proofs in KeYmaera X
- 5 Differential Invariants for Differential Equations
 - Axiomatics
 - Examples
- 6 Summary



Which control decisions are safe for aircraft collision avoidance?

Cyber-Physical Systems

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

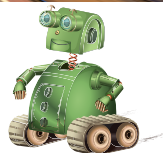
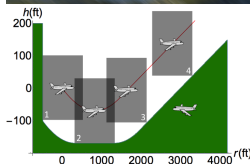
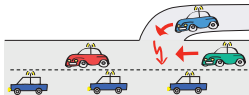
Cyber-Physical Systems Promise Transformative Impact!

Prospects: Safety & Efficiency

(Autonomous) cars

(Auto)Pilot support

Robots near humans



Cyber-Physical Systems

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

Can you trust a computer to control physics?

Can you trust a computer to control physics?

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

Rationale

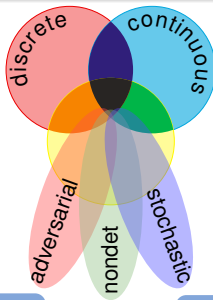
- 1 Safety guarantees require analytic foundations.
- 2 A common foundational core helps all application domains.
- 3 Foundations revolutionized digital computer science & our society.
- 4 Need even stronger foundations when software reaches out into our physical world.

CPSs deserve proofs as safety evidence!

CPSs are Multi-Dynamical Systems

CPS Dynamics

CPS are characterized by multiple facets of dynamical systems.



CPS Compositions

CPS combines multiple simple dynamical effects.

Descriptive simplification

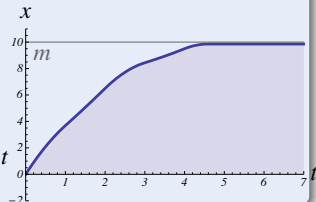
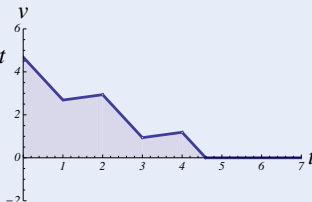
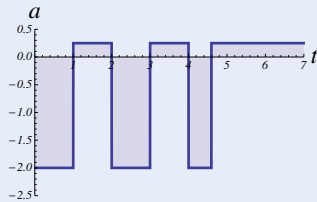
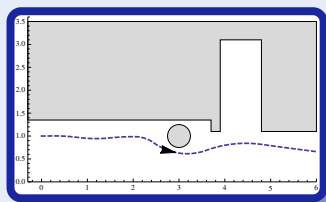
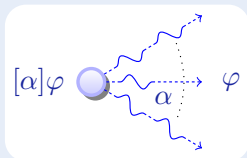
Tame Parts

Exploiting compositionality tames CPS complexity.

Analytic simplification

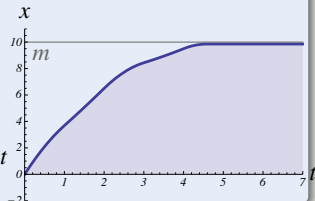
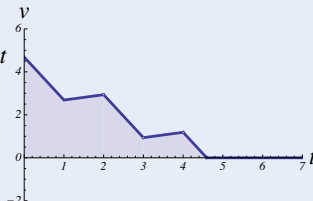
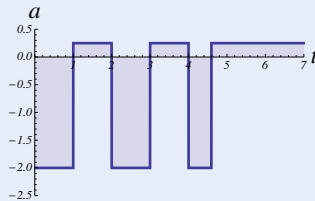
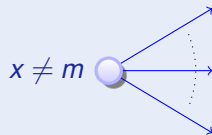
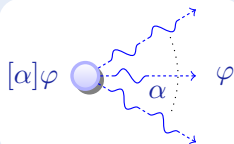
Concept (Differential Dynamic Logic)

(JAR'08, LICS'12)



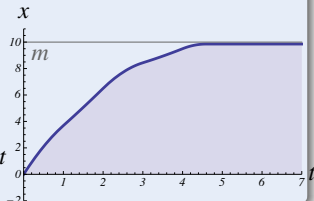
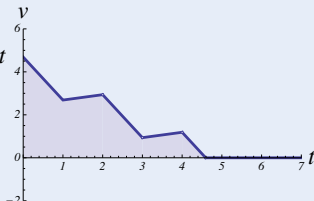
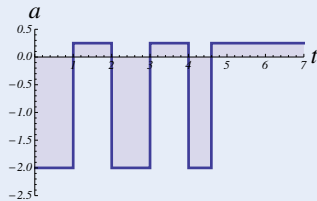
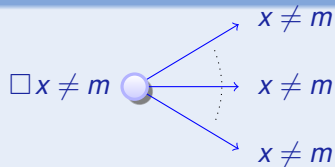
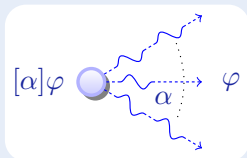
Concept (Differential Dynamic Logic)

(JAR'08, LICS'12)



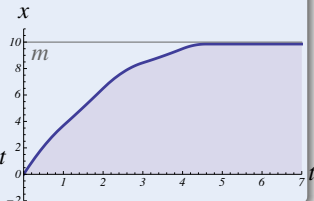
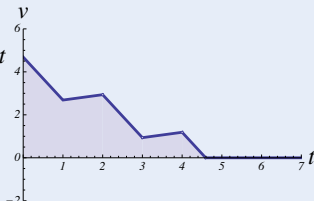
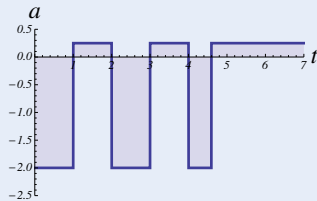
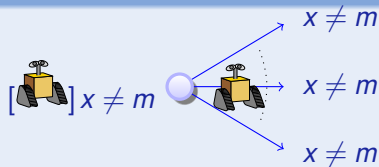
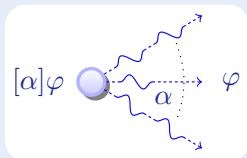
Concept (Differential Dynamic Logic)

(JAR'08, LICS'12)



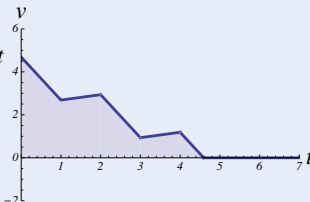
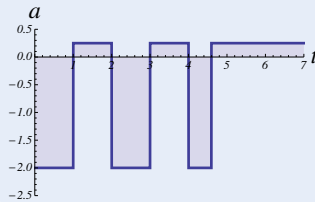
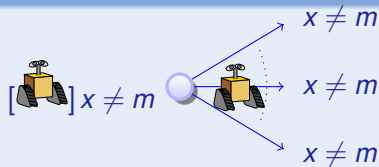
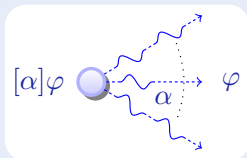
Concept (Differential Dynamic Logic)

(JAR'08, LICS'12)



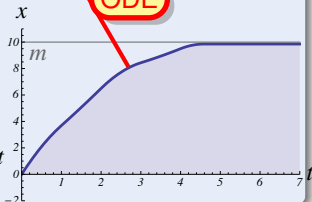
Concept (Differential Dynamic Logic)

(JAR'08, LICS'12)



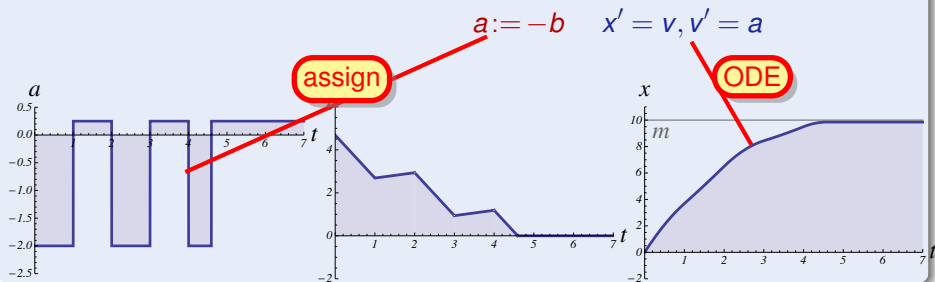
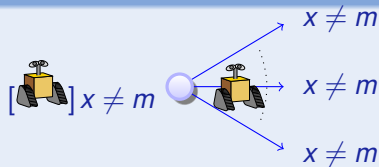
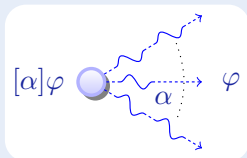
$$x' = v, v' = a$$

ODE



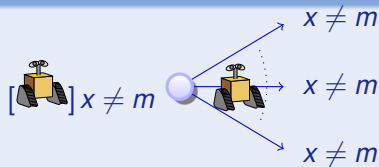
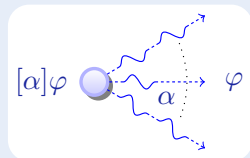
Concept (Differential Dynamic Logic)

(JAR'08, LICS'12)



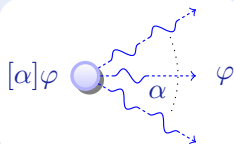
Concept (Differential Dynamic Logic)

(JAR'08, LICS'12)



Concept (Differential Dynamic Logic)

(JAR'08, LICS'12)



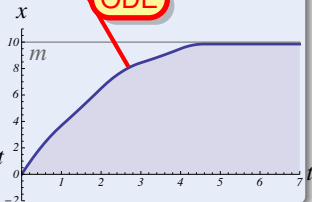
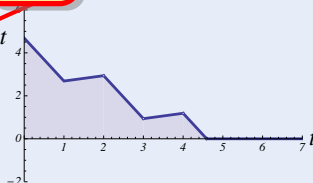
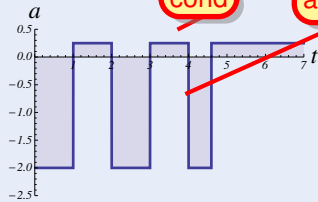
seq.
compose

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

cond

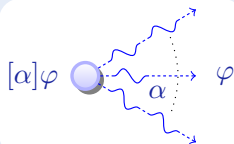
assign

ODE



Concept (Differential Dynamic Logic)

(JAR'08, LICS'12)



seq.
compose

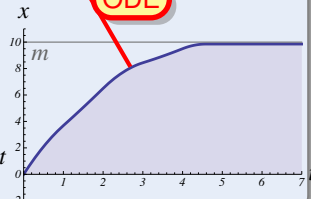
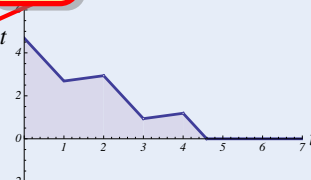
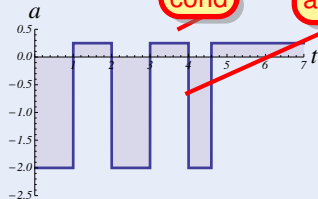
nondet.
repeat

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

cond

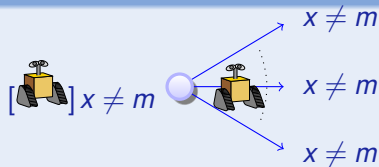
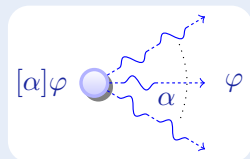
assign

ODE



Concept (Differential Dynamic Logic)

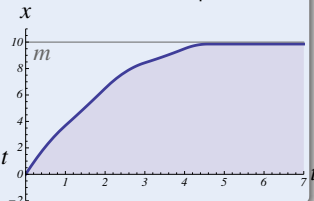
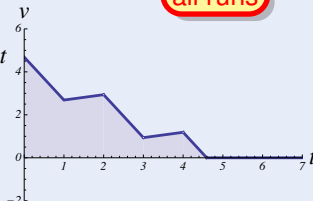
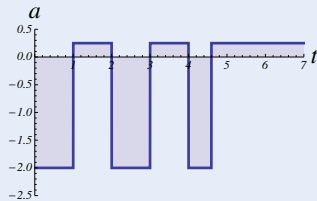
(JAR'08, LICS'12)



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

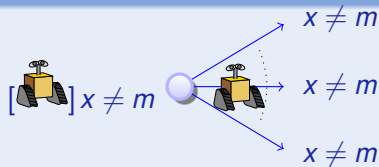
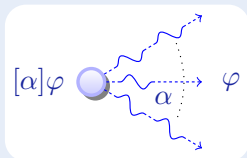
all runs

post



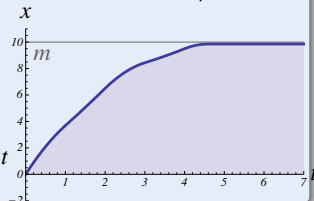
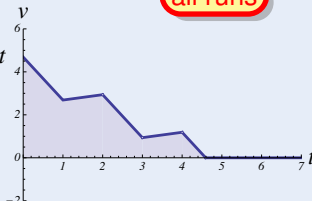
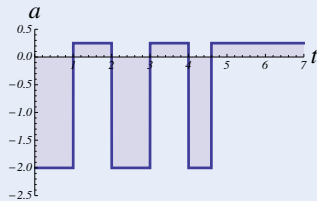
Concept (Differential Dynamic Logic)

(JAR'08, LICS'12)



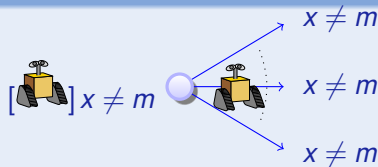
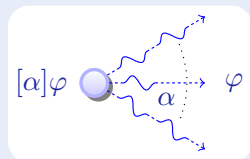
$$\underbrace{x \neq m \wedge b > 0}_{\text{init}} \rightarrow \left[\left(\left(\text{if}(\text{SB}(x, m)) \quad a := -b \right) ; x' = v, v' = a \right)^* \right] \underbrace{x \neq m}_{\text{post}}$$

all runs



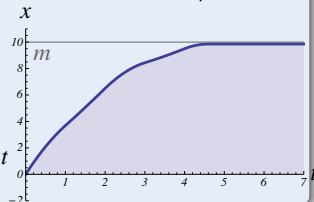
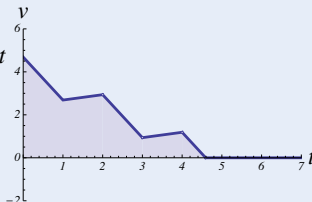
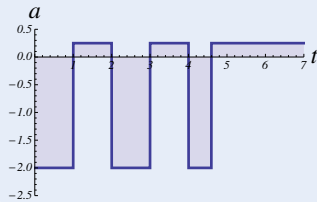
Concept (Differential Dynamic Logic)

(JAR'08, LICS'12)



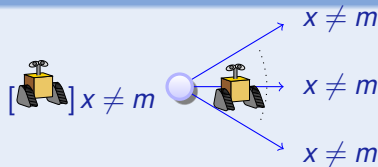
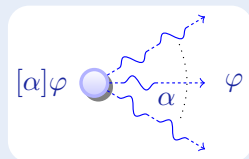
nondet.
choice

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



Concept (Differential Dynamic Logic)

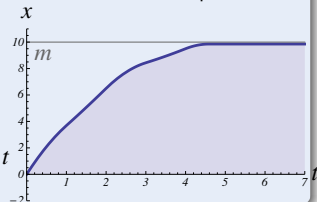
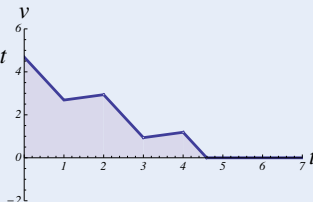
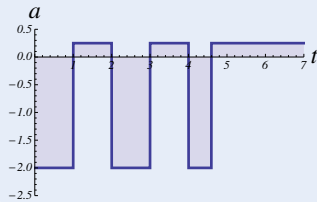
(JAR'08, LICS'12)



test

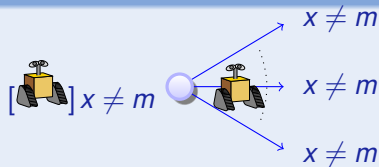
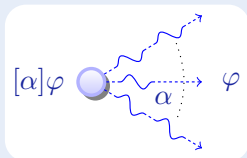
nondet.
choice

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



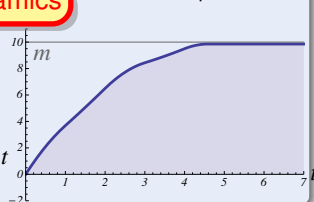
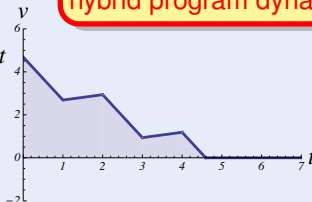
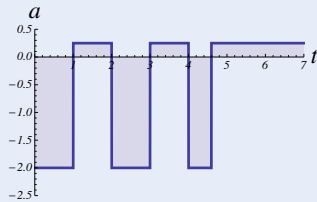
Concept (Differential Dynamic Logic)

(JAR'08, LICS'12)



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

hybrid program dynamics



- 1 CPS are Multi-Dynamical Systems
- 2 **CPS Programs**
 - Syntax
 - Semantics
 - Examples
- 3 Differential Dynamic Logic
 - Syntax
 - Semantics
 - Example: Car Control Design
- 4 Dynamic Axioms for Dynamical Systems
 - Axiomatics
 - dL Proofs in KeYmaera X
- 5 Differential Invariants for Differential Equations
 - Axiomatics
 - Examples
- 6 Summary

Definition (Syntax of hybrid program α)

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

Definition (Syntax of hybrid program α)

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

Discrete
Assign

Test
Condition

Differential
Equation

Nondet.
Choice

Seq.
Compose

Nondet.
Repeat

Definition (Syntax of hybrid program α)

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

Discrete
Assign

Test
Condition

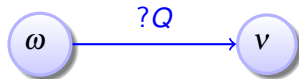
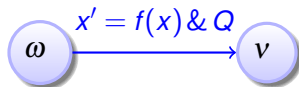
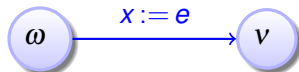
Differential
Equation

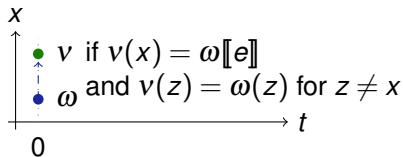
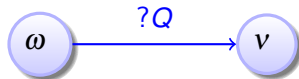
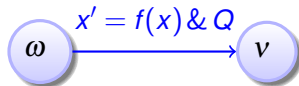
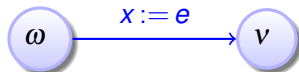
Nondet.
Choice

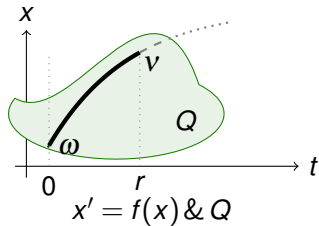
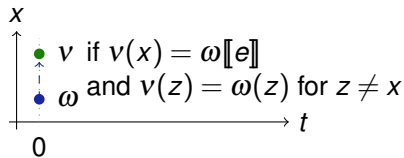
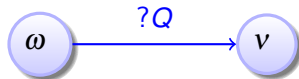
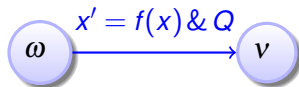
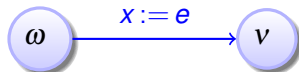
Seq.
Compose

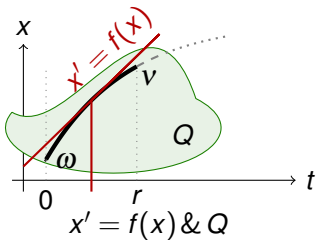
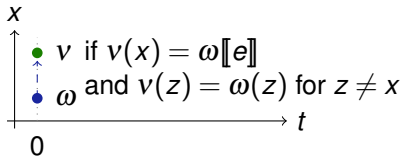
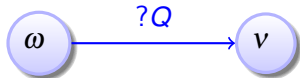
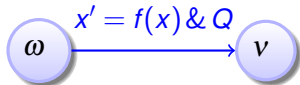
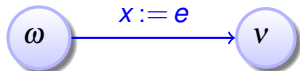
Nondet.
Repeat

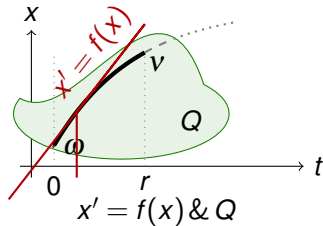
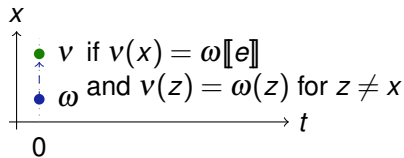
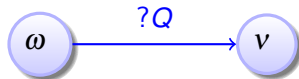
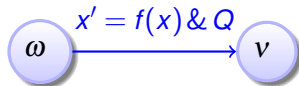
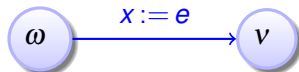
Like regular expressions. Everything nondeterministic

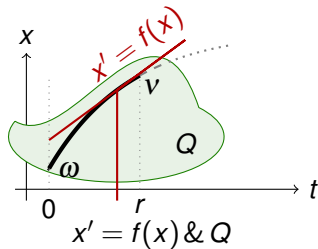
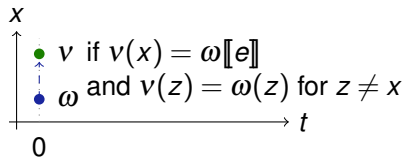
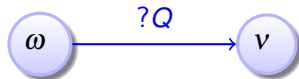
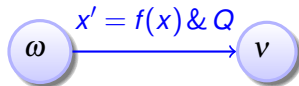
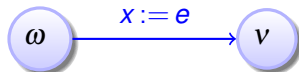


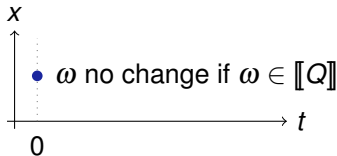
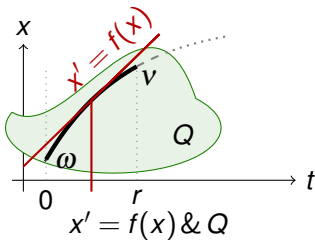
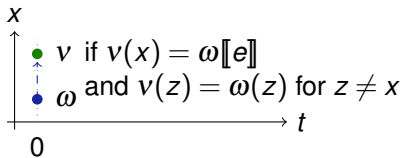
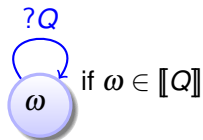
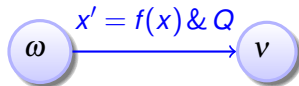
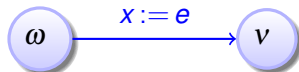


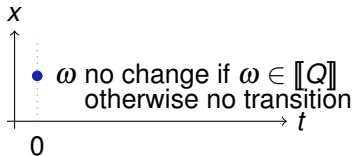
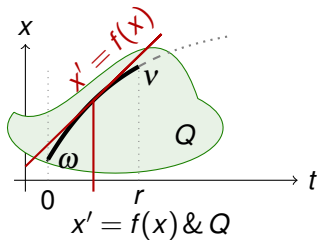
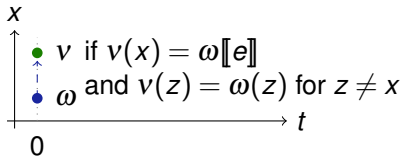
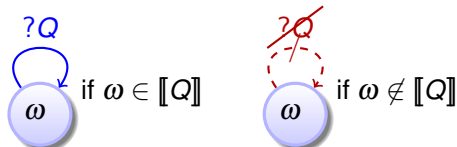
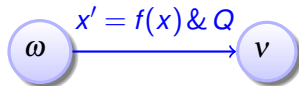
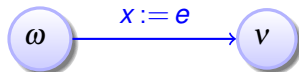


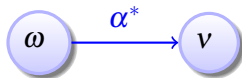
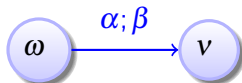
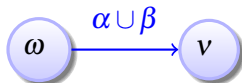


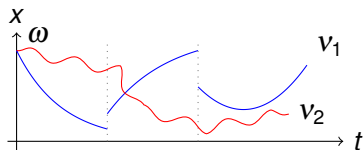
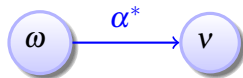
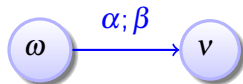
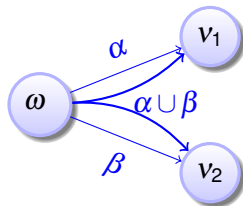


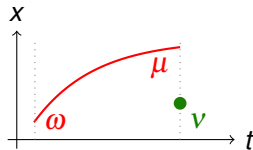
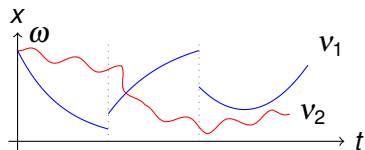
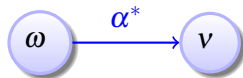
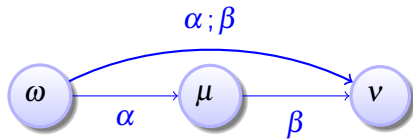
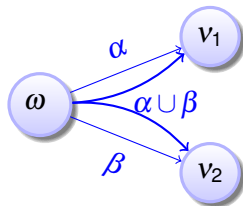


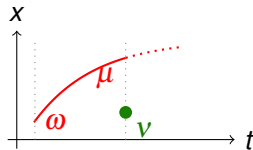
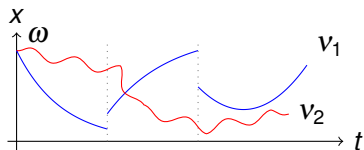
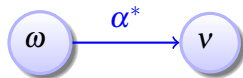
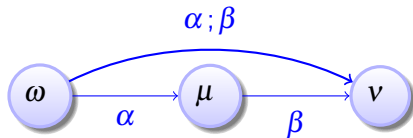
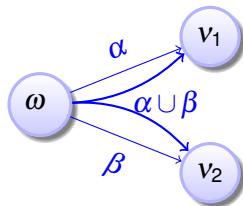


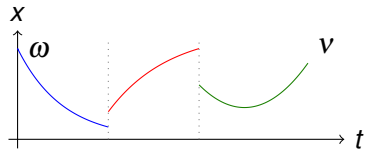
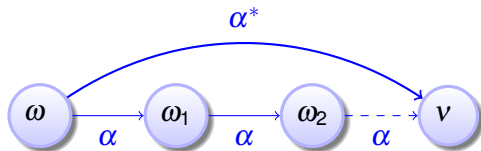
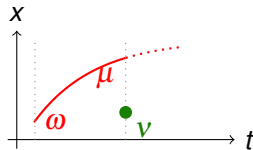
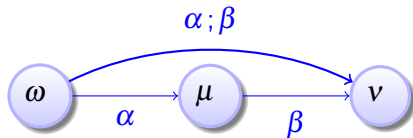
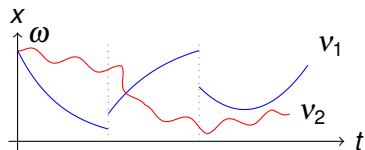
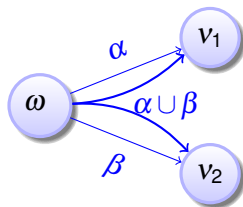


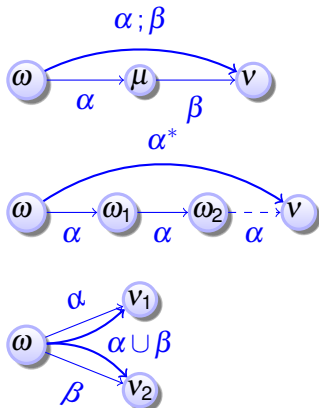


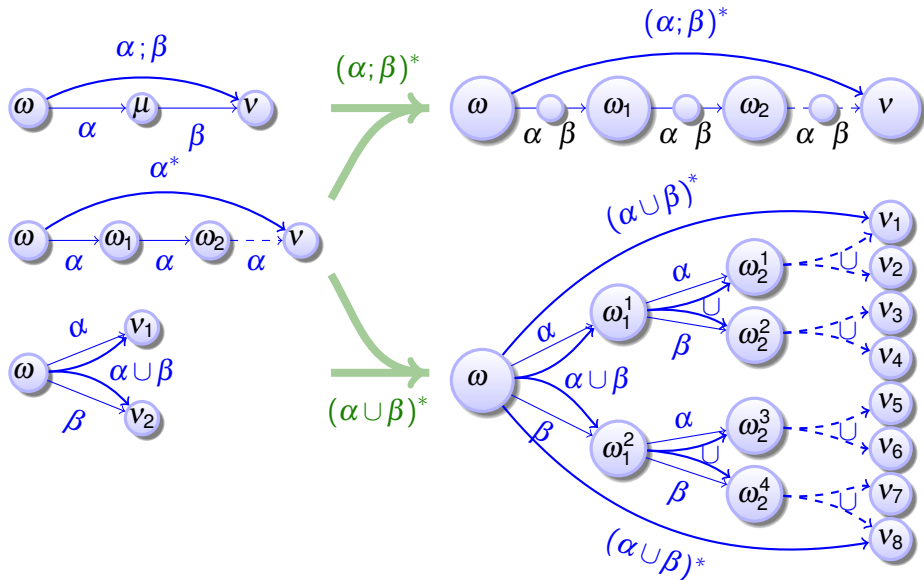












Definition (Syntax of hybrid program α)

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

Definition (Semantics of hybrid programs) $(\llbracket \cdot \rrbracket : \text{HP} \rightarrow \wp(\mathcal{S} \times \mathcal{S}))$

$$\llbracket x := e \rrbracket = \{(\omega, v) : v = \omega \text{ except } v[x] = \omega[e]\}$$

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

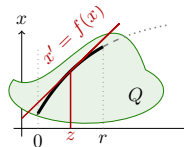
$$\llbracket x' = f(x) \rrbracket = \{(\varphi(0), \varphi(r)) : \varphi \models x' = f(x) \text{ for some duration } r \geq 0\}$$

$$\llbracket \alpha \cup \beta \rrbracket = \llbracket \alpha \rrbracket \cup \llbracket \beta \rrbracket$$

$$\llbracket \alpha; \beta \rrbracket = \llbracket \alpha \rrbracket \circ \llbracket \beta \rrbracket = \{(\omega, v) : (\omega, \mu) \in \llbracket \alpha \rrbracket \text{ and } (\mu, v) \in \llbracket \beta \rrbracket\}$$

$$\llbracket \alpha^* \rrbracket = \llbracket \alpha \rrbracket^* = \bigcup_{n \in \mathbb{N}} \llbracket \alpha^n \rrbracket \quad \alpha^n \equiv \underbrace{\alpha; \alpha; \alpha; \dots; \alpha}_{n \text{ times}}$$

compositional



Definition (Syntax of hybrid program α)

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

Definition (Semantics of hybrid programs) $([\![\cdot]\!] : \text{HP} \rightarrow \wp(\mathcal{S} \times \mathcal{S}))$

$$[\![x := e]\!] = \{(\omega, v) : v = \omega \text{ except } v[x] = \omega[e]\}$$

$$[\![?Q]\!] = \{(\omega, \omega) : \omega \in [Q]\}$$

$$[\![x' = f(x)]\!] = \{(\varphi(0), \varphi(r)) : \varphi \models x' = f(x) \text{ for some duration } r \geq 0\}$$

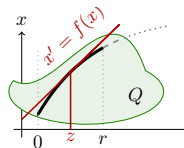
$$[\![\alpha \cup \beta]\!] = [\![\alpha]\!] \cup [\![\beta]\!]$$

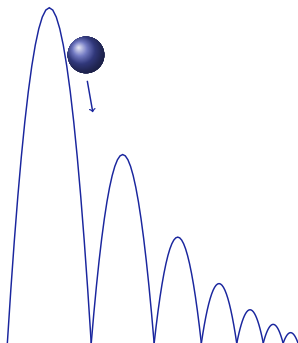
$$[\![\alpha; \beta]\!] = [\![\alpha]\!] \circ [\![\beta]\!]$$

$$[\![\alpha^*]\!] = [\![\alpha]\!]^* = \bigcup_{n \in \mathbb{N}} [\![\alpha^n]\!]$$

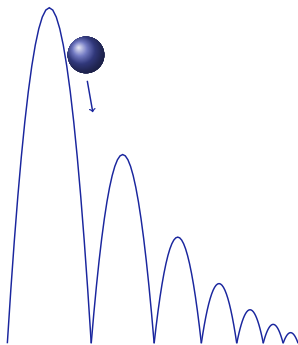
compositional

- 1 $\varphi(z)(x') = \frac{d\varphi(t)(x)}{dt}(z)$ exists at all times $0 \leq z \leq r$
- 2 $\varphi(z) \in [x' = f(x) \wedge Q]$ for all times $0 \leq z \leq r$
- 3 $\varphi(z) = \varphi(0)$ except at x, x'



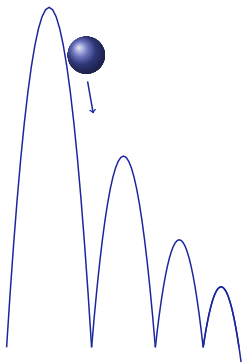


Example (Quantum the Bouncing Ball)



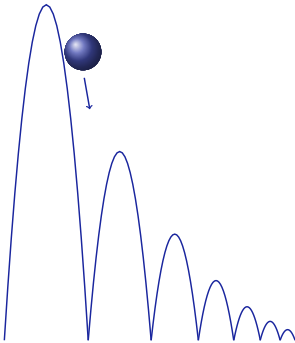
Example (Quantum the Bouncing Ball)

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



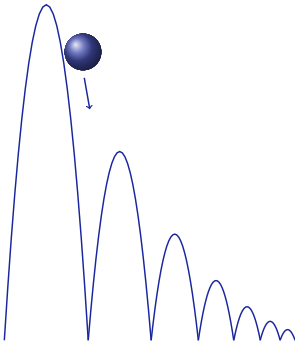
Example (Quantum the Bouncing Ball)

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



Example (Quantum the Bouncing Ball)

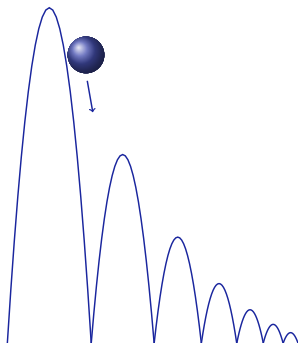
$$\{x' = v, v' = -g \& x \geq 0\}$$



Example (Quantum the Bouncing Ball)

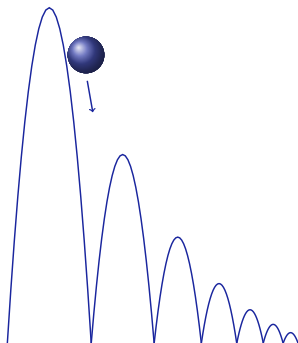
$$\{x' = v, v' = -g \& x \geq 0\};$$

$$\text{if}(x = 0) \quad v := -cv$$



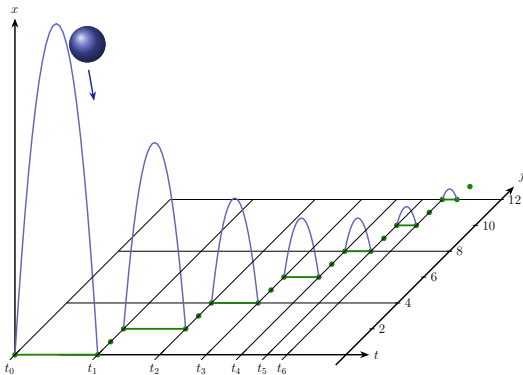
Example (Quantum the Bouncing Ball)

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



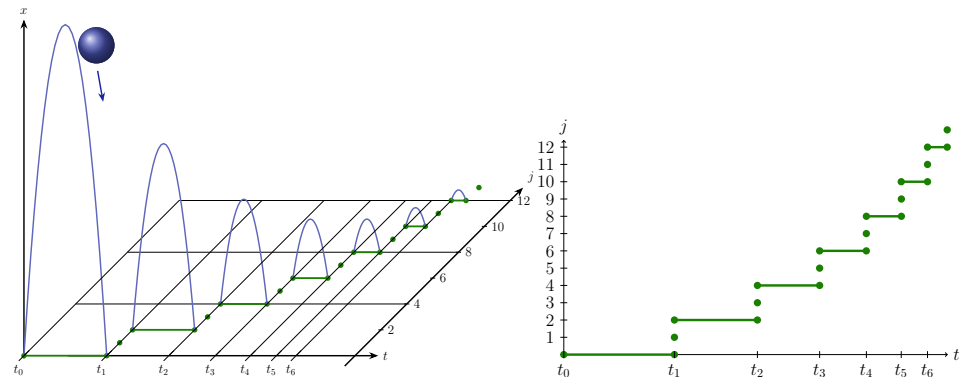
Example (Quantum the Bouncing Ball)

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



Example (Quantum the Bouncing Ball)

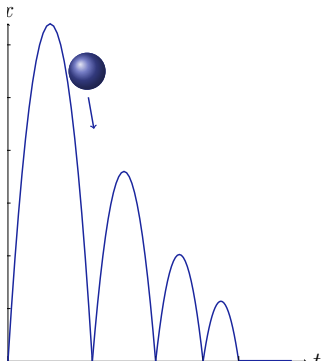
$$(\{x' = v, v' = -g \& x \geq 0\}; \\ \text{if}(x = 0) \ v := -cv)^*$$



Example (Quantum the Bouncing Ball)

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

$$\text{if}(x = 0) \ v := -cv)^*$$

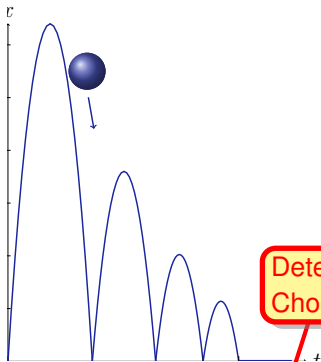


if(Q) α else $\beta \equiv$

Example (Quantum the Bouncing Ball)

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

$\text{if}(x = 0) \ v := -cv)^*$



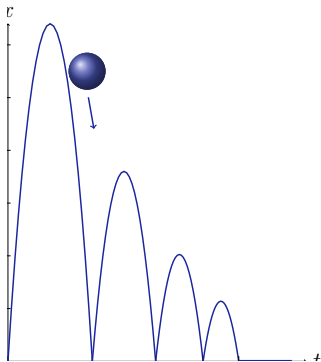
$\text{if}(Q) \alpha \text{ else } \beta \equiv (?Q; \alpha) \cup (? \neg Q; \beta)$

Determ.
Choice

Nondet.
Choice

Example (Quantum the Bouncing Ball)

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

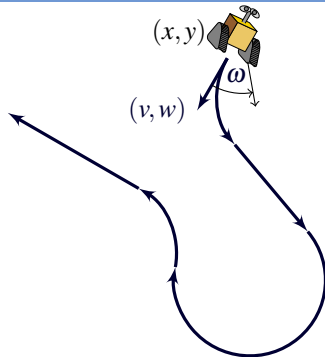


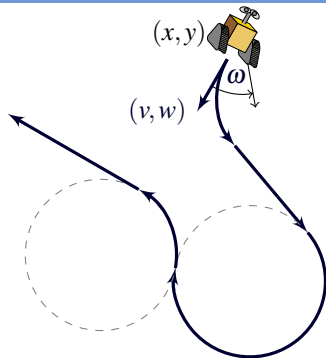
Nondet.
Assign

Test
Limits

Example (Quantum the Bouncing Ball)

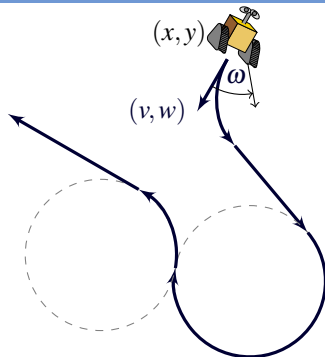
$$(\{x' = v, v' = -g \ \& \ x \geq 0\}; \\ \text{if}(x = 0) (\textcolor{red}{c} := *; ?c \geq 0; v := -cv))^*$$





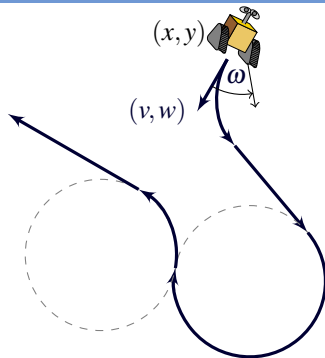
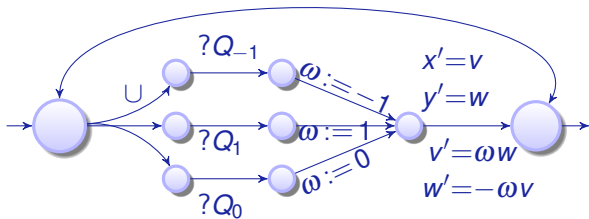
Example (Runaround Robot)

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



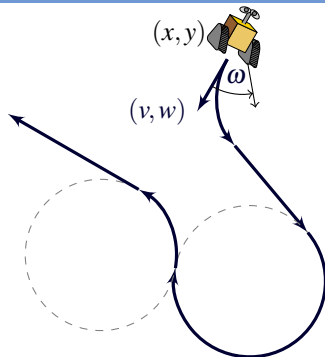
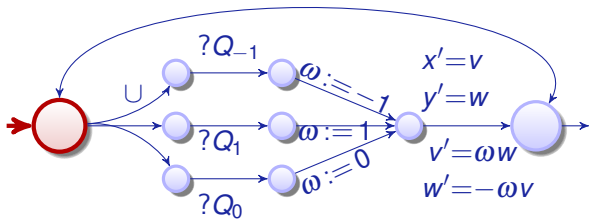
Example (Runaround Robot)

$$((?Q_{-1}; \omega := -1 \cup ?Q_1; \omega := 1 \cup ?Q_0; \omega := 0); \\ \{x' = v, y' = w, v' = \omega w, w' = -\omega v\})^*$$



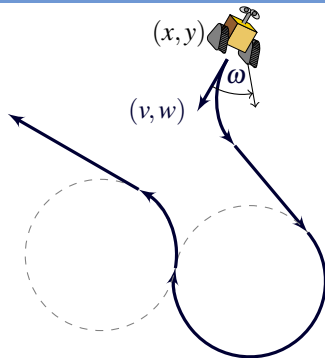
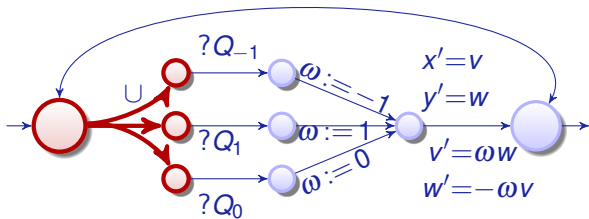
Example (Runaround Robot)

$$((?Q_{-1}; \omega := -1 \cup ?Q_1; \omega := 1 \cup ?Q_0; \omega := 0); \{x' = v, y' = w, v' = \omega w, w' = -\omega v\})^*$$



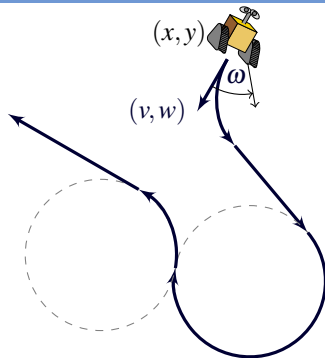
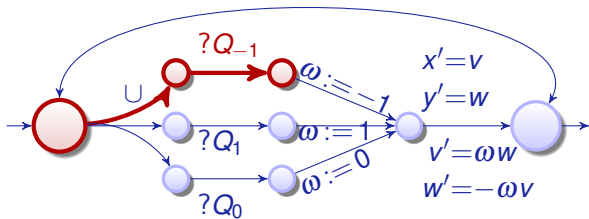
Example (Runaround Robot)

$$((?Q_{-1}; \omega := -1 \cup ?Q_1; \omega := 1 \cup ?Q_0; \omega := 0); \{x' = v, y' = w, v' = \omega w, w' = -\omega v\})^*$$



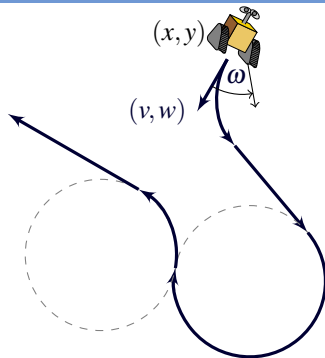
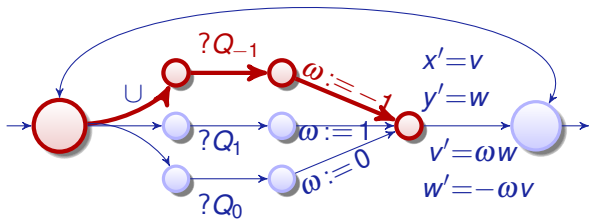
Example (Runaround Robot)

$$((?Q_{-1}; \omega := -1 \cup ?Q_1; \omega := 1 \cup ?Q_0; \omega := 0); \{x' = v, y' = w, v' = \omega w, w' = -\omega v\})^*$$



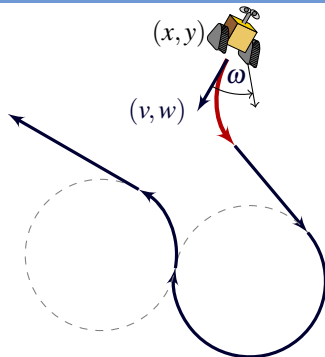
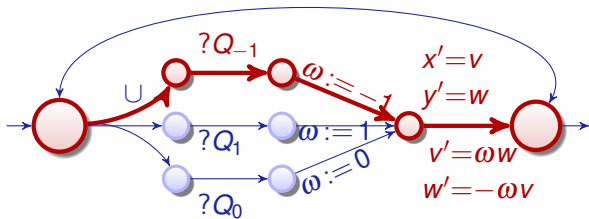
Example (Runaround Robot)

$$((?Q_{-1}; \omega := -1 \cup ?Q_1; \omega := 1 \cup ?Q_0; \omega := 0); \{x' = v, y' = w, v' = \omega w, w' = -\omega v\})^*$$



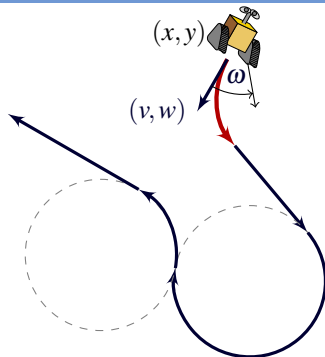
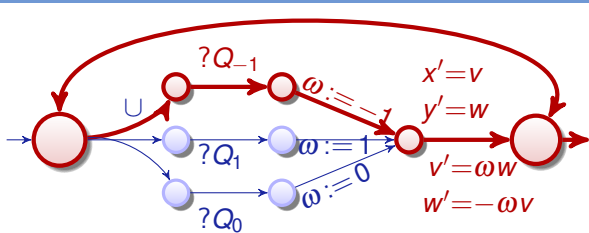
Example (Runaround Robot)

$$((?Q_{-1}; \omega := -1 \cup ?Q_1; \omega := 1 \cup ?Q_0; \omega := 0); \{x' = v, y' = w, v' = \omega w, w' = -\omega v\})^*$$



Example (Runaround Robot)

$$((?Q_{-1}; \omega := -1 \cup ?Q_1; \omega := 1 \cup ?Q_0; \omega := 0); \\ \{x' = v, y' = w, v' = \omega w, w' = -\omega v\})^*$$

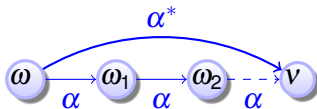
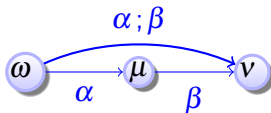
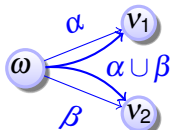
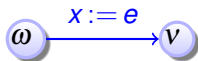
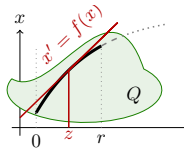


Example (Runaround Robot)

$$((?Q_{-1}; \omega := -1 \cup ?Q_1; \omega := 1 \cup ?Q_0; \omega := 0); \{x' = v, y' = w, v' = \omega w, w' = -\omega v\})^*$$

Definition (Hybrid program)

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

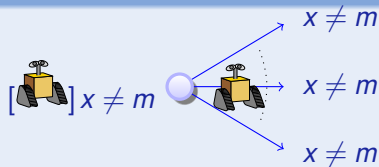
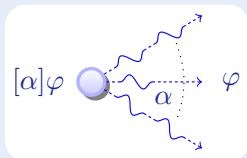


Programming CPS $\neq$ program cyber $\parallel$ program physics (mutual ignorance)

- 1 CPS are Multi-Dynamical Systems
- 2 CPS Programs
 - Syntax
 - Semantics
 - Examples
- 3 Differential Dynamic Logic
 - Syntax
 - Semantics
 - Example: Car Control Design
- 4 Dynamic Axioms for Dynamical Systems
 - Axiomatics
 - dL Proofs in KeYmaera X
- 5 Differential Invariants for Differential Equations
 - Axiomatics
 - Examples
- 6 Summary

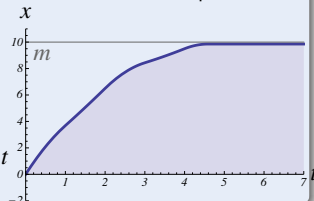
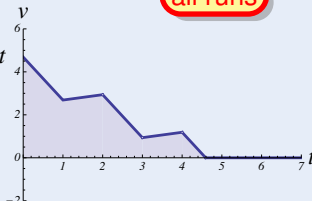
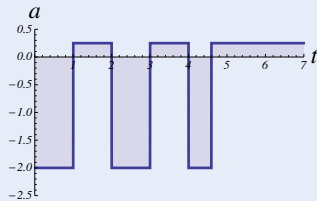
Concept (Differential Dynamic Logic)

(JAR'08, LICS'12)



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

all runs



Definition (Syntax of differential dynamic logic)

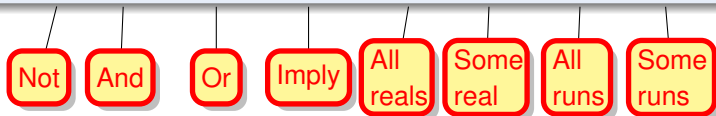
The *formulas of differential dynamic logic* are defined by the grammar:

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

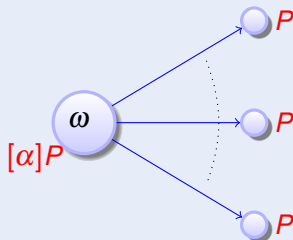
Definition (Syntax of differential dynamic logic)

The *formulas of differential dynamic logic* are defined by the grammar:

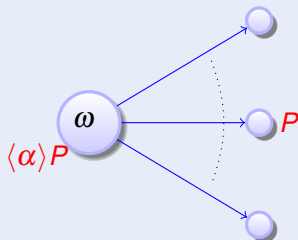
$$P, Q ::= e \geq \tilde{e} \mid \neg P \mid P \wedge Q \mid P \vee Q \mid P \rightarrow Q \mid \forall x P \mid \exists x P \mid [\alpha]P \mid \langle \alpha \rangle P$$



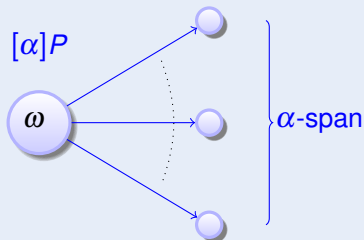
Definition (dL Formulas)



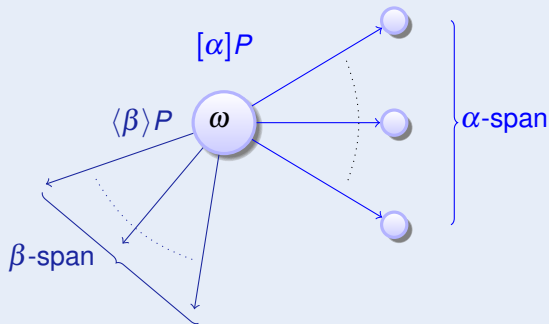
Definition (dL Formulas)



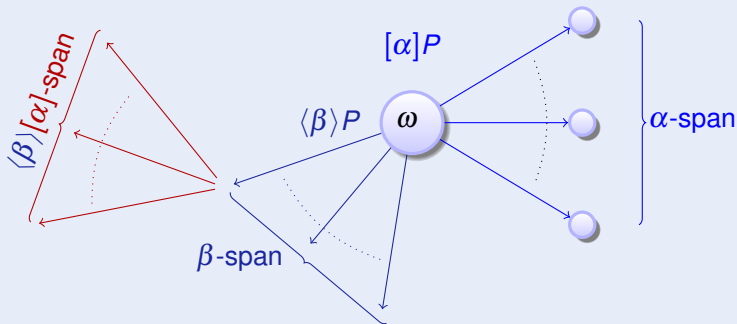
Definition (dL Formulas)



Definition (dL Formulas)



Definition (dL Formulas)



Definition (Syntax of differential dynamic logic)

The *formulas of differential dynamic logic* are defined by the grammar:

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

Definition (dL semantics)

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

$$\llbracket e \geq \tilde{e} \rrbracket = \{\omega : \omega[e] \geq \omega[\tilde{e}]\}$$

$$\llbracket \neg P \rrbracket = \llbracket P \rrbracket^c = \mathcal{S} \setminus \llbracket P \rrbracket$$

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

$$\llbracket P \vee Q \rrbracket = \llbracket P \rrbracket \cup \llbracket Q \rrbracket$$

$$\llbracket P \rightarrow Q \rrbracket = \llbracket P \rrbracket^c \cup \llbracket Q \rrbracket$$

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

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

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

$$\llbracket \forall x P \rrbracket = \{\omega : \omega_x^r \in \llbracket P \rrbracket \text{ for all } r \in \mathbb{R}\}$$

$$\omega_x^d(y) = \begin{cases} d & \text{if } y=x \\ \omega(y) & \text{if } y \neq x \end{cases}$$

$\llbracket P \rrbracket$ the set of states in which formula P is true

$\omega \models P$ formula P is true in state ω , alias $\omega \in \llbracket P \rrbracket$

$\models P$ formula P is valid, i.e., true in all states ω , i.e., $\llbracket P \rrbracket = \mathcal{S}$

Definition (dL semantics)

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

$$\llbracket e \geq \tilde{e} \rrbracket = \{ \omega : \omega[e] \geq \omega[\tilde{e}] \}$$

$$\llbracket \neg P \rrbracket = \llbracket P \rrbracket^c = \mathcal{S} \setminus \llbracket P \rrbracket$$

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

$$\llbracket P \vee Q \rrbracket = \llbracket P \rrbracket \cup \llbracket Q \rrbracket$$

$$\llbracket P \rightarrow Q \rrbracket = \llbracket P \rrbracket^c \cup \llbracket Q \rrbracket$$

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

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

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

$$\llbracket \forall x P \rrbracket = \{ \omega : \omega_x^r \in \llbracket P \rrbracket \text{ for all } r \in \mathbb{R} \}$$

$$\omega_x^d(y) = \begin{cases} d & \text{if } y=x \\ \omega(y) & \text{if } y \neq x \end{cases}$$

$\llbracket P \rrbracket$ the set of states in which formula P is true

$\omega \models P$ formula P is true in state ω , alias $\omega \in \llbracket P \rrbracket$

$\models P$ formula P is valid, i.e., true in all states ω , i.e., $\llbracket P \rrbracket = \mathcal{S}$

$$\exists d[x := 1; x' = d]x \geq 0 \text{ and } [x := x + 1; x' = d]x \geq 0 \text{ and } \langle x' = d \rangle x \geq 0$$

Definition (dL semantics)

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

$$\llbracket e \geq \tilde{e} \rrbracket = \{ \omega : \omega[e] \geq \omega[\tilde{e}] \}$$

$$\llbracket \neg P \rrbracket = \llbracket P \rrbracket^c = \mathcal{S} \setminus \llbracket P \rrbracket$$

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

$$\llbracket P \vee Q \rrbracket = \llbracket P \rrbracket \cup \llbracket Q \rrbracket$$

$$\llbracket P \rightarrow Q \rrbracket = \llbracket P \rrbracket^c \cup \llbracket Q \rrbracket$$

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

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

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

$$\llbracket \forall x P \rrbracket = \{ \omega : \omega_x^r \in \llbracket P \rrbracket \text{ for all } r \in \mathbb{R} \}$$

$$\omega_x^d(y) = \begin{cases} d & \text{if } y = x \\ \omega(y) & \text{if } y \neq x \end{cases}$$

$\llbracket P \rrbracket$ the set of states in which formula P is true

$\omega \models P$ formula P is true in state ω , alias $\omega \in \llbracket P \rrbracket$

$\models P$ formula P is valid, i.e., true in all states ω , i.e., $\llbracket P \rrbracket = \mathcal{S}$

$\models \exists d[x := 1; x' = d]x \geq 0$ and $\not\models [x := x + 1; x' = d]x \geq 0$ and $\not\models \langle x' = d \rangle x \geq 0$

Definition (dL semantics)

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

$$\llbracket e \geq \tilde{e} \rrbracket = \{ \omega : \omega[e] \geq \omega[\tilde{e}] \}$$

$$\llbracket \neg P \rrbracket = \llbracket P \rrbracket^c = \mathcal{S} \setminus \llbracket P \rrbracket$$

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

$$\llbracket P \vee Q \rrbracket = \llbracket P \rrbracket \cup \llbracket Q \rrbracket$$

$$\llbracket P \rightarrow Q \rrbracket = \llbracket P \rrbracket^c \cup \llbracket Q \rrbracket$$

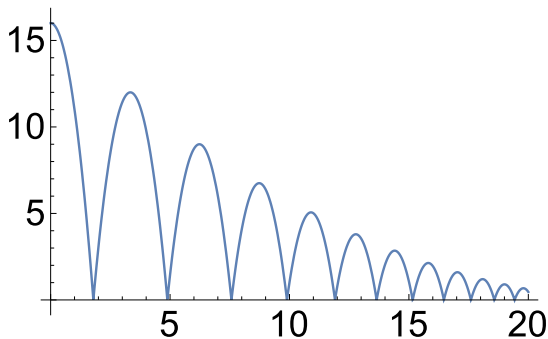
$$\llbracket \langle \alpha \rangle P \rrbracket = \llbracket \alpha \rrbracket \circ \llbracket P \rrbracket = \{ \omega : v \in \llbracket P \rrbracket \text{ for some } v : (\omega, v) \in \llbracket \alpha \rrbracket \}$$

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

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

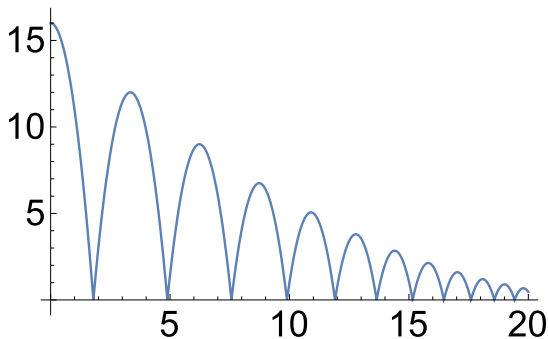
$$\llbracket \forall x P \rrbracket = \{ \omega : \omega_x^r \in \llbracket P \rrbracket \text{ for all } r \in \mathbb{R} \}$$

$$\omega_x^d(y) = \begin{cases} d & \text{if } y = x \\ \omega(y) & \text{if } y \neq x \end{cases}$$



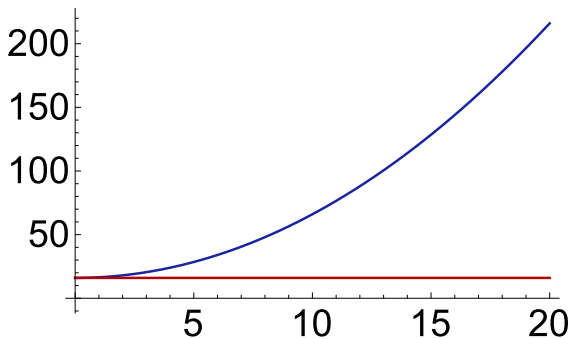
Example (▶ Bouncing Ball)

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



Example (▶ Bouncing Ball)

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

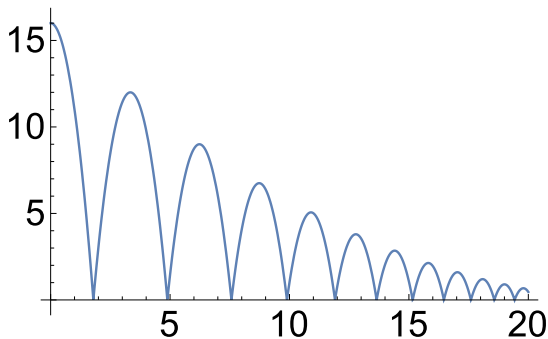


Not if $g < 0$ in anti-gravity

Example (▶ Bouncing Ball)

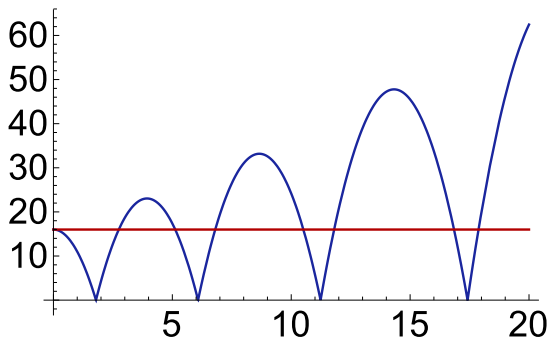
$$H = x \geq 0$$

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



Example (▶ Bouncing Ball)

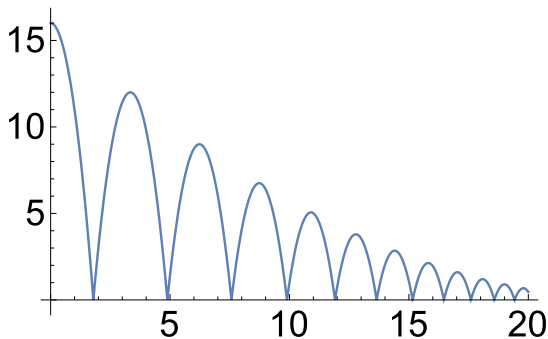
$$H = x \geq 0 \wedge g > 0 \rightarrow \left[\left(\{x' = v, v' = -g \wedge x \geq 0\}; \right. \right. \\ \left. \left. \text{if}(x = 0) v := -cv \right)^* \right] 0 \leq x \leq H$$



Not if $c > 1$ for anti-damping

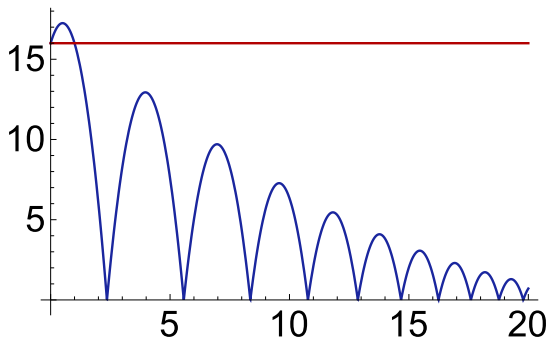
Example (▶ Bouncing Ball)

$$H = x \geq 0 \wedge g > 0 \rightarrow \left[\left(\{x' = v, v' = -g \mid x \geq 0\}; \right. \right. \\ \left. \left. \text{if } (x = 0) v := -cv \right)^* \right] 0 \leq x \leq H$$



Example (▶ Bouncing Ball)

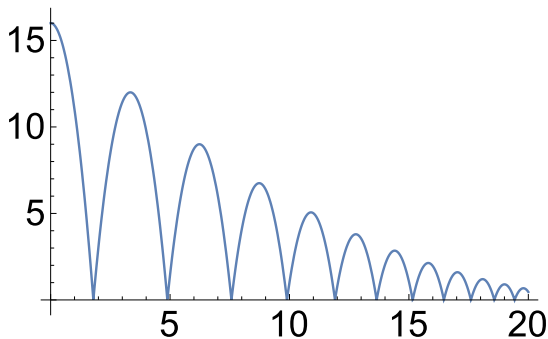
$$1 \geq c \geq 0 \wedge H = x \geq 0 \wedge g > 0 \rightarrow \left[\left(\{x' = v, v' = -g \mid x \geq 0\}; \right. \right. \\ \left. \left. \text{if}(x = 0) v := -cv \right)^* \right] 0 \leq x \leq H$$



Not if $v > 0$ initial climbing

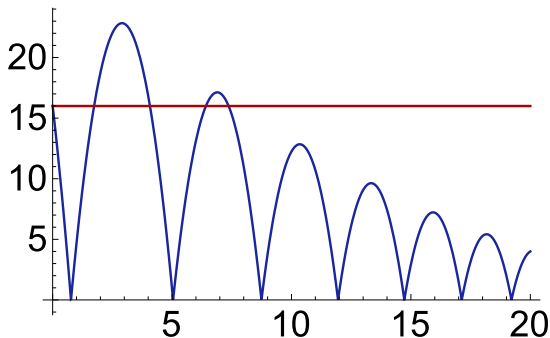
Example (▶ Bouncing Ball)

$$1 \geq c \geq 0 \wedge H = x \geq 0 \wedge g > 0 \rightarrow \left[\left(\{x' = v, v' = -g \wedge x \geq 0\}; \right. \right. \\ \left. \left. \text{if}(x = 0) v := -cv \right)^* \right] 0 \leq x \leq H$$



Example (▶ Bouncing Ball)

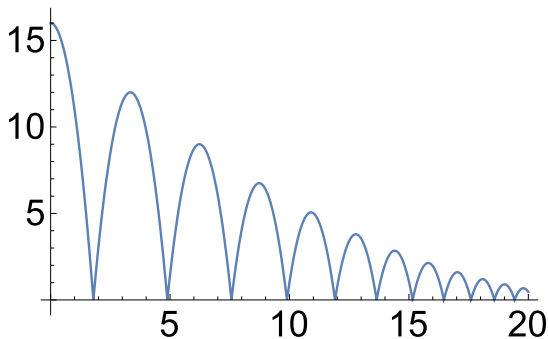
$$v \leq 0 \wedge 1 \geq c \geq 0 \wedge H = x \geq 0 \wedge g > 0 \rightarrow \left[\left(\{x' = v, v' = -g \ \& \ x \geq 0\}; \right. \right. \\ \left. \left. \text{if}(x = 0) \ v := -cv \right)^* \right] 0 \leq x \leq H$$



Not if $v \ll 0$ initial dribbling

Example (▶ Bouncing Ball)

$$v \leq 0 \wedge 1 \geq c \geq 0 \wedge H = x \geq 0 \wedge g > 0 \rightarrow \left[\left(\{x' = v, v' = -g \wedge x \geq 0\}; \right. \right. \\ \left. \left. \text{if}(x = 0) v := -cv \right)^* \right] 0 \leq x \leq H$$



Example (▶ Bouncing Ball)

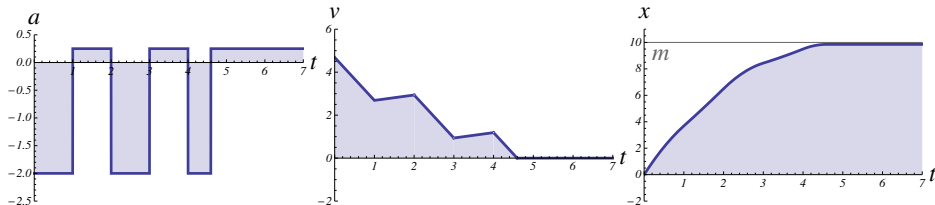
$$v=0 \wedge 1 \geq c \geq 0 \wedge H=x \geq 0 \wedge g > 0 \rightarrow \left[\left(\{x' = v, v' = -g \ \& \ x \geq 0\}; \right. \right. \\ \left. \left. \text{if}(x = 0) \ v := -cv \right)^* \right] \ 0 \leq x \leq H$$

Acceleration condition ?Q



Example (Single car car_s)

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



$Q \equiv$

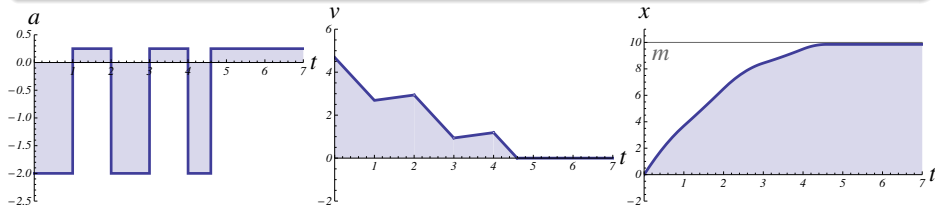


Example (Single car car_ε time-triggered)

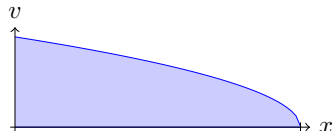
$$(((?Q; a := A) \cup a := -b); t := 0; \{x' = v, v' = a, t' = 1 \& v \geq 0 \wedge t \leq \varepsilon\})^*$$

Example (Safely stays before traffic light m)

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



$Q \equiv$

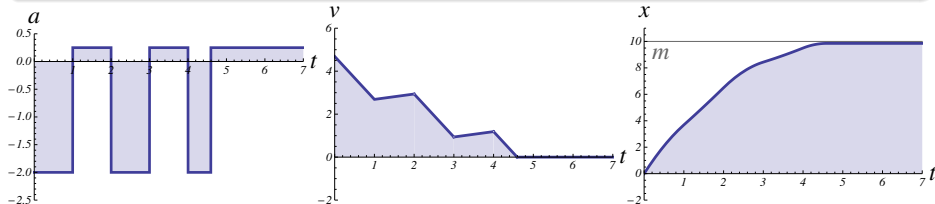


Example (Single car car_ε time-triggered)

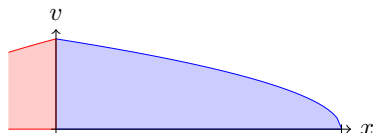
$$(((?Q; a := A) \cup a := -b); t := 0; \{x' = v, v' = a, t' = 1 \& v \geq 0 \wedge t \leq \varepsilon\})^*$$

Example (Safely stays before traffic light m)

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



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

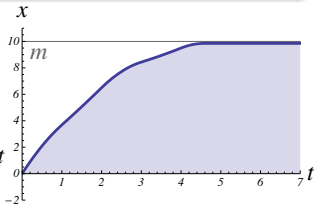
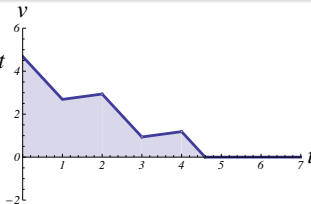
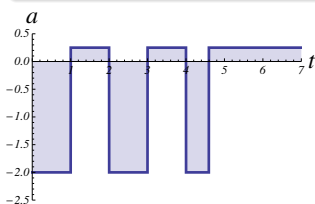


Example (Single car car_ε time-triggered)

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

Example (Safely stays before traffic light m)

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



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

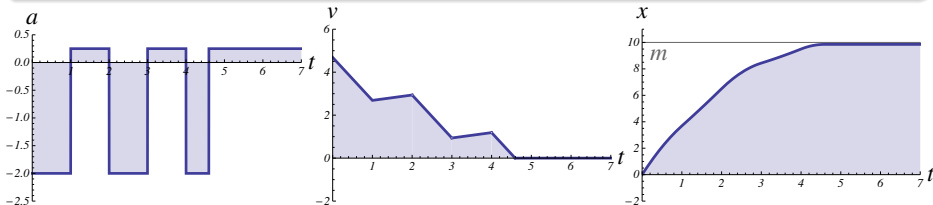


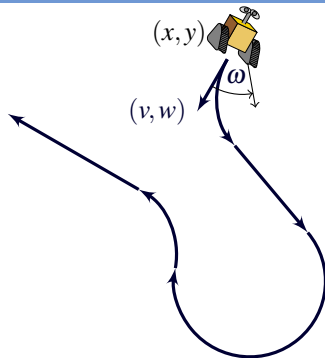
Example (Single car car_ε time-triggered)

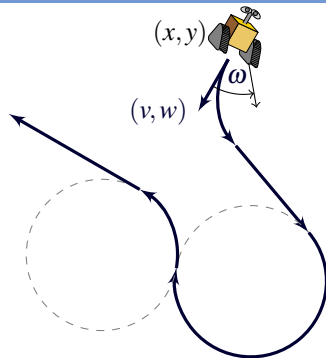
$$(((?Q; a := A) \cup a := -b); t := 0; \{x' = v, v' = a, t' = 1 \& v \geq 0 \wedge t \leq \varepsilon\})^*$$

Example (Live, can move everywhere)

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

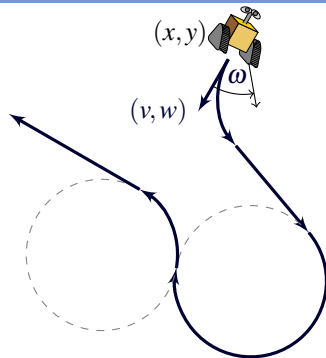






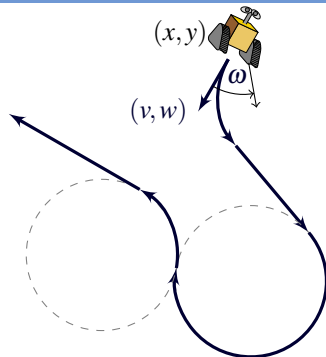
Example (Runaround Robot)

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



Example (Runaround Robot)

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

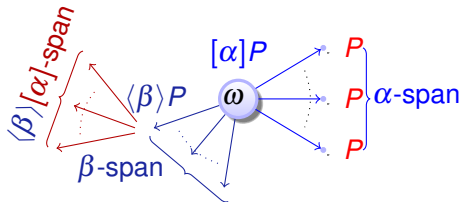


Example (Runaround Robot)

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

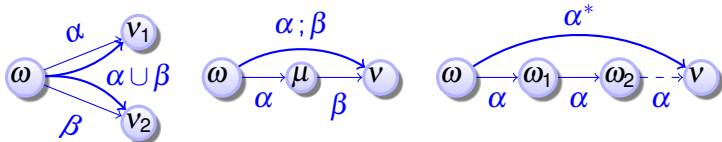
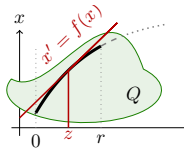
Definition (Differential dynamic logic)

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



Definition (Hybrid program)

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

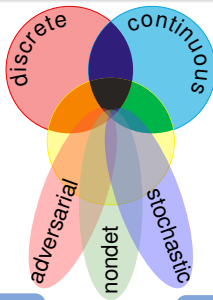


- 1 CPS are Multi-Dynamical Systems
- 2 CPS Programs
 - Syntax
 - Semantics
 - Examples
- 3 Differential Dynamic Logic
 - Syntax
 - Semantics
 - Example: Car Control Design
- 4 Dynamic Axioms for Dynamical Systems**
 - Axiomatics**
 - dL Proofs in KeYmaera X**
- 5 Differential Invariants for Differential Equations
 - Axiomatics
 - Examples
- 6 Summary

CPSs are Multi-Dynamical Systems

CPS Dynamics

CPS are characterized by multiple facets of dynamical systems.



CPS Compositions

CPS combines multiple simple dynamical effects.

Descriptive simplification

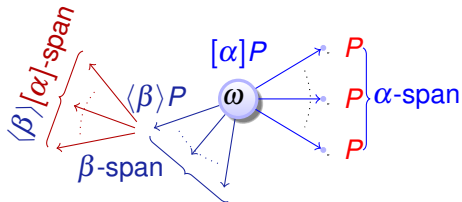
Tame Parts

Exploiting compositionality tames CPS complexity.

Analytic simplification

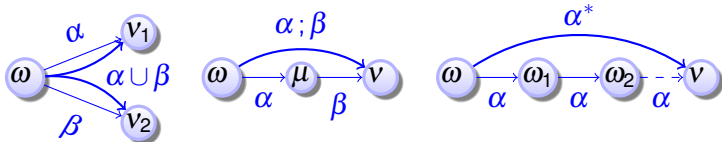
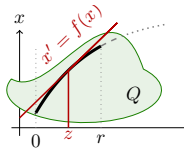
Definition (Differential dynamic logic)

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

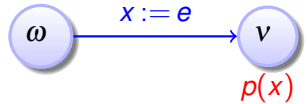


Definition (Hybrid program)

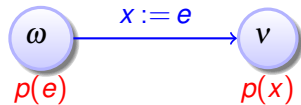
$$\alpha, \beta ::= x := e \mid ?Q \mid x' = f(x) \ \& \ Q \mid \alpha \cup \beta \mid \alpha; \beta \mid \alpha^*$$



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

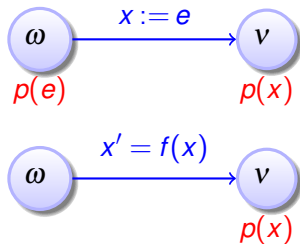


$$[:=] [x := e]p(x) \leftrightarrow p(e)$$



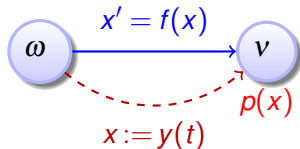
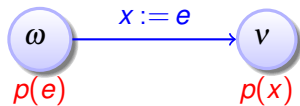
$$[:=] \quad [x := e]p(x) \leftrightarrow p(e)$$

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



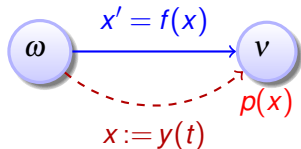
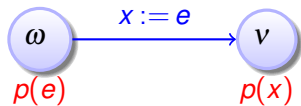
$$[:=] [x := e]p(x) \leftrightarrow p(e)$$

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



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

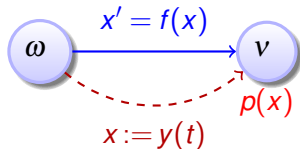
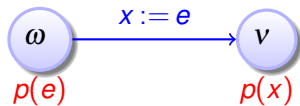
$$['] [x' = f(x)]p(x) \leftrightarrow \forall t \geq 0 [x := y(t)]p(x)$$



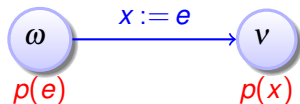
$$[:=] [x := e]p(x) \leftrightarrow p(e)$$

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

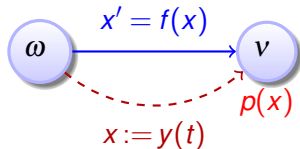
$$['] [x' = f(x) \& q(x)]p(x) \leftrightarrow \forall t \geq 0 ([x := y(t)]p(x))$$



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

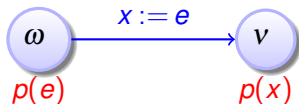


$$['] [x' = f(x)]p(x) \leftrightarrow \forall t \geq 0 [x := y(t)]p(x)$$

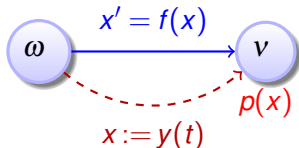


$$['] [x' = f(x) \& q(x)]p(x) \leftrightarrow \forall t \geq 0 (\forall 0 \leq s \leq t q(y(s)) \rightarrow [x := y(t)]p(x))$$

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



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



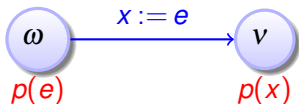
$$['] [x' = f(x) \& q(x)]p(x) \leftrightarrow \forall t \geq 0 (\forall 0 \leq s \leq t q(y(s)) \rightarrow [x := y(t)]p(x))$$

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

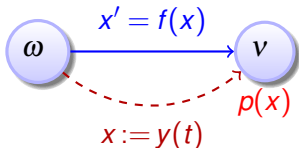


if $\omega \in \llbracket Q \rrbracket$

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



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



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

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

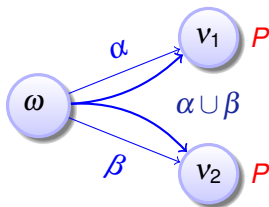


if $\omega \in \llbracket Q \rrbracket$

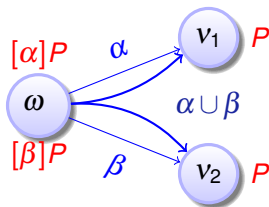


compositional semantics $\Rightarrow$ compositional proofs

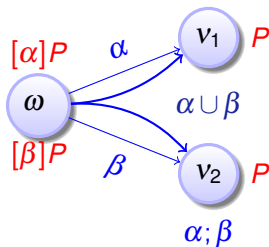
$[\cup] [\alpha \cup \beta] P \leftrightarrow$



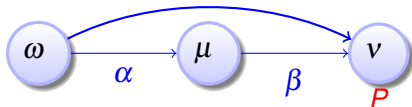
$$[\cup] \quad [\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$$



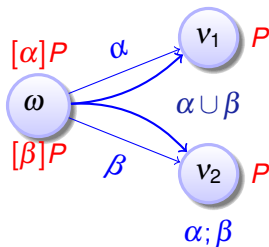
$$[\cup] \quad [\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$$



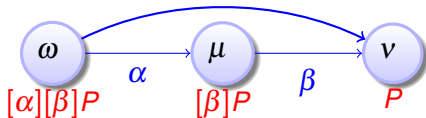
$$[;] \quad [\alpha; \beta]P \leftrightarrow$$



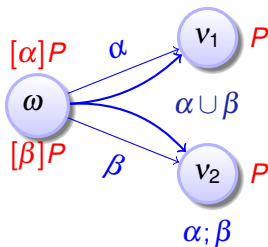
$$[\cup] \quad [\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$$



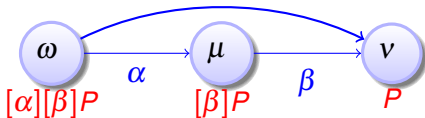
$$[;] \quad [\alpha; \beta]P \leftrightarrow [\alpha][\beta]P$$



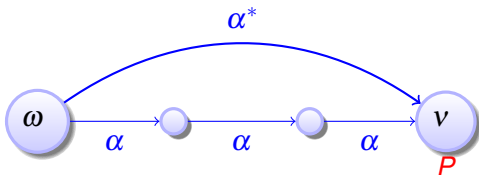
$$[\cup] \quad [\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$$



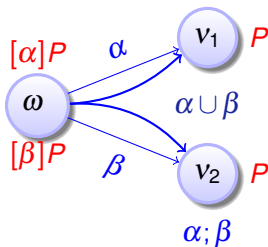
$$[;] \quad [\alpha; \beta]P \leftrightarrow [\alpha][\beta]P$$



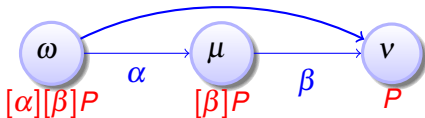
$$[*] \quad [\alpha^*]P \leftrightarrow$$



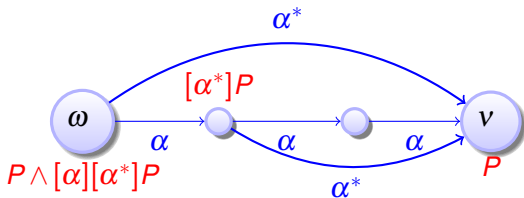
$$[\cup] \quad [\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$$



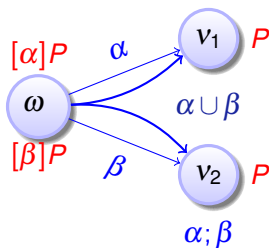
$$[;] \quad [\alpha; \beta]P \leftrightarrow [\alpha][\beta]P$$



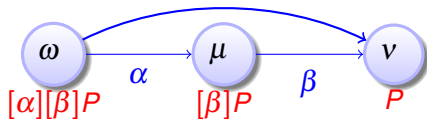
$$[*] \quad [\alpha^*]P \leftrightarrow P \wedge [\alpha][\alpha^*]P$$



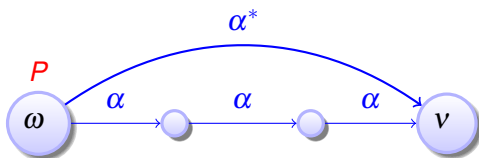
$$[\cup] \quad [\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$$



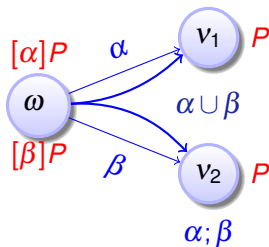
$$[;] \quad [\alpha; \beta]P \leftrightarrow [\alpha][\beta]P$$



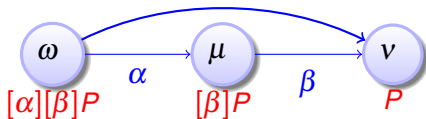
$$| \quad [\alpha^*]P \leftrightarrow P \wedge$$



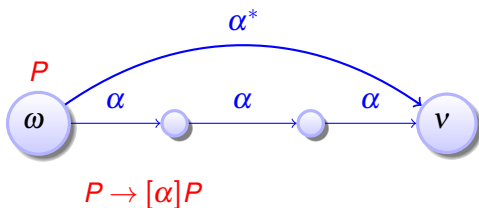
$$[\cup] \quad [\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$$



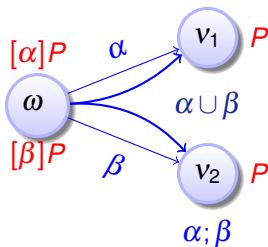
$$[;] \quad [\alpha; \beta]P \leftrightarrow [\alpha][\beta]P$$



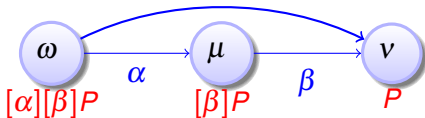
$$I \quad [\alpha^*]P \leftrightarrow P \wedge (P \rightarrow [\alpha]P)$$



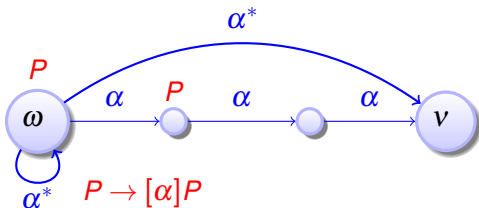
$$[\cup] \quad [\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$$



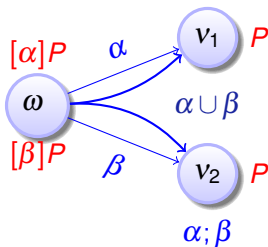
$$[;] \quad [\alpha; \beta]P \leftrightarrow [\alpha][\beta]P$$



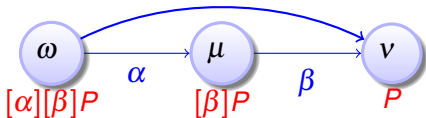
$$! \quad [\alpha^*]P \leftrightarrow P \wedge [\alpha^*](P \rightarrow [\alpha]P)$$



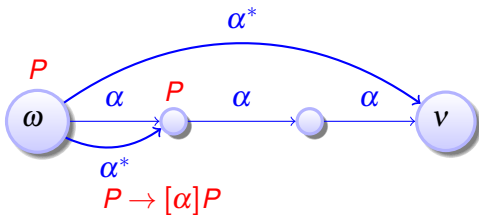
$$[\cup] \quad [\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$$



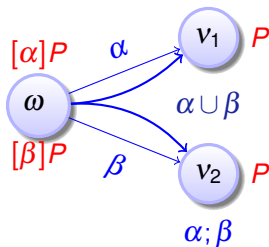
$$[;] \quad [\alpha; \beta]P \leftrightarrow [\alpha][\beta]P$$



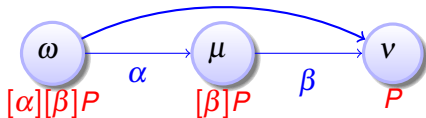
$$I \quad [\alpha^*]P \leftrightarrow P \wedge [\alpha^*](P \rightarrow [\alpha]P)$$



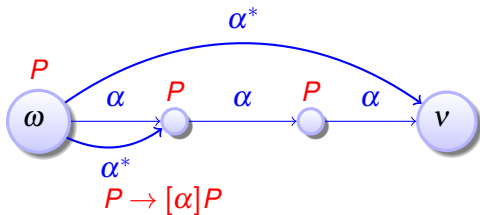
$$[\cup] [\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$$



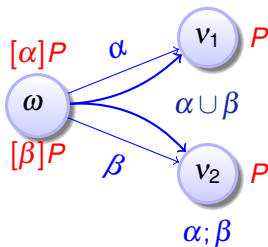
$$[;] [\alpha; \beta]P \leftrightarrow [\alpha][\beta]P$$



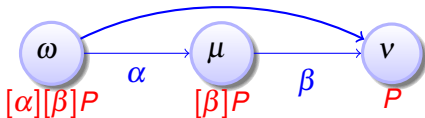
$$[\alpha^*]P \leftrightarrow P \wedge [\alpha^*](P \rightarrow [\alpha]P)$$



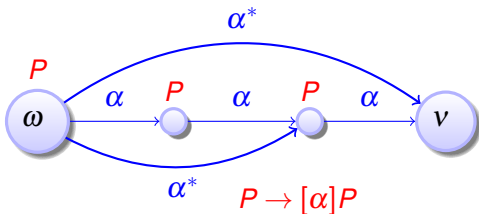
$$[\cup] \quad [\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$$



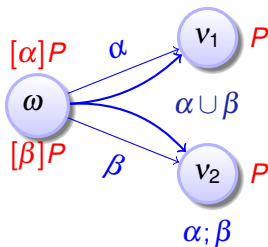
$$[;] \quad [\alpha; \beta]P \leftrightarrow [\alpha][\beta]P$$



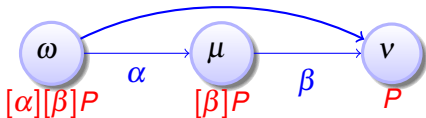
$$! \quad [\alpha^*]P \leftrightarrow P \wedge [\alpha^*](P \rightarrow [\alpha]P)$$



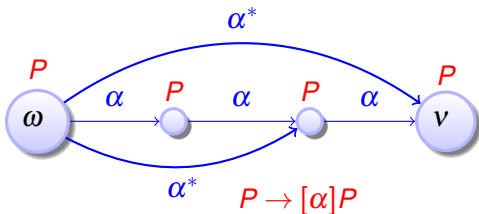
$$[\cup] \quad [\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$$



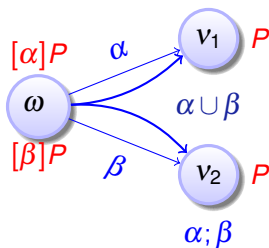
$$[;] \quad [\alpha; \beta]P \leftrightarrow [\alpha][\beta]P$$



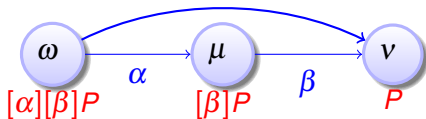
$$I \quad [\alpha^*]P \leftrightarrow P \wedge [\alpha^*](P \rightarrow [\alpha]P)$$



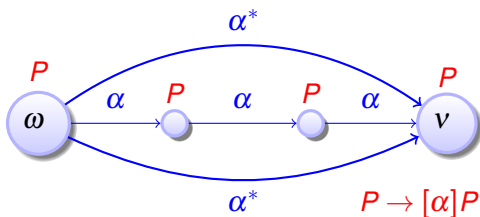
$$[\cup] \quad [\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$$



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



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



Proof Rule: Loop Invariants

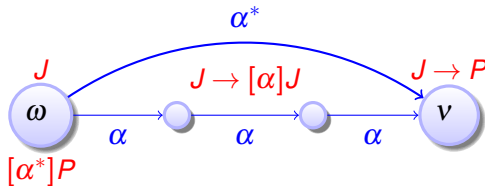
$$\text{G} \frac{P}{[\alpha]P}$$

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

$$\text{M}[\cdot] \frac{P \rightarrow Q}{[\alpha]P \rightarrow [\alpha]Q}$$

Lemma (Loop invariant rule is derived syntactically)

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



Sequent notation $\Gamma \rightarrow \Delta$ means $(\bigwedge_{A \in \Gamma} A) \rightarrow (\bigvee_{B \in \Delta} B)$ for sets Γ, Δ

Proof Rule: Loop Invariants

$$\text{G} \frac{P}{[\alpha]P}$$

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

$$\text{M}[\cdot] \frac{P \rightarrow Q}{[\alpha]P \rightarrow [\alpha]Q}$$

Lemma (Loop invariant rule is derived syntactically)

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

Proof (Derived rule).

$$\text{cut} \frac{\Gamma \rightarrow J, \Delta \quad \text{I} \frac{\text{G} \frac{J \rightarrow [\alpha]J}{J \rightarrow J \wedge [\alpha^*](J \rightarrow [\alpha]J)}}{J \rightarrow [\alpha^*]J}}{\Gamma \rightarrow [\alpha^*]P, \Delta} \quad \text{M}[\cdot] \frac{J \rightarrow P}{[\alpha^*]J \rightarrow [\alpha^*]P}$$



Proof Rule: Loop Invariants

$$\text{G} \frac{P}{[\alpha]P}$$

$$\text{I} \quad [\alpha^*]P \leftrightarrow P \wedge [\alpha^*](P \rightarrow [\alpha]P)$$

$$\text{M}[\cdot] \frac{P \rightarrow Q}{[\alpha]P \rightarrow [\alpha]Q}$$

Lemma (Loop invariant rule is derived syntactically)

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

Proof (Derived rule).

$$\text{cut} \frac{\Gamma \rightarrow J, \Delta \quad \begin{array}{c} J \rightarrow [\alpha]J \\ \text{G} \frac{J \rightarrow J \wedge [\alpha^*](J \rightarrow [\alpha]J)}{J \rightarrow J \wedge [\alpha^*](J \rightarrow [\alpha]J)} \\ \text{I} \frac{J \rightarrow J \wedge [\alpha^*](J \rightarrow [\alpha]J)}{J \rightarrow [\alpha^*]J} \end{array}}{\Gamma \rightarrow [\alpha^*]P, \Delta} \quad \text{M}[\cdot] \frac{J \rightarrow P}{[\alpha^*]J \rightarrow [\alpha^*]P}$$

Finding invariant J can be a challenge.

Misplaced $[\alpha^*]$ suggests that J needs to carry along info about α^* history.



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

equations of truth

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

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

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

$$[:,] \quad [\alpha; \beta]P \leftrightarrow [\alpha][\beta]P$$

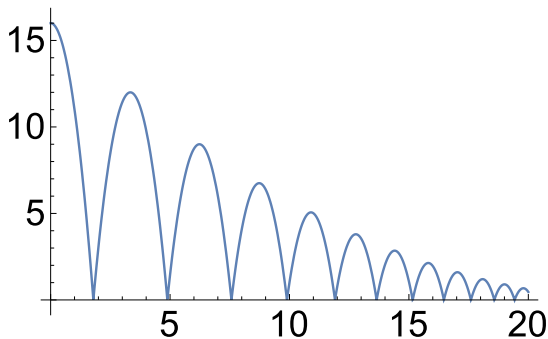
$$[*] \quad [\alpha^*]P \leftrightarrow P \wedge [\alpha][\alpha^*]P$$

$$\mathsf{K} \quad [\alpha](P \rightarrow Q) \rightarrow ([\alpha]P \rightarrow [\alpha]Q)$$

laws of logic of
laws of physics

$$\mathsf{I} \quad [\alpha^*]P \leftrightarrow P \wedge [\alpha^*](P \rightarrow [\alpha]P)$$

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



Example (▶ Bouncing Ball)

$$v=0 \wedge 1 \geq c \geq 0 \wedge H=x \geq 0 \wedge g>0 \rightarrow \left[\left(\{x' = v, v' = -g \ \& \ x \geq 0\}; \right. \right. \\ \left. \left. \text{if}(x = 0) \ v := -cv \right)^* \right] \ 0 \leq x \leq H$$

$$A \rightarrow [(\text{grav}; (?x=0; v := -cv \cup ?x \neq 0))^*] B_{(x,v)}$$

$$A \equiv 0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0$$

$$B_{(x,v)} \equiv 0 \leq x \wedge x \leq H$$

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

$$\text{loop} \frac{A \rightarrow j(x, v) \quad \frac{j(x, v) \rightarrow [\text{grav}; (?x=0; v := -cv \cup ?x \neq 0)] j(x, v) \quad j(x, v) \rightarrow B(x, v)}{A \rightarrow [(\text{grav}; (?x=0; v := -cv \cup ?x \neq 0))^*] B(x, v)}}{A \rightarrow [(\text{grav}; (?x=0; v := -cv \cup ?x \neq 0))^*] B(x, v)}$$

$$A \equiv 0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0$$

$$B(x, v) \equiv 0 \leq x \wedge x \leq H$$

$$\text{grav} \equiv \{x' = v, v' = -g \wedge x \geq 0\}$$

$$\begin{array}{c}
 \text{MR} \frac{j(x, v) \rightarrow [\text{grav}]j(x, v) \quad \text{loop} \frac{A \rightarrow j(x, v) \quad j(x, v) \rightarrow B(x, v)}{A \rightarrow \left((\text{grav}; (?x=0; v:=-cv \cup ?x \neq 0))^* \right) B(x, v)}}{j(x, v) \rightarrow [\text{grav}] \left((\text{grav}; (?x=0; v:=-cv \cup ?x \neq 0))^* \right) B(x, v)} \\
 \text{[?], } \rightarrow R \frac{[:=] \frac{j(x, v), x=0 \rightarrow [v:=-cv]j(x, v)}{j(x, v) \rightarrow [?x=0][v:=-cv]j(x, v)}}{j(x, v) \rightarrow [?x=0; v:=-cv]j(x, v)} \quad [?] \frac{j(x, v), x \neq 0 \rightarrow j(x, v)}{j(x, v) \rightarrow [?x \neq 0]j(x, v)} \\
 \wedge R \frac{j(x, v) \rightarrow [?x=0; v:=-cv]j(x, v) \wedge [?x \neq 0]j(x, v)}{j(x, v) \rightarrow [?x=0; v:=-cv \cup ?x \neq 0]j(x, v)} \\
 \text{[?], } \rightarrow R \frac{j(x, v) \rightarrow [?x=0; v:=-cv \cup ?x \neq 0]j(x, v)}{j(x, v) \rightarrow [\text{grav}] [?x=0; v:=-cv \cup ?x \neq 0]j(x, v)} \\
 \text{[?], } \rightarrow R \frac{j(x, v) \rightarrow [\text{grav}] [?x=0; v:=-cv \cup ?x \neq 0]j(x, v)}{j(x, v) \rightarrow [\text{grav}; (?x=0; v:=-cv \cup ?x \neq 0)]j(x, v)} \\
 \text{[?], } \rightarrow R \frac{j(x, v) \rightarrow [\text{grav}; (?x=0; v:=-cv \cup ?x \neq 0)]j(x, v)}{j(x, v) \rightarrow [\text{grav}; (?x=0; v:=-cv \cup ?x \neq 0)]^* B(x, v)}
 \end{array}$$

$$A \equiv 0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0$$

$$B(x, v) \equiv 0 \leq x \wedge x \leq H$$

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

$$A \rightarrow j(x, v)$$

$$j(x, v) \rightarrow [\text{grav}](j(x, v))$$

$$j(x, v), x = 0 \rightarrow j(x, (-cv))$$

$$j(x, v), x \neq 0 \rightarrow j(x, v)$$

$$j(x, v) \rightarrow B(x, v)$$

$$A \equiv 0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0$$

$$B(x, v) \equiv 0 \leq x \wedge x \leq H$$

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

$$0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0 \rightarrow j(x, v)$$

$$j(x, v) \rightarrow [\{x' = v, v' = -g \ \& \ x \geq 0\}](j(x, v))$$

$$j(x, v), x = 0 \rightarrow j(x, (-cv))$$

$$j(x, v), x \neq 0 \rightarrow j(x, v)$$

$$j(x, v) \rightarrow 0 \leq x \wedge x \leq H$$

$$A \equiv 0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0$$

$$B(x, v) \equiv 0 \leq x \wedge x \leq H$$

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

$$0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0 \rightarrow j(x, v)$$

$$j(x, v) \rightarrow [\{x' = v, v' = -g \ \& \ x \geq 0\}](j(x, v))$$

$$j(x, v), x = 0 \rightarrow j(x, (-cv))$$

$$j(x, v), x \neq 0 \rightarrow j(x, v)$$

$$j(x, v) \rightarrow 0 \leq x \wedge x \leq H$$

2 $j(x, v) \equiv 0 \leq x \wedge x \leq H$

$$A \equiv 0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0$$

$$B(x, v) \equiv 0 \leq x \wedge x \leq H$$

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

$$0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0 \rightarrow j(x, v)$$

$$j(x, v) \rightarrow \{ \{ x' = v, v' = -g \ \& \ x \geq 0 \} \} (j(x, v))$$

$$j(x, v), x = 0 \rightarrow j(x, (-cv))$$

$$j(x, v), x \neq 0 \rightarrow j(x, v)$$

$$j(x, v) \rightarrow 0 \leq x \wedge x \leq H$$

2 $j(x, v) \equiv 0 \leq x \wedge x \leq H$

weak: fails ODE if $v \gg 0$

$$A \equiv 0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0$$

$$B(x, v) \equiv 0 \leq x \wedge x \leq H$$

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

$$0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0 \rightarrow j(x, v)$$

$$j(x, v) \rightarrow \{x' = v, v' = -g \wedge x \geq 0\}(j(x, v))$$

$$j(x, v), x = 0 \rightarrow j(x, (-cv))$$

$$j(x, v), x \neq 0 \rightarrow j(x, v)$$

$$j(x, v) \rightarrow 0 \leq x \wedge x \leq H$$

$$1 \quad j(x, v) \equiv x \geq 0$$

$$2 \quad j(x, v) \equiv 0 \leq x \wedge x \leq H$$

weak: fails ODE if $v \gg 0$

$$A \equiv 0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0$$

$$B(x, v) \equiv 0 \leq x \wedge x \leq H$$

$$\text{grav} \equiv \{x' = v, v' = -g \wedge x \geq 0\}$$

$$0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0 \rightarrow j(x, v)$$

$$j(x, v) \rightarrow [\{x' = v, v' = -g \& x \geq 0\}](j(x, v))$$

$$j(x, v), x = 0 \rightarrow j(x, (-cv))$$

$$j(x, v), x \neq 0 \rightarrow j(x, v)$$

$$j(x, v) \rightarrow 0 \leq x \wedge x \leq H$$

$$1 \quad j(x, v) \equiv x \geq 0$$

weaker: fails postcondition if $x > H$

$$2 \quad j(x, v) \equiv 0 \leq x \wedge x \leq H$$

weak: fails ODE if $v \gg 0$

$$A \equiv 0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0$$

$$B(x, v) \equiv 0 \leq x \wedge x \leq H$$

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

$$0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0 \rightarrow j(x, v)$$

$$j(x, v) \rightarrow [\{x' = v, v' = -g \& x \geq 0\}](j(x, v))$$

$$j(x, v), x = 0 \rightarrow j(x, (-cv))$$

$$j(x, v), x \neq 0 \rightarrow j(x, v)$$

$$j(x, v) \rightarrow 0 \leq x \wedge x \leq H$$

$$1 \quad j(x, v) \equiv x \geq 0$$

weaker: fails postcondition if $x > H$

$$2 \quad j(x, v) \equiv 0 \leq x \wedge x \leq H$$

weak: fails ODE if $v \gg 0$

$$3 \quad j(x, v) \equiv x = 0 \wedge v = 0$$

$$A \equiv 0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0$$

$$B(x, v) \equiv 0 \leq x \wedge x \leq H$$

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

$$0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0 \rightarrow j(x, v)$$

$$j(x, v) \rightarrow [\{x' = v, v' = -g \ \& \ x \geq 0\}](j(x, v))$$

$$j(x, v), x = 0 \rightarrow j(x, (-cv))$$

$$j(x, v), x \neq 0 \rightarrow j(x, v)$$

$$j(x, v) \rightarrow 0 \leq x \wedge x \leq H$$

$$1 \quad j(x, v) \equiv x \geq 0$$

weaker: fails postcondition if $x > H$

$$2 \quad j(x, v) \equiv 0 \leq x \wedge x \leq H$$

weak: fails ODE if $v \gg 0$

$$3 \quad j(x, v) \equiv x = 0 \wedge v = 0$$

strong: fails initial condition if $x > 0$

$$A \equiv 0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0$$

$$B(x, v) \equiv 0 \leq x \wedge x \leq H$$

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

$$0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0 \rightarrow j(x, v)$$

$$j(x, v) \rightarrow [\{x' = v, v' = -g \& x \geq 0\}](j(x, v))$$

$$j(x, v), x = 0 \rightarrow j(x, (-cv))$$

$$j(x, v), x \neq 0 \rightarrow j(x, v)$$

$$j(x, v) \rightarrow 0 \leq x \wedge x \leq H$$

$$① \quad j(x, v) \equiv x \geq 0$$

weaker: fails postcondition if $x > H$

$$② \quad j(x, v) \equiv 0 \leq x \wedge x \leq H$$

weak: fails ODE if $v \gg 0$

$$③ \quad j(x, v) \equiv x = 0 \wedge v = 0$$

strong: fails initial condition if $x > 0$

$$④ \quad j(x, v) \equiv x = 0 \vee x = H \wedge v = 0$$

no space for intermediate states

$$⑤ \quad j(x, v) \equiv 2gx = 2gH - v^2 \wedge x \geq 0$$

$$A \equiv 0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0$$

$$B(x, v) \equiv 0 \leq x \wedge x \leq H$$

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

$$0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0 \rightarrow j(x, v)$$

$$j(x, v) \rightarrow \{ \{ x' = v, v' = -g \ \& \ x \geq 0 \} \} (j(x, v))$$

$$j(x, v), x = 0 \rightarrow j(x, (-cv))$$

$$j(x, v), x \neq 0 \rightarrow j(x, v)$$

$$j(x, v) \rightarrow 0 \leq x \wedge x \leq H$$

$$① \quad j(x, v) \equiv x \geq 0$$

weaker: fails postcondition if $x > H$

$$② \quad j(x, v) \equiv 0 \leq x \wedge x \leq H$$

weak: fails ODE if $v \gg 0$

$$③ \quad j(x, v) \equiv x = 0 \wedge v = 0$$

strong: fails initial condition if $x > 0$

$$④ \quad j(x, v) \equiv x = 0 \vee x = H \wedge v = 0$$

no space for intermediate states

$$⑤ \quad j(x, v) \equiv 2gx = 2gH - v^2 \wedge x \geq 0$$

works: implicitly links v and x

$$A \equiv 0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0$$

$$B(x, v) \equiv 0 \leq x \wedge x \leq H$$

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

$$\begin{aligned}
&0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0 \rightarrow 2gx = 2gH - v^2 \wedge x \geq 0 \\
&2gx = 2gH - v^2 \wedge x \geq 0 \rightarrow [\{x' = v, v' = -g \ \& \ x \geq 0\}](2gx = 2gH - v^2 \wedge x \geq 0) \\
&2gx = 2gH - v^2 \wedge x \geq 0, x = 0 \rightarrow 2gx = 2gH - (-cv)^2 \wedge x \geq 0 \\
&2gx = 2gH - v^2 \wedge x \geq 0, x \neq 0 \rightarrow 2gx = 2gH - v^2 \wedge x \geq 0 \\
&2gx = 2gH - v^2 \wedge x \geq 0 \rightarrow 0 \leq x \wedge x \leq H
\end{aligned}$$

1

2

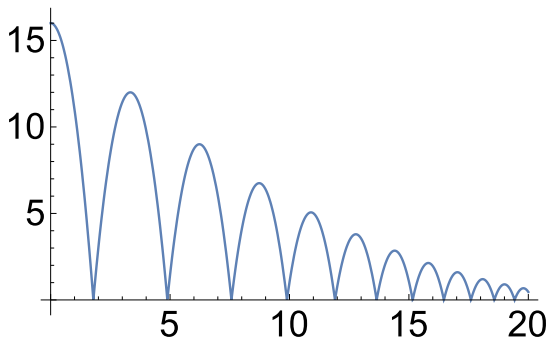
3

4

5

$$j_{(x,v)} \equiv 2gx = 2gH - v^2 \wedge x \geq 0$$

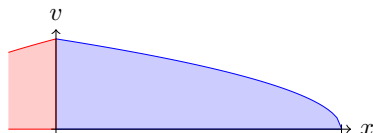
works: implicitly links v and x



Example (▶ Bouncing Ball)

$$v=0 \wedge 1 \geq c \geq 0 \wedge H=x \geq 0 \wedge g>0 \rightarrow \left[\left(\{x' = v, v' = -g \wedge x \geq 0\}; \right. \right. \\ \left. \left. \text{if}(x=0) v := -cv \right)^* \right] 0 \leq x \leq H$$

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

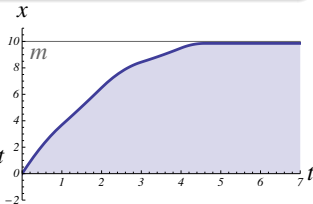
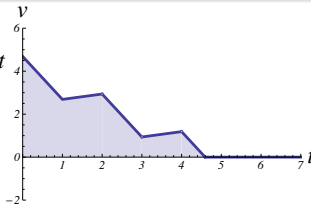
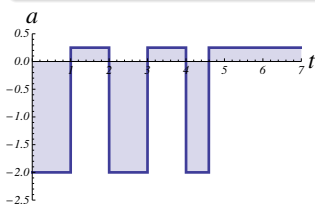


Example (Single car car_ε time-triggered)

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

Example (Safely stays before traffic light m)

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



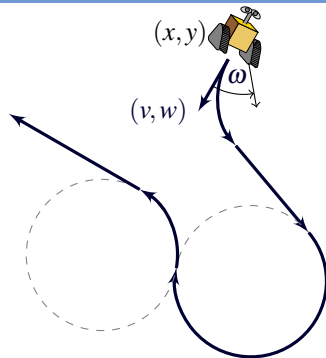
The lion's share of understanding comes from understanding what does change (variants/progress measures) and what doesn't change (invariants).

Invariants are a fundamental force of CS

Variants are another fundamental force of CS

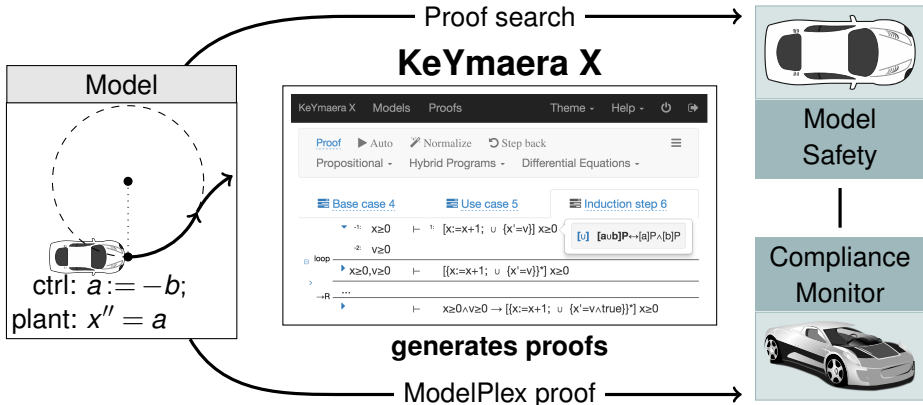
“Making something variable is easy.

Controlling duration of constancy is the trick.” – Alan J. Perlis



Example (Runaround Robot)

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



Trustworthy

Uniform substitution
Sound & complete
Small core: 1700 LOC

Flexible

Proof automation
Interactive UI
Programmable

Customizable

Scala+Java API
Command line
REST API

Theorem (Soundness)

replace all occurrences of $p(\cdot)$

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

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

i.e. bound variables $U = BV(\otimes(\cdot))$ of **no** operator $\otimes$

are free in the substitution on its argument θ

(U -admissible)

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

Theorem (Soundness)

replace all occurrences of $p(\cdot)$

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

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

i.e. bound variables $U = BV(\otimes(\cdot))$ of **no** operator $\otimes$
are free in the substitution on its argument θ

(U -admissible)

$$\frac{[v := f]p(v) \leftrightarrow p(f)}{[v := -x][x' = v]x \geq 0 \leftrightarrow [x' = -x]x \geq 0}$$

Theorem (Soundness)

replace all occurrences of $p(\cdot)$

Modular interface:
Prover vs. Logic

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

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

i.e. bound variables $U = BV(\otimes(\cdot))$ of **no** operator $\otimes$

are free in the substitution on its argument θ

(U -admissible)

If you bind a free variable, you go to logic jail!

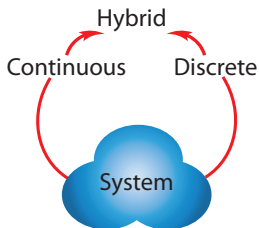
$$\frac{[v := f]p(v) \leftrightarrow p(f)}{[v := -x][x' = v]x \geq 0 \leftrightarrow [x' = -x]x \geq 0}$$

Clash

Theorem (Sound & Complete)

(JAR'08, LICS'12, JAR'17)

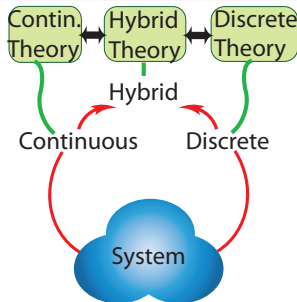
*dL calculus is a sound & complete axiomatization of hybrid systems relative to either differential equations **or** to discrete dynamics.*



Theorem (Sound & Complete)

(JAR'08, LICS'12, JAR'17)

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



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

equations of truth

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

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

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

$$[:,] \quad [\alpha; \beta]P \leftrightarrow [\alpha][\beta]P$$

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

$$\mathsf{K} \quad [\alpha](P \rightarrow Q) \rightarrow ([\alpha]P \rightarrow [\alpha]Q)$$

laws of logic of
laws of physics

$$\mathsf{I} \quad [\alpha^*]P \leftrightarrow P \wedge [\alpha^*](P \rightarrow [\alpha]P)$$

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

- 1 CPS are Multi-Dynamical Systems
- 2 CPS Programs
 - Syntax
 - Semantics
 - Examples
- 3 Differential Dynamic Logic
 - Syntax
 - Semantics
 - Example: Car Control Design
- 4 Dynamic Axioms for Dynamical Systems
 - Axiomatics
 - dL Proofs in KeYmaera X
- 5 Differential Invariants for Differential Equations**
 - Axiomatics**
 - Examples**
- 6 Summary

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

equations of truth

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

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

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

$$[:,] \quad [\alpha; \beta]P \leftrightarrow [\alpha][\beta]P$$

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

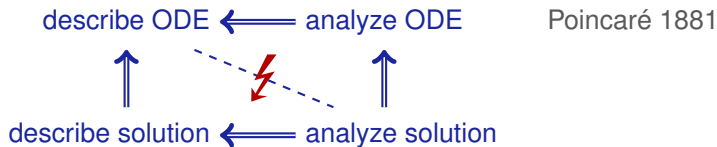
$$\mathsf{K} \quad [\alpha](P \rightarrow Q) \rightarrow ([\alpha]P \rightarrow [\alpha]Q)$$

laws of logic of
laws of physics

$$\mathsf{I} \quad [\alpha^*]P \leftrightarrow P \wedge [\alpha^*](P \rightarrow [\alpha]P)$$

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

- Classical approach: ① Given ODE ② Solve ODE ③ Analyze solution
- Descriptive power of ODEs: ODE much easier than its solution
- ⚡ Analyzing ODEs via their solutions undoes their descriptive power!



- ① Logical foundations of differential equation invariants LICS'18
- ② Decide invariance by dL proof

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

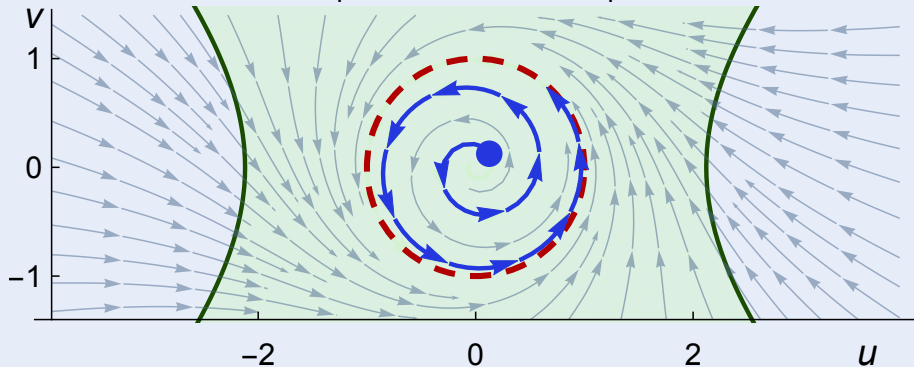
$$x''(t) = e^{t^2} \quad \text{has no elementary closed-form solution}$$

Concept (Differential Dynamic Logic)

(JAR'08,LICS'12)

$$u^2 \leq v^2 + \frac{9}{2} \rightarrow [u' = -v + \frac{u}{4}(1-u^2-v^2), v' = u + \frac{v}{4}(1-u^2-v^2)] u^2 \leq v^2 + \frac{9}{2}$$

$$u^2 + v^2 = 1 \rightarrow [u' = -v + \frac{u}{4}(1-u^2-v^2), v' = u + \frac{v}{4}(1-u^2-v^2)] u^2 + v^2 = 1$$

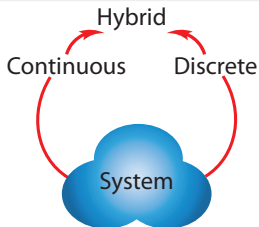


Theorem (Invariant Completeness) (LICS'18)

dL calculus is a sound & complete axiomatization of arithmetic invariants of differential equations. They are decidable with a derived axiom.

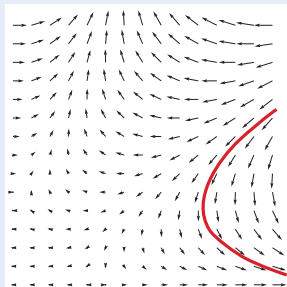
Theorem (Sound & Complete) (JAR'08, LICS'12, JAR'17)

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

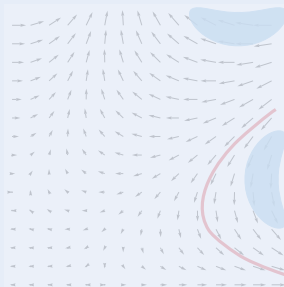


Differential Invariants for Differential Equations

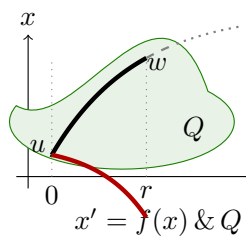
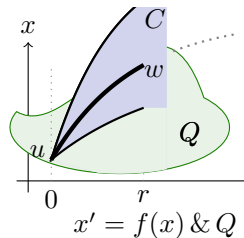
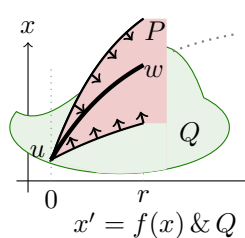
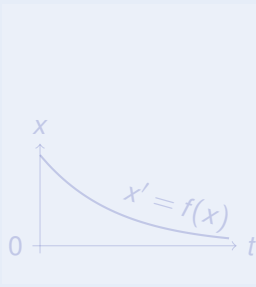
Differential Invariant



Differential Cut

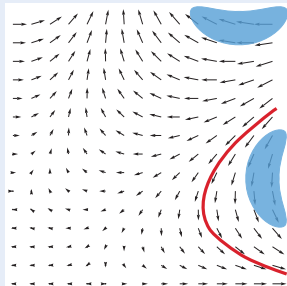


Differential Ghost

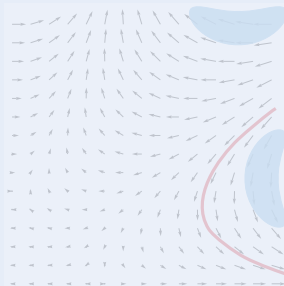


Differential Invariants for Differential Equations

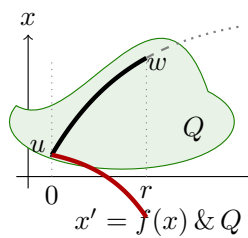
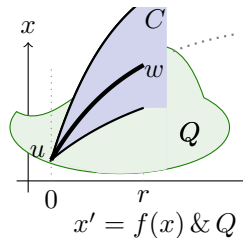
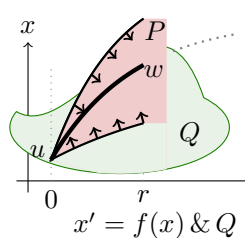
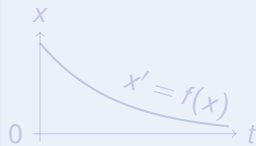
Differential Invariant



Differential Cut

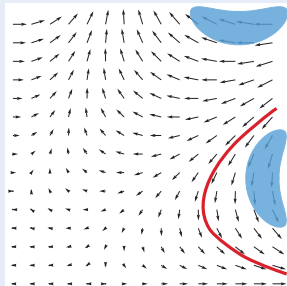


Differential Ghost

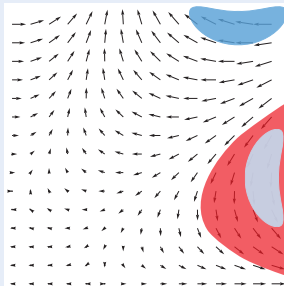


Differential Invariants for Differential Equations

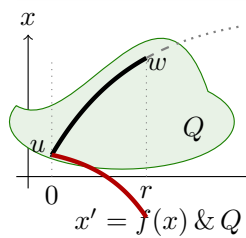
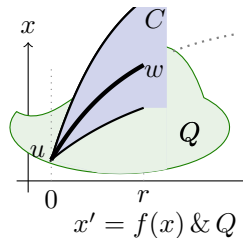
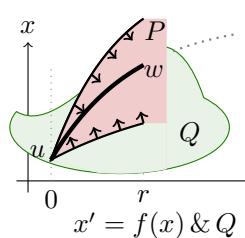
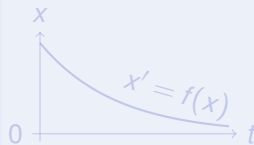
Differential Invariant



Differential Cut

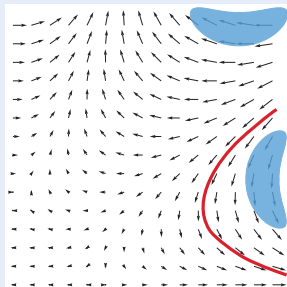


Differential Ghost

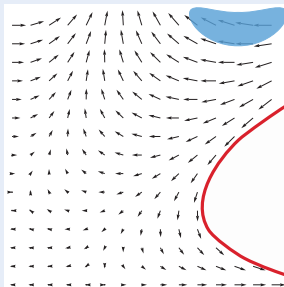


Differential Invariants for Differential Equations

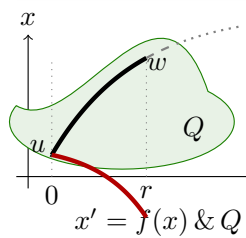
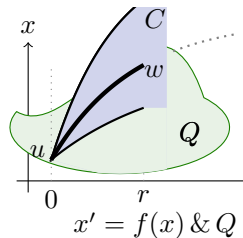
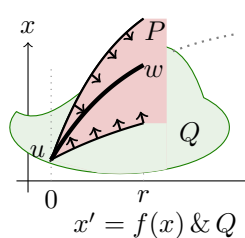
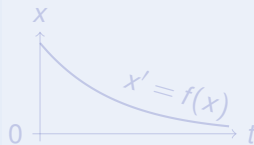
Differential Invariant



Differential Cut

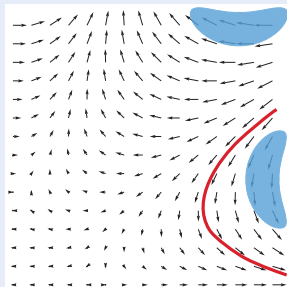


Differential Ghost

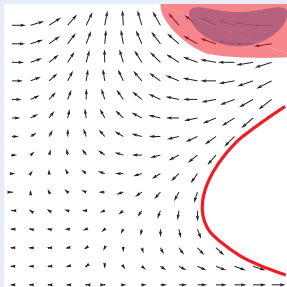


Differential Invariants for Differential Equations

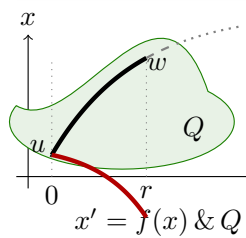
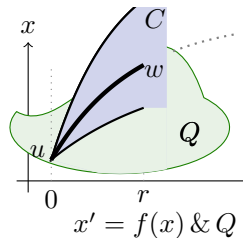
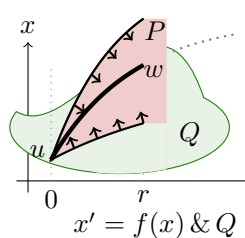
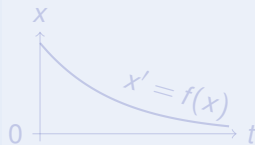
Differential Invariant



Differential Cut

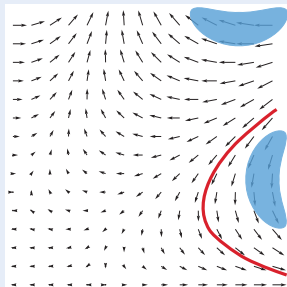


Differential Ghost

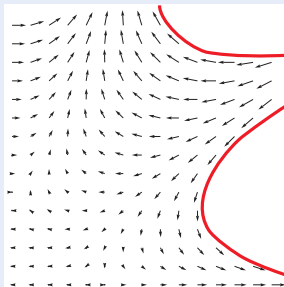


Differential Invariants for Differential Equations

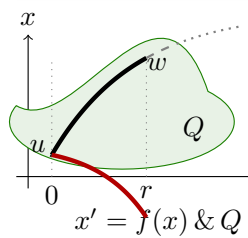
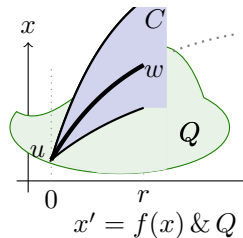
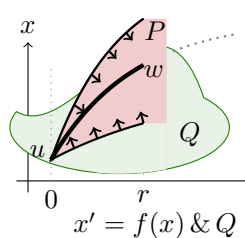
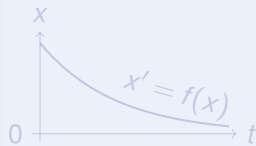
Differential Invariant



Differential Cut

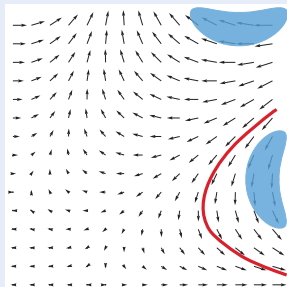


Differential Ghost

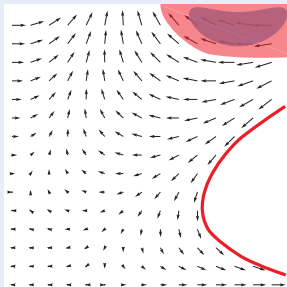


Differential Invariants for Differential Equations

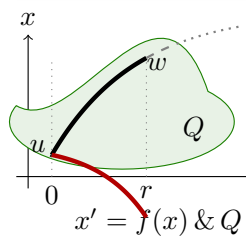
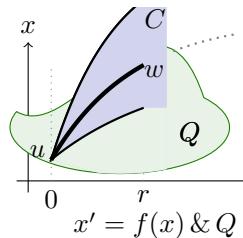
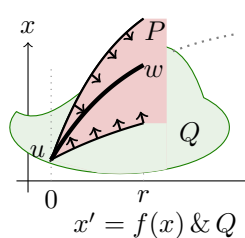
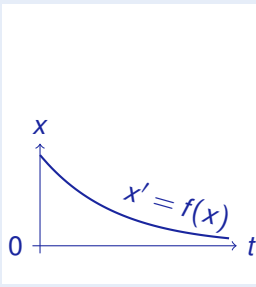
Differential Invariant



Differential Cut

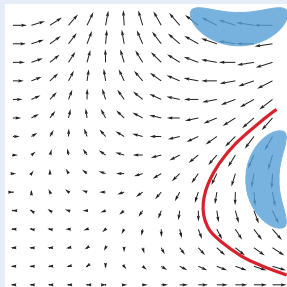


Differential Ghost

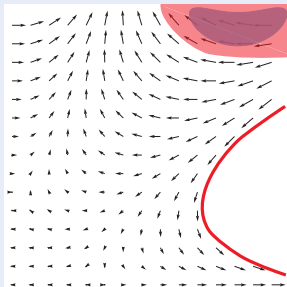


Differential Invariants for Differential Equations

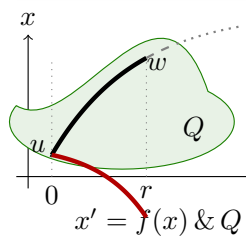
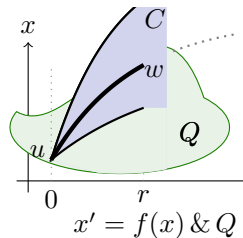
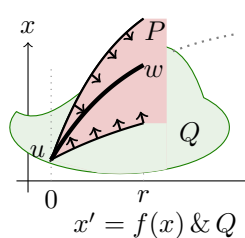
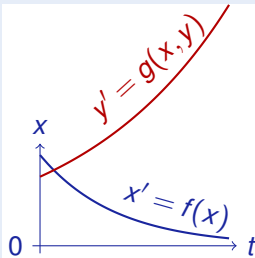
Differential Invariant



Differential Cut

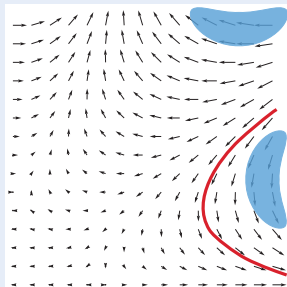


Differential Ghost

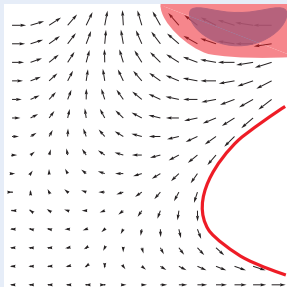


Differential Invariants for Differential Equations

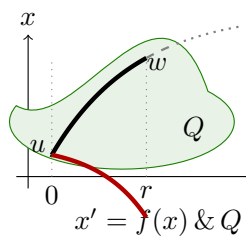
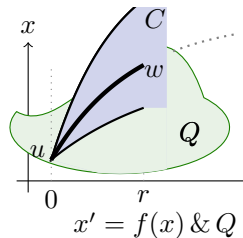
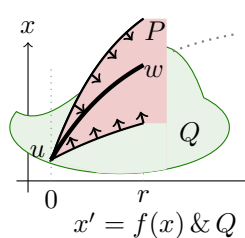
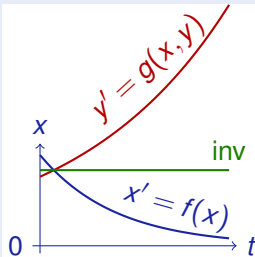
Differential Invariant



Differential Cut



Differential Ghost





Differential Invariants for Differential Equations

Differential Invariant

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

Differential Cut

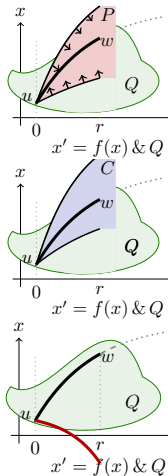
$$\frac{P \rightarrow [x' = f(x) \ \& \ Q]C \quad P \rightarrow [x' = f(x) \ \& \ Q \wedge C]P}{P \rightarrow [x' = f(x) \ \& \ Q]P}$$

Differential Ghost

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

deductive power added $DI \prec DI+DC \prec DI+DC+DG$

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





Differential Invariants for Differential Equations

Differential Invariant

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

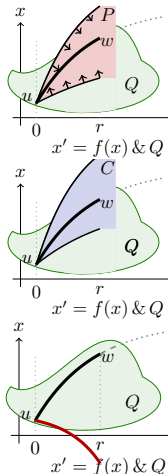
Differential Cut

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

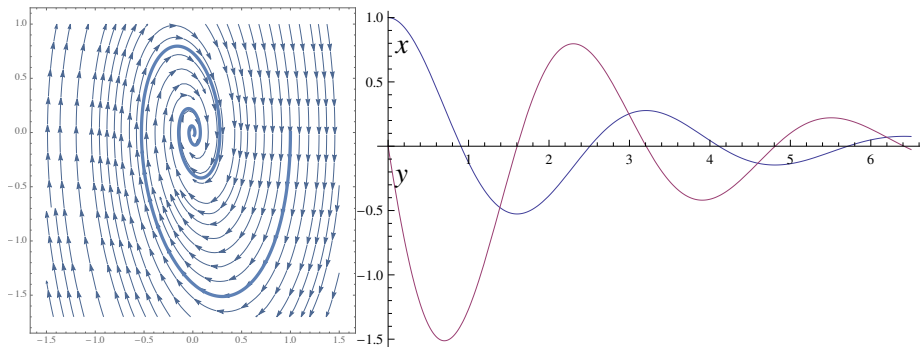
Differential Ghost

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

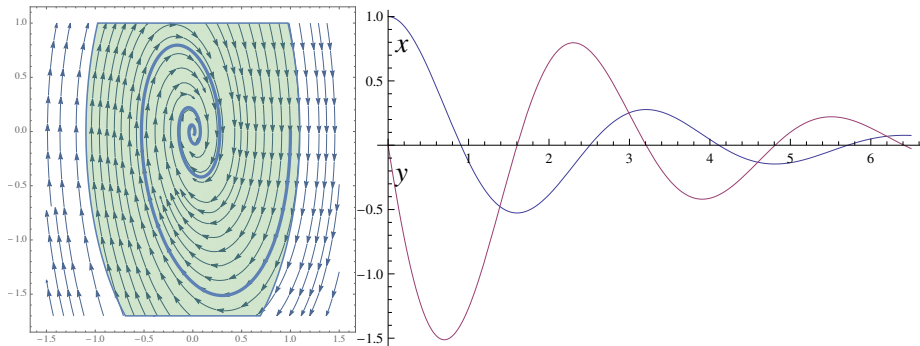
if $g(x, y) = a(x)y + b(x)$, so has long solution!



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



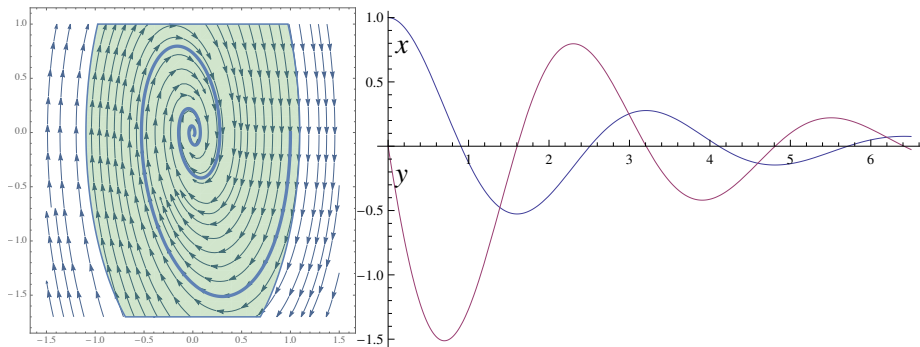
$$\omega^2 x^2 + y^2 \leq c^2 \rightarrow [x' = y, y' = -\omega^2 x - 2d\omega y \ \& \ \omega \geq 0 \wedge d \geq 0] \ \omega^2 x^2 + y^2 \leq c^2$$



damped oscillator

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

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

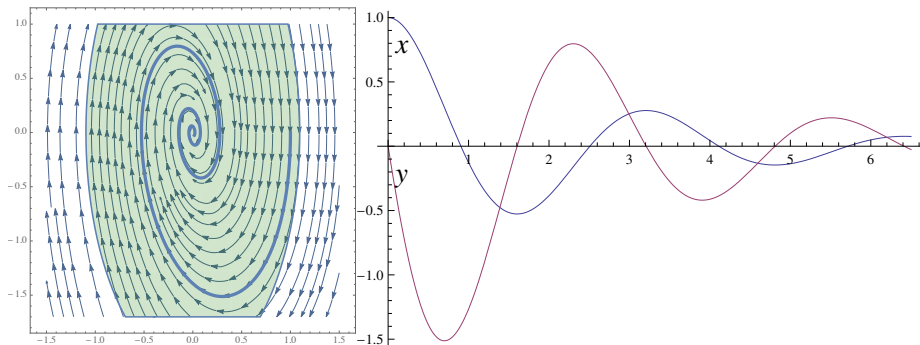


damped oscillator

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

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

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



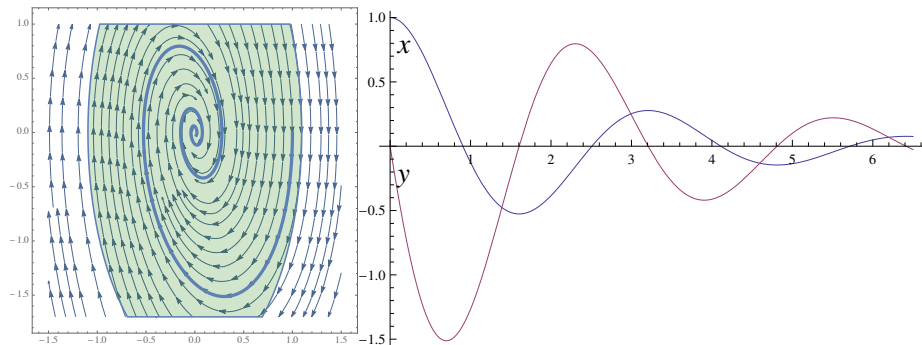
damped oscillator

*

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

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

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



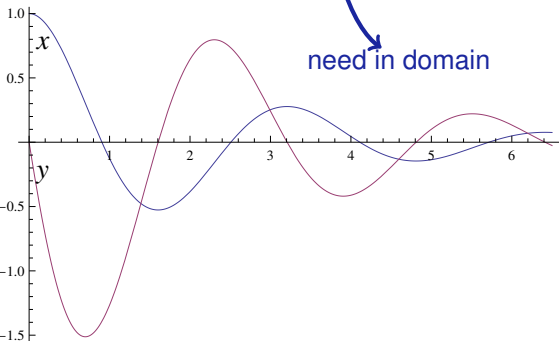
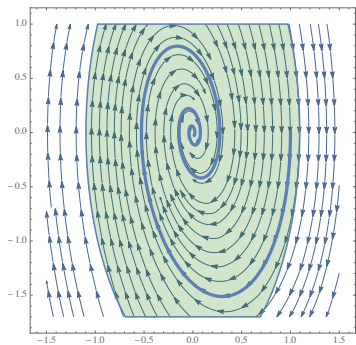
damped oscillator

*

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

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

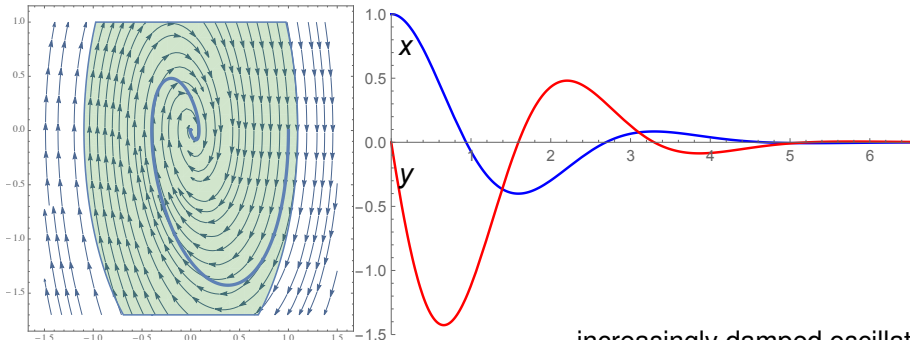
$$\omega^2 x^2 + y^2 \leq c^2 \rightarrow [x' = y, y' = -\omega^2 x - 2d\omega y \ \& \ \omega \geq 0 \wedge d \geq 0] \omega^2 x^2 + y^2 \leq c^2$$



damped oscillator

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

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



increasingly damped oscillator

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

increasingly damped oscillator

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

$$\omega^2 x^2 + y^2 \leq c^2 \rightarrow [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 \ \& \ \omega \geq 0] \omega^2 x^2 + y^2 \leq c^2$$

ask

$$\frac{}{d \geq 0 \rightarrow [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 \ \& \ \omega \geq 0] d \geq 0}$$

increasingly damped oscillator

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

$$\omega \geq 0 \rightarrow [d' := 7] d' \geq 0$$

$$d \geq 0 \rightarrow [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 \ \& \ \omega \geq 0] d \geq 0$$

increasingly damped oscillator

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

$$\omega \geq 0 \rightarrow 7 \geq 0$$

$$\omega \geq 0 \rightarrow [d' := 7] d' \geq 0$$

$$d \geq 0 \rightarrow [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 \ \& \ \omega \geq 0] d \geq 0$$

increasingly damped oscillator

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

$$\omega^2 x^2 + y^2 \leq c^2 \rightarrow [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 \ \& \ \omega \geq 0] \omega^2 x^2 + y^2 \leq c^2$$

DC

*

$$\frac{}{\omega \geq 0 \rightarrow 7 \geq 0}$$

$$\frac{}{\omega \geq 0 \rightarrow [d' := 7] d' \geq 0}$$

$$\frac{}{d \geq 0 \rightarrow [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 \ \& \ \omega \geq 0] d \geq 0}$$

increasingly damped oscillator



$$\begin{array}{c}
 \omega \geq 0 \wedge d \geq 0 \rightarrow [x' := y][y' := -\omega^2 x - 2d\omega y] 2\omega^2 x x' + 2y y' \leq 0 \\
 \hline
 \omega^2 x^2 + y^2 \leq c^2 \rightarrow [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 \ \& \ \omega \geq 0 \wedge d \geq 0] \omega^2 x^2 + y^2 \leq c^2 \\
 \hline
 \omega^2 x^2 + y^2 \leq c^2 \rightarrow [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 \ \& \ \omega \geq 0] \omega^2 x^2 + y^2 \leq c^2
 \end{array}$$

*

$$\omega \geq 0 \rightarrow 7 \geq 0$$

$$\omega \geq 0 \rightarrow [d' := 7] d' \geq 0$$

$$d \geq 0 \rightarrow [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 \ \& \ \omega \geq 0] d \geq 0$$

increasingly damped oscillator

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

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

$$\omega^2 x^2 + y^2 \leq c^2 \rightarrow [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 \ \& \ \omega \geq 0 \wedge d \geq 0] \omega^2 x^2 + y^2 \leq c^2$$

$$\omega^2 x^2 + y^2 \leq c^2 \rightarrow [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 \ \& \ \omega \geq 0] \omega^2 x^2 + y^2 \leq c^2$$

*

$$\omega \geq 0 \rightarrow 7 \geq 0$$

$$\omega \geq 0 \rightarrow [d' := 7] d' \geq 0$$

$$d \geq 0 \rightarrow [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 \ \& \ \omega \geq 0] d \geq 0$$

increasingly damped oscillator

*

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

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

$$\omega^2 x^2 + y^2 \leq c^2 \rightarrow [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 \ \& \ \omega \geq 0 \wedge d \geq 0] \omega^2 x^2 + y^2 \leq c^2$$

$$\omega^2 x^2 + y^2 \leq c^2 \rightarrow [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 \ \& \ \omega \geq 0] \omega^2 x^2 + y^2 \leq c^2$$

*

$$\omega \geq 0 \rightarrow 7 \geq 0$$

$$\omega \geq 0 \rightarrow [d' := 7] d' \geq 0$$

$$d \geq 0 \rightarrow [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 \ \& \ \omega \geq 0] d \geq 0$$

increasingly damped oscillator

*

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

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

$$\omega^2 x^2 + y^2 \leq c^2 \rightarrow [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 \ \& \ \omega \geq 0 \wedge d \geq 0] \omega^2 x^2 + y^2 \leq c^2$$

$$\omega^2 x^2 + y^2 \leq c^2 \rightarrow [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 \ \& \ \omega \geq 0] \omega^2 x^2 + y^2 \leq c^2$$

init

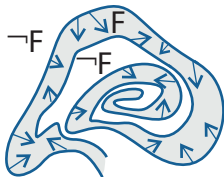
*

$$\omega \geq 0 \rightarrow 7 \geq 0$$

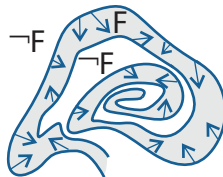
$$\omega \geq 0 \rightarrow [d' := 7] d' \geq 0$$

$$d \geq 0 \rightarrow [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 \ \& \ \omega \geq 0] d \geq 0$$

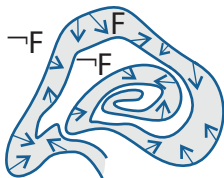
Could repeatedly diffcut in formulas to help the proof



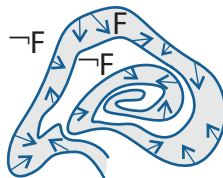
$$\frac{Q \rightarrow [x' := f(x)](F)'}{F \rightarrow [x' = f(x) \ \& \ Q] F}$$



$$\frac{\textcolor{red}{F} \wedge Q \rightarrow [x' := f(x)](F)'}{F \rightarrow [x' = f(x) \ \& \ Q] F}$$



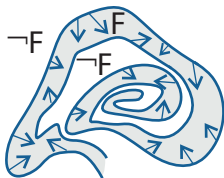
$$\frac{Q \rightarrow [x' := f(x)](F)'}{F \rightarrow [x' = f(x) \& Q]F}$$



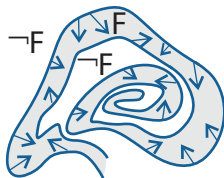
$$\frac{\textcolor{red}{F} \wedge Q \rightarrow [x' := f(x)](F)'}{F \rightarrow [x' = f(x) \& Q]F}$$

Example (Inductive hypothesis)

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



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

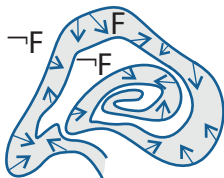


$$\frac{\textcolor{red}{F} \wedge Q \rightarrow [x' := f(x)](F)'}{F \rightarrow [x' = f(x) \& Q]F}$$

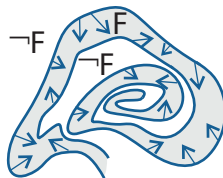
Example (Inductive hypothesis)

$$v^2 - 2v + 1 = 0 \rightarrow [\textcolor{red}{v}' := w][\textcolor{red}{w}' := -v] 2v\textcolor{red}{v}' - 2\textcolor{red}{v}' = 0$$

$$v^2 - 2v + 1 = 0 \rightarrow [v' = w, w' = -v] v^2 - 2v + 1 = 0$$



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



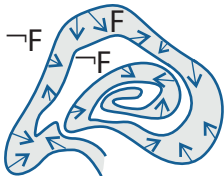
$$\frac{\textcolor{red}{F} \wedge Q \rightarrow [x' := f(x)](F)'}{F \rightarrow [x' = f(x) \ \& \ Q]F}$$

Example (Inductive hypothesis)

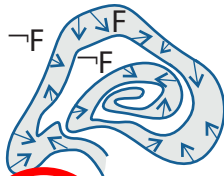
$$\frac{}{v^2 - 2v + 1 = 0 \rightarrow 2v\textcolor{red}{w} - 2\textcolor{red}{w} = 0}$$

$$\frac{}{v^2 - 2v + 1 = 0 \rightarrow [v' := \textcolor{red}{w}][w' := -\textcolor{red}{v}]2vv' - 2v' = 0}$$

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



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



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

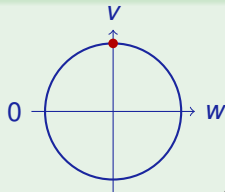
Example (Inductive hypothesis is unsound!)

(unsound)

$$v^2 - 2v + 1 = 0 \rightarrow 2vw - 2w = 0$$

$$v^2 - 2v + 1 = 0 \rightarrow [v' := w][w' := -v]2vv' - 2v' = 0$$

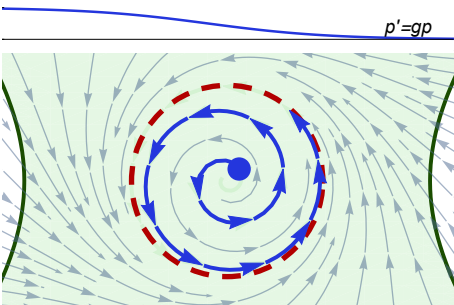
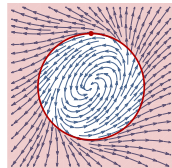
$$v^2 - 2v + 1 = 0 \rightarrow [v' = w, w' = -v]v^2 - 2v + 1 = 0$$



Induction for ODEs is subtle!

Darboux inequalities are DG

$$\frac{Q \rightarrow p^\bullet \geq gp}{p \succ 0 \rightarrow [x' = f(x) \& Q] p \succ 0} \quad (g \in \mathbb{R}[x])$$



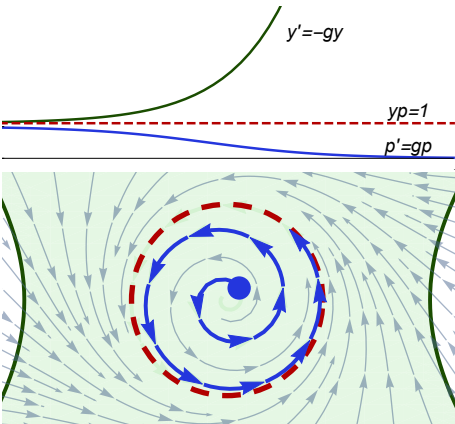
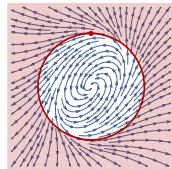
$$\begin{aligned} (1-u^2-v^2)^\bullet &\geq -\frac{1}{2}(u^2+v^2)(1-u^2-v^2) \\ \dots \rightarrow \begin{cases} u' = -v + \frac{u}{4}(1-u^2-v^2) \\ v' = u + \frac{v}{4}(1-u^2-v^2) \end{cases} \end{aligned}$$

$$\underbrace{1-u^2-v^2}_{>0}$$

Definable $p^\bullet$ for Lie-derivative w.r.t. ODE

Darboux inequalities are DG

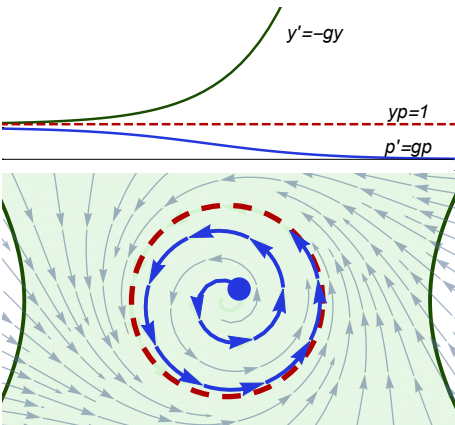
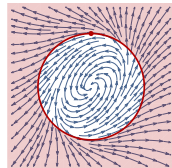
$$\frac{Q \rightarrow p^\bullet \geq gp}{p \succ 0 \rightarrow [x' = f(x) \& Q] p \succ 0} \quad (g \in \mathbb{R}[x])$$



$$\begin{aligned} (1-u^2-v^2)^\bullet &\geq -\frac{1}{2}(u^2+v^2)(1-u^2-v^2) \\ \dots \rightarrow &\begin{cases} u' = -v + \frac{u}{4}(1-u^2-v^2) \\ v' = u + \frac{v}{4}(1-u^2-v^2) \\ y' = \frac{1}{2}(u^2+v^2)y \end{cases} \\ &] \underbrace{1-u^2-v^2}_{y(1-u^2-v^2)=1} > 0 \end{aligned}$$

Darboux inequalities are DG

$$\frac{Q \rightarrow p^\bullet \geq gp}{p \succcurlyeq 0 \rightarrow [x' = f(x) \& Q] p \succcurlyeq 0} \quad (g \in \mathbb{R}[x])$$

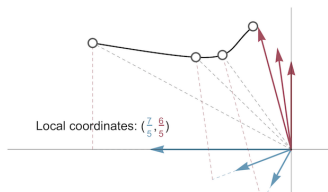
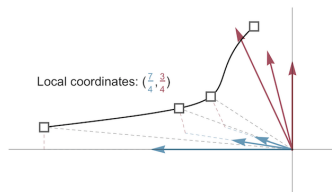
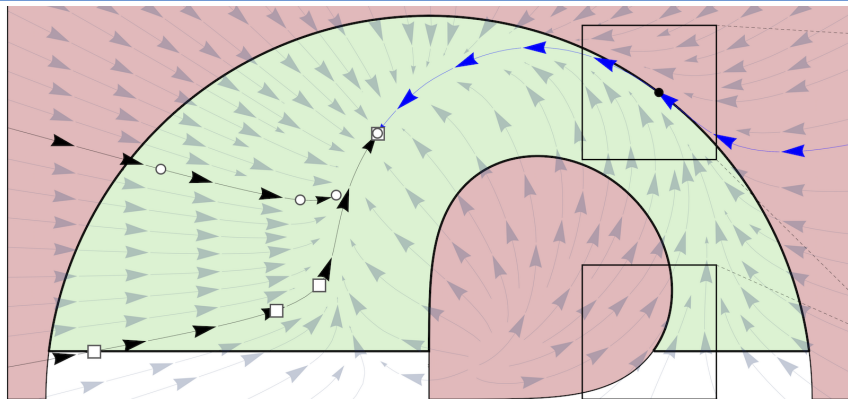


$$\begin{aligned} (1-u^2-v^2)^\bullet &\geq -\frac{1}{2}(u^2+v^2)(1-u^2-v^2) \\ \dots \rightarrow &\left[\begin{aligned} u' &= -v + \frac{u}{4}(1-u^2-v^2) \\ v' &= u + \frac{v}{4}(1-u^2-v^2) \\ y' &= \frac{1}{2}(u^2+v^2)y \\ z' &= -\frac{1}{4}(u^2+v^2)z \end{aligned} \right] \underbrace{1-u^2-v^2}_{y(1-u^2-v^2)=1} > 0 \end{aligned}$$

$$\begin{array}{c}
 \text{dG} \quad \frac{y > 0 \rightarrow [x' = f(x), y' = -gy \& Q] y > 0}{y > 0 \rightarrow \exists z [x' = f(x), y' = -gy, z' = \frac{g}{2}z \& Q] y > 0} \\
 \text{M}[\cdot, \exists \mathbb{R}] \quad \frac{y > 0 \rightarrow \exists z [x' = f(x), y' = -gy, z' = \frac{g}{2}z \& Q] y > 0}{yz^2 = 1 \rightarrow [x' = f(x), y' = -gy, z' = \frac{g}{2}z \& Q] yz^2 = 1} \\
 \text{dl} \quad \frac{yz^2 = 1 \rightarrow [x' = f(x), y' = -gy, z' = \frac{g}{2}z \& Q] yz^2 = 1}{Q \rightarrow (-gy)z^2 + y(2z(\frac{g}{2}z)) = 0} \\
 \mathbb{R} \quad \frac{Q \rightarrow (-gy)z^2 + y(2z(\frac{g}{2}z)) = 0}{*}
 \end{array}$$

$$\begin{array}{c}
 \text{dG} \quad \frac{p \succcurlyeq 0 \rightarrow [x' = f(x), y' = -gy \& Q] p \succcurlyeq 0}{p \succcurlyeq 0 \rightarrow \exists y [x' = f(x), y' = -gy \& Q] p \succcurlyeq 0} \\
 \text{M}[\cdot, \exists \mathbb{R}] \quad \frac{p \succcurlyeq 0 \rightarrow \exists y [x' = f(x), y' = -gy \& Q] p \succcurlyeq 0}{p \succcurlyeq 0, y > 0 \rightarrow [x' = f(x), y' = -gy \& Q] (y > 0 \wedge p \succcurlyeq 0)} \\
 \text{dC} \quad \frac{p \succcurlyeq 0, y > 0 \rightarrow [x' = f(x), y' = -gy \& Q] (y > 0 \wedge p \succcurlyeq 0)}{p \succcurlyeq 0, y > 0 \rightarrow [x' = f(x), y' = -gy \& Q \wedge y > 0] p \succcurlyeq 0} \\
 \text{dl} \quad \frac{p \succcurlyeq 0, y > 0 \rightarrow [x' = f(x), y' = -gy \& Q \wedge y > 0] p \succcurlyeq 0}{Q, y > 0 \rightarrow p \dot{\succcurlyeq} y - gyp \geq 0} \\
 \text{cut} \quad \frac{Q, y > 0 \rightarrow p \dot{\succcurlyeq} y - gyp \geq 0}{Q \rightarrow p \dot{\succcurlyeq} \geq gp} \\
 \mathbb{R} \quad \frac{Q \rightarrow p \dot{\succcurlyeq} \geq gp, y > 0 \rightarrow p \dot{\succcurlyeq} y - gyp \geq 0}{*}
 \end{array}$$

Completeness for Differential Equation Invariants



Theorem (Algebraic Completeness) (LICS'18,JACM'20)

dL calculus is a sound & complete axiomatization of algebraic invariants of polynomial differential equations. They are decidable by DI,DC,DG in dL.

Theorem (Semialgebraic Completeness) (LICS'18,JACM'20)

dL calculus with RI is a sound & complete axiomatization of semialgebraic invariants of differential equations. They are decidable in dL.

Theorem (Algebraic Completeness) (LICS'18,JACM'20)

dL calculus is a sound & complete axiomatization of algebraic invariants of polynomial differential equations. They are decidable

$$\text{DRI } [x' = f(x) \& Q]e = 0 \leftrightarrow (Q \rightarrow e'^* = 0) \quad (Q \text{ open})$$

Theorem (Semialgebraic Completeness) (LICS'18,JACM'20)

dL calculus with RI is a sound & complete axiomatization of semialgebraic invariants of differential equations. They are decidable

$$\text{SAI } \forall x (P \rightarrow [x' = f(x)]P) \leftrightarrow \forall x (P \rightarrow P'^*) \wedge \forall x (\neg P \rightarrow (\neg P)^{'*-})$$

Definable e'^* is short for *all/significant* Lie derivative w.r.t. ODE

Definable $e'^*{}_-$ is w.r.t. backwards ODE $x' = -f(x)$. Also for P .

$$e'^* = 0 \equiv e=0 \wedge (e')'^*=0 \quad (P \wedge Q)^{'*} \equiv P'^* \wedge Q'^*$$

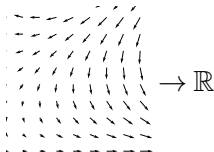
$$e'^* \geq 0 \equiv e \geq 0 \wedge (e=0 \rightarrow (e')'^* \geq 0) \quad (P \vee Q)^{'*} \equiv P'^* \vee Q'^*$$

Syntax

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

Semantics

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



Axioms

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

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

$$(c())' = 0$$

for constants/numbers $c()$

$$(x)' = x'$$

for variables $x \in \mathcal{V}$

ODE

$$\llbracket x' = f(x) \& Q \rrbracket = \{(\varphi(0)|_{\{x'\}^{\mathbb{C}}}, \varphi(r)) : \varphi \models x' = f(x) \wedge Q \text{ for some } \varphi : [0, r] \rightarrow \mathcal{S}, \text{ some } r \in \mathbb{R}\}$$

$$\varphi(z)(x') = \frac{d\varphi(t)(x)}{dt}(z) \quad \dots$$

Differential Substitution Lemmas $\rightsquigarrow$ Proofs

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

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

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

Lemma (Differential assignment) (Effect on Differentials)

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

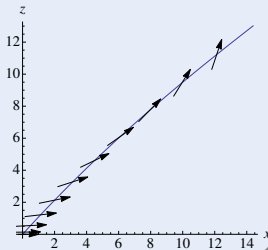
Lemma (Derivations) (Equations of Differentials)

$$\begin{array}{ll} +' & (e + k)' = (e)' + (k)' \\ \cdot' & (e \cdot k)' = (e)' \cdot k + e \cdot (k)' \\ c' & (c())' = 0 \\ x' & (x)' = x' \end{array}$$

Example: Longitudinal Dynamics of an Airplane

Study (6th Order Longitudinal Flight Equations)

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



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

Example: Longitudinal Dynamics of an Airplane

Study (6th Order Longitudinal Flight Equations)

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

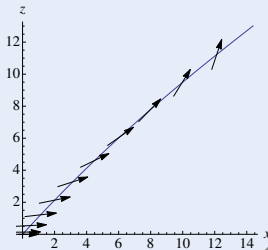
$$w' = \frac{Z}{m} + g \cos(\theta) + qu \quad \text{vertical velocity}$$

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

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

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

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

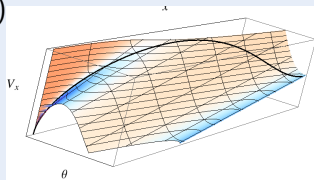


Result (DRI Automatically Generates Invariant Functions)

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

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

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

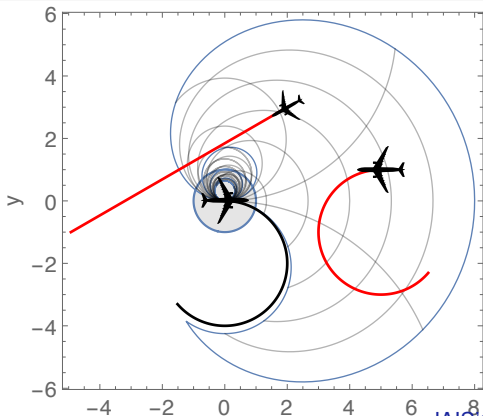
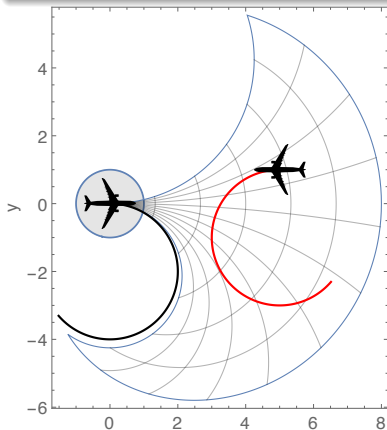


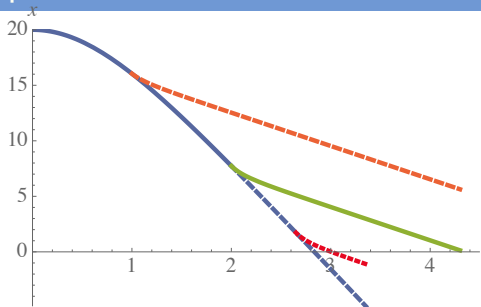
Example: Dubins Dynamics of 2 Airplanes

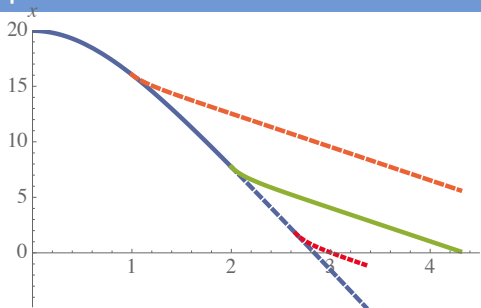
Result (DRI Automatically Generates Invariants)

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

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

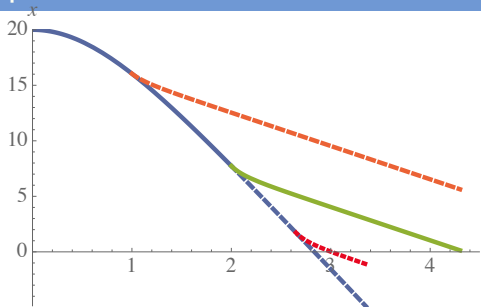






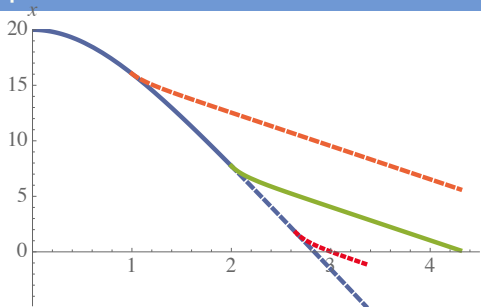
Example (▶ Parachute)

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



Example (▶ Parachute)

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

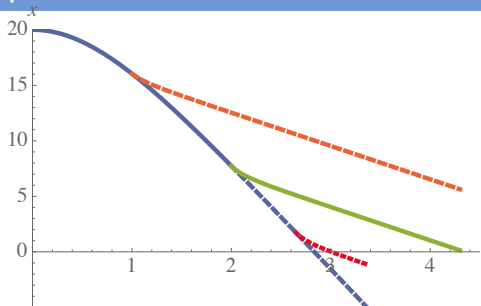


Example (▶ Parachute)

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

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

Conservatively bounded next velocity above parachute's **limit velocity**.



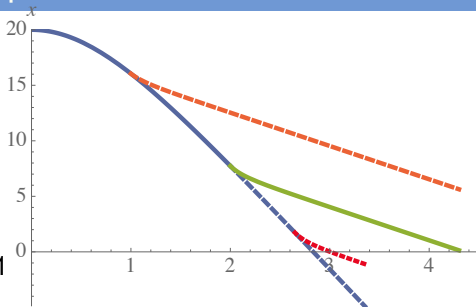
Example (▶ Parachute)

$$m < -\sqrt{g/p} \rightarrow \left[\left((Q \wedge r = a) \cup r := p \right); t := 0; \right. \\ \left. \{x' = v, v' = -g + rv^2, t' = 1 \ \& \ t \leq T \wedge x \geq 0 \wedge v < 0\}^* \right] \\ (x = 0 \rightarrow v \geq m)$$

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

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

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



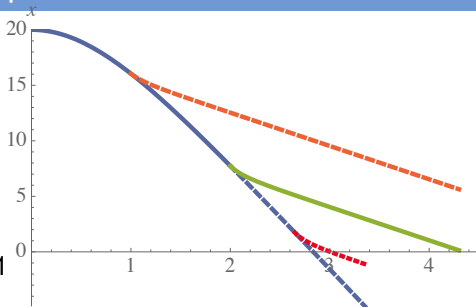
Example (▶ Parachute)

$$m < -\sqrt{g/p} \rightarrow \left[\left((Q \wedge r = a) \cup r := p \right); t := 0; \right. \\ \left. \{x' = v, v' = -g + rv^2, t' = 1 \ \& \ t \leq T \wedge x \geq 0 \wedge v < 0\}^* \right] \\ (x = 0 \rightarrow v \geq m)$$

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

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

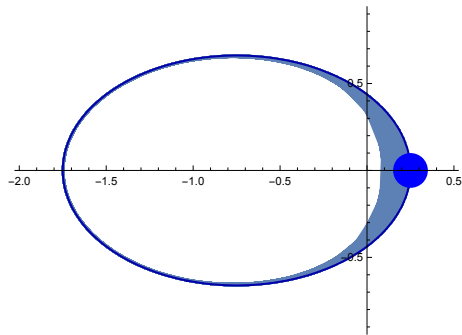
$$y' = -\frac{p}{2}(v - \sqrt{g/p}) \quad y^2(\underbrace{v + \sqrt{g/p}}_{>0}) = 1$$



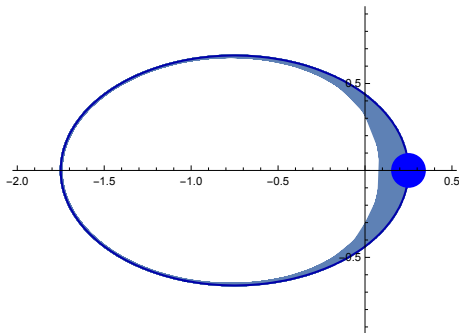
$$v \geq \text{old}(v) - gt \text{ if closed}$$

Example (▶ Parachute)

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



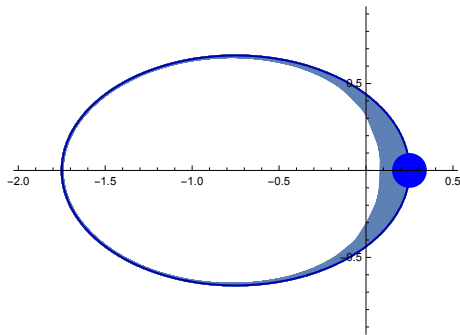
- $-\frac{x}{\sqrt{x^2+y^2}}$ opposite direction
- $\frac{1}{x^2+y^2}$ inverse-square law



Example (▶ Two Body Problem)

$$\begin{aligned} [x' = v, v' = -x/(x^2 + y^2)^{3/2}, \\ y' = w, w' = -y/(x^2 + y^2)^{3/2}] \end{aligned}$$

- $-\frac{x}{\sqrt{x^2+y^2}}$ opposite direction
- $\frac{1}{x^2+y^2}$ inverse-square law
- Energy preservation



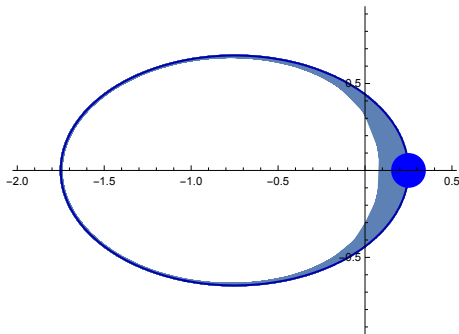
Example (▶ Two Body Problem)

$$\frac{v^2 + w^2}{2} - \frac{1}{\sqrt{x^2 + y^2}} = E \rightarrow$$

$$[x' = v, v' = -x/(x^2 + y^2)^{3/2},$$

$$y' = w, w' = -y/(x^2 + y^2)^{3/2}] \frac{v^2 + w^2}{2} - \frac{1}{\sqrt{x^2 + y^2}} = E$$

- $-\frac{x}{\sqrt{x^2+y^2}}$ opposite direction
- $\frac{1}{x^2+y^2}$ inverse-square law
- Energy preservation
- Well-definedness



Example (▶ Two Body Problem)

$$\frac{v^2 + w^2}{2} - \frac{1}{\sqrt{x^2 + y^2}} = E \rightarrow$$

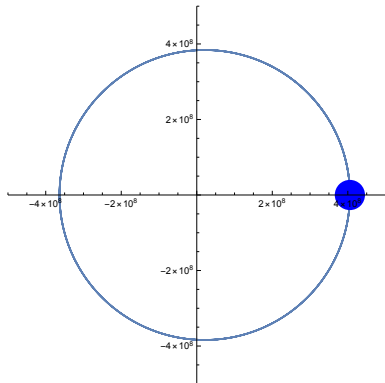
$$[x' = v, v' = -x/(x^2 + y^2)^{3/2},$$

& $x \neq 0 \vee y \neq 0$

$$y' = w, w' = -y/(x^2 + y^2)^{3/2}] \frac{v^2 + w^2}{2} - \frac{1}{\sqrt{x^2 + y^2}} = E$$

Exercise: Moon Gravitates Around the Earth

- G Gravitational constant
 $6.67430 * 10^{-11}$
- M Mass of the Earth
- m Mass of the Moon



Example (▶ Moon around Earth)

$$\dots \rightarrow [x' = v, v' = -GMx/(x^2 + y^2)^{3/2}, \\ y' = w, w' = -GMy/(x^2 + y^2)^{3/2} \ \& \ x \neq 0 \vee y \neq 0] \dots$$

Summary: Proving ODEs

Differential Invariant

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

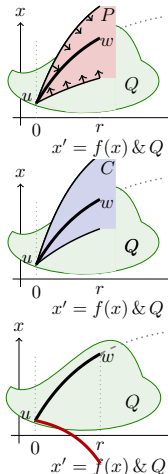
Differential Cut

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

Differential Ghost

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

if $g(x, y) = a(x)y + b(x)$, so has long solution!

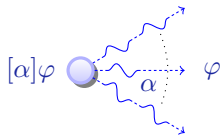


- 1 CPS are Multi-Dynamical Systems
- 2 CPS Programs
 - Syntax
 - Semantics
 - Examples
- 3 Differential Dynamic Logic
 - Syntax
 - Semantics
 - Example: Car Control Design
- 4 Dynamic Axioms for Dynamical Systems
 - Axiomatics
 - dL Proofs in KeYmaera X
- 5 Differential Invariants for Differential Equations
 - Axiomatics
 - Examples
- 6 Summary

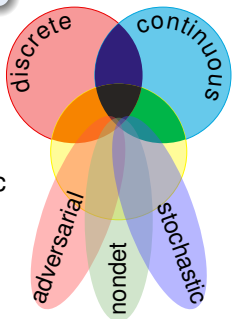
Logical foundations make a big difference for CPS, and vice versa

differential dynamic logic

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



- Multi-dynamical systems
- Hybrid programs + dL logic
- Compositional proofs
- Decide invariant by dL



- 1 Analytic foundations
- 2 Practical proving
- 3 Significant applications
- 4 Bring sciences together

Programming CPS $\neq$ program cyber || program physics (mutual ignorance)

CPSs deserve proofs as safety evidence!

- Verified CPS implementations by ModelPlex
- Correct CPS execution
- CPS proof and tactic languages+libraries
- Big CPS built from safe components
- ODE invariance
- ODE liveness
- ODE stability
- Invariant generation
- Safe AI autonomy in CPS
- Refinement + system property proofs
- CPS information flow
- Hybrid games
- Constructive hybrid games

FMSD'16

PLDI'18

ITP'17

STTT'18

JACM'20

FAC'21

TACAS'21

FMSD'21

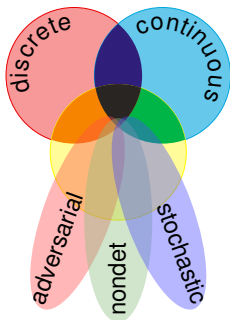
AAAI'18

LICS'16

LICS'18

TOCL'15

IJCAR'20



I Part: Elementary Cyber-Physical Systems

2. Differential Equations & Domains
3. Choice & Control
4. Safety & Contracts
5. Dynamical Systems & Dynamic Axioms
6. Truth & Proof
7. Control Loops & Invariants
8. Events & Responses
9. Reactions & Delays

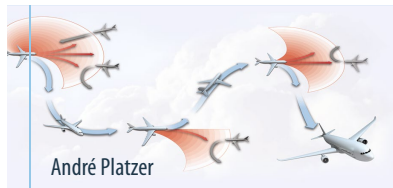
II Part: Differential Equations Analysis

10. Differential Equations & Differential Invariants
11. Differential Equations & Proofs
12. Ghosts & Differential Ghosts
13. Differential Invariants & Proof Theory

III Part: Adversarial Cyber-Physical Systems

- 14-17. Hybrid Systems & Hybrid Games

IV Part: Comprehensive CPS Correctness



Logical Foundations of Cyber-Physical Systems



André Platzer.

Logical Foundations of Cyber-Physical Systems.

Springer, Cham, 2018.

[doi:10.1007/978-3-319-63588-0](https://doi.org/10.1007/978-3-319-63588-0).



André Platzer.

Logic & proofs for cyber-physical systems.

In Nicola Olivetti and Ashish Tiwari, editors, *IJCAR*, volume 9706 of *LNCS*, pages 15–21, Cham, 2016. Springer.

[doi:10.1007/978-3-319-40229-1_3](https://doi.org/10.1007/978-3-319-40229-1_3).



André Platzer.

Logics of dynamical systems.

In LICS [18], pages 13–24.

[doi:10.1109/LICS.2012.13](https://doi.org/10.1109/LICS.2012.13).



André Platzer.

A complete uniform substitution calculus for differential dynamic logic.

J. Autom. Reas., 59(2):219–265, 2017.

[doi:10.1007/s10817-016-9385-1](https://doi.org/10.1007/s10817-016-9385-1).



André Platzer.

Differential dynamic logic for hybrid systems.

J. Autom. Reas., 41(2):143–189, 2008.

doi:10.1007/s10817-008-9103-8.



André Platzer.

Differential game logic.

ACM Trans. Comput. Log., 17(1):1:1–1:51, 2015.

doi:10.1145/2817824.



André Platzer.

Differential hybrid games.

ACM Trans. Comput. Log., 18(3):19:1–19:44, 2017.

doi:10.1145/3091123.



André Platzer.

The complete proof theory of hybrid systems.

In LICS [18], pages 541–550.

doi:10.1109/LICS.2012.64.



Nathan Fulton, Stefan Mitsch, Jan-David Quesel, Marcus Völp, and André Platzer.

KeYmaera X: An axiomatic tactical theorem prover for hybrid systems.

In Amy Felty and Aart Middeldorp, editors, *CADE*, volume 9195 of *LNCS*, pages 527–538, Berlin, 2015. Springer.

[doi:10.1007/978-3-319-21401-6_36](https://doi.org/10.1007/978-3-319-21401-6_36).



Stefan Mitsch and André Platzer.

ModelPlex: Verified runtime validation of verified cyber-physical system models.

Form. Methods Syst. Des., 49(1-2):33–74, 2016.

Special issue of selected papers from RV'14.

[doi:10.1007/s10703-016-0241-z](https://doi.org/10.1007/s10703-016-0241-z).



André Platzer.

Differential-algebraic dynamic logic for differential-algebraic programs.

J. Log. Comput., 20(1):309–352, 2010.

[doi:10.1093/logcom/exn070](https://doi.org/10.1093/logcom/exn070).



André Platzer.

The structure of differential invariants and differential cut elimination.

Log. Meth. Comput. Sci., 8(4:16):1–38, 2012.

doi:10.2168/LMCS-8(4:16)2012.



André Platzer and Yong Kiam Tan.

Differential equation axiomatization: The impressive power of differential ghosts.

In Anuj Dawar and Erich Grädel, editors, *LICS*, pages 819–828, New York, 2018. ACM.

doi:10.1145/3209108.3209147.



André Platzer and Yong Kiam Tan.

Differential equation invariance axiomatization.

J. ACM, 67(1):6:1–6:66, 2020.

doi:10.1145/3380825.



Nathan Fulton, Stefan Mitsch, Brandon Bohrer, and André Platzer.

Bellerophon: Tactical theorem proving for hybrid systems.

In Mauricio Ayala-Rincón and César A. Muñoz, editors, *ITP*, volume 10499 of *LNCS*, pages 207–224. Springer, 2017.

doi:10.1007/978-3-319-66107-0_14.



Thomas A. Henzinger.

The theory of hybrid automata.

In *LICS*, pages 278–292, Los Alamitos, 1996. IEEE Computer Society.
[doi:10.1109/LICS.1996.561342](https://doi.org/10.1109/LICS.1996.561342).



Jennifer M. Davoren and Anil Nerode.

Logics for hybrid systems.

IEEE, 88(7):985–1010, 2000.

[doi:10.1109/5.871305](https://doi.org/10.1109/5.871305).



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