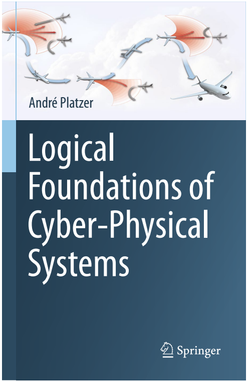
Logical Foundations of Cyber-Physical Systems



André Platzer

Carnegie Mellon University
Computer Science Department

Outline

Outline (Introduction to CPS)

Cyber-Physical Systems Analysis: Aircraft Example

Which control decisions are safe for aircraft collision avoidance?

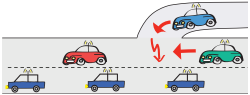
Cyber-Physical Systems

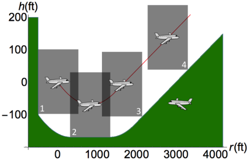
CPSs combine cyber capabilities with physical capabilities
to solve problems that neither part could solve alone.

CPSs Promise Transformative Impact!

Prospects: Safe & Efficient

Driver assistance	Pilot decision support	Train protection
Autonomous cars	Autopilots / UAVs	Robots near humans





Prerequisite: CPSs need to be safe

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

Can you trust a computer to control physics?

Can you trust a computer to control physics?

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

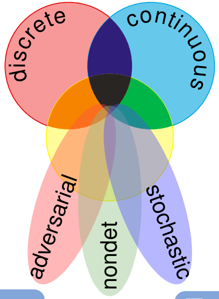
Rationale

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

CPSs deserve proofs as safety evidence!

CPS Dynamics

CPS are characterized by multiple facets of dynamical systems.



CPS Compositions

CPS combines multiple simple dynamical effects.

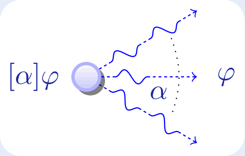
Descriptive simplification

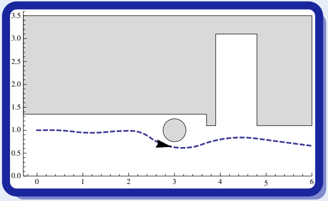
Tame Parts

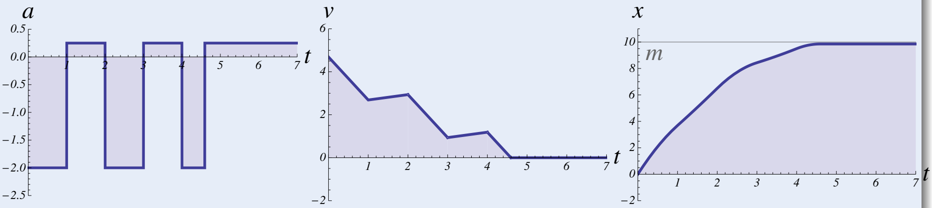
Exploiting compositionality tames CPS complexity.

Analytic simplification

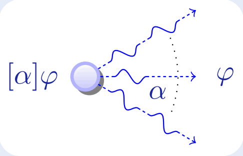
Concept (Differential Dynamic Logic) (JAR'08,LICS'12)

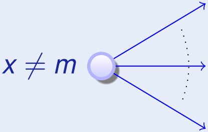


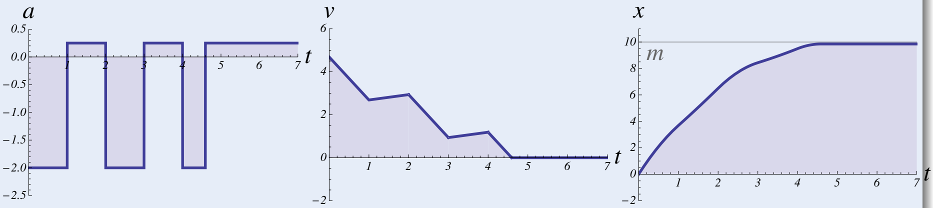




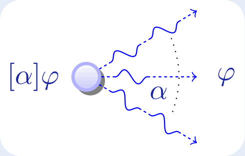
Concept (Differential Dynamic Logic) (JAR'08,LICS'12)

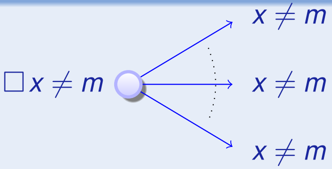


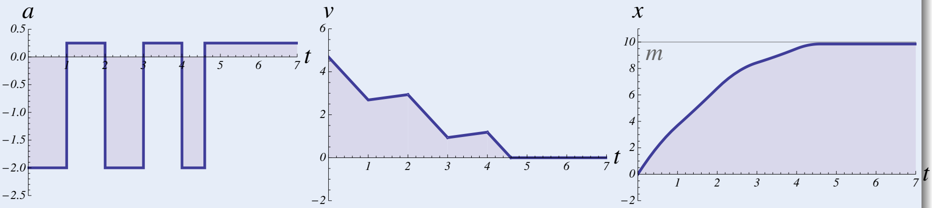




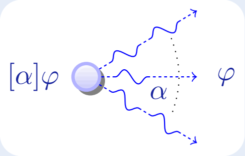
Concept (Differential Dynamic Logic) (JAR'08,LICS'12)

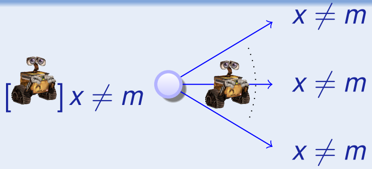


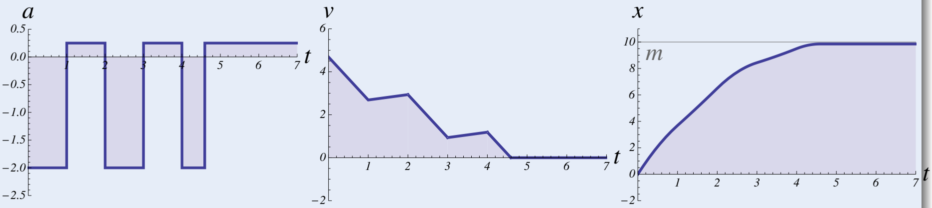




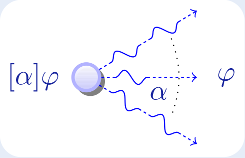
Concept (Differential Dynamic Logic) (JAR'08,LICS'12)

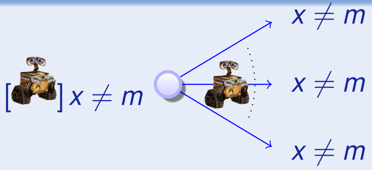




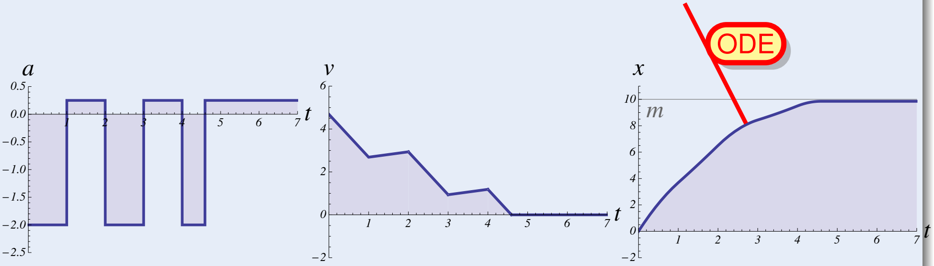


Concept (Differential Dynamic Logic) (JAR'08,LICS'12)

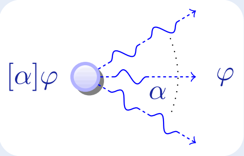


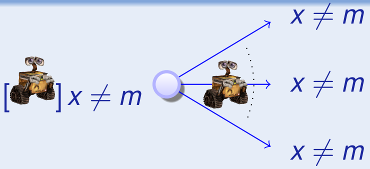


$$x' = v, v' = a$$

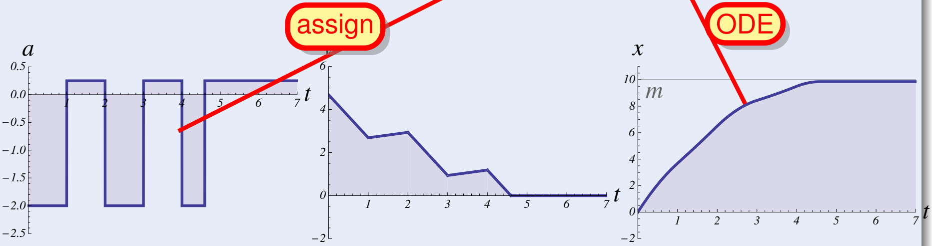


Concept (Differential Dynamic Logic) (JAR'08,LICS'12)



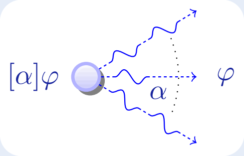


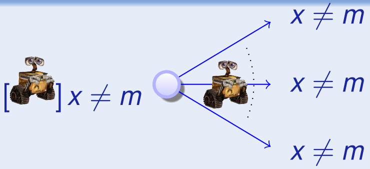
$a := -b$ $\quad x' = v, v' = a$



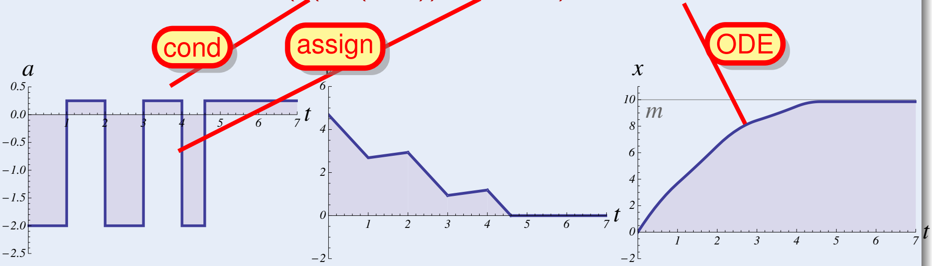
CPS Analysis

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



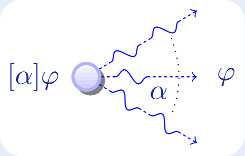


$(\text{if}(SB(x,m))\quad a := -b)\quad x' = v, v' = a$



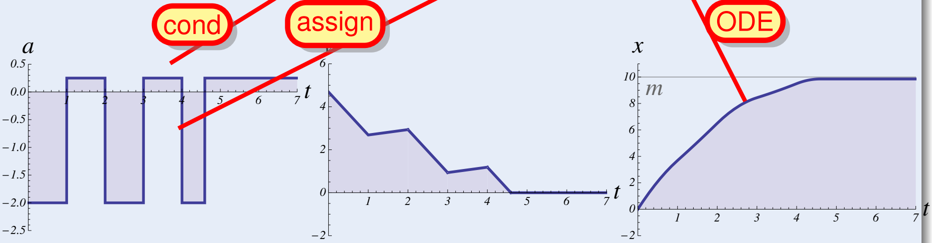
CPS Analysis

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

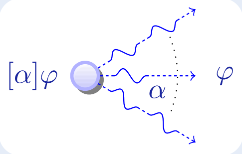


seq. compose

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



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



seq. compose

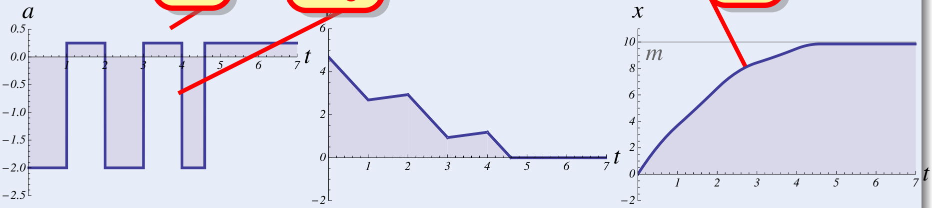
nondet. repeat

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

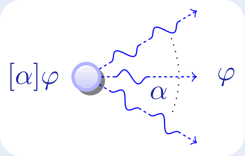
cond

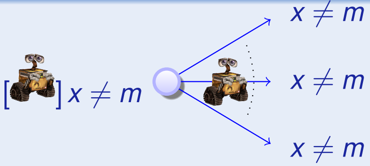
assign

ODE



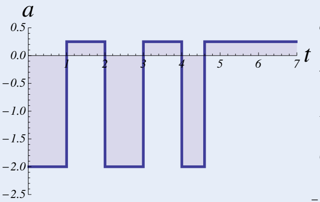
Concept (Differential Dynamic Logic) (JAR'08,LICS'12)

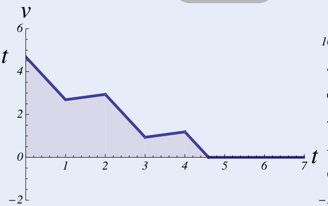


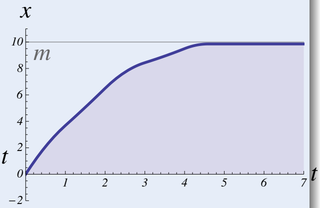


$$\left[\left((\text{if}(SB(x,m))\quad a:=-b)\ ;\ x'=v, v'=a\right)^*\right] \underbrace{x \neq m}_{\text{post}}$$

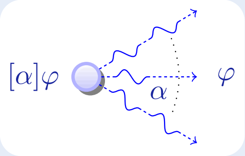
all runs

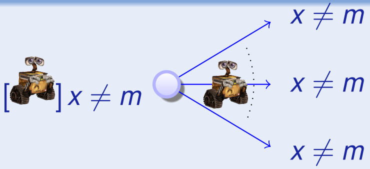






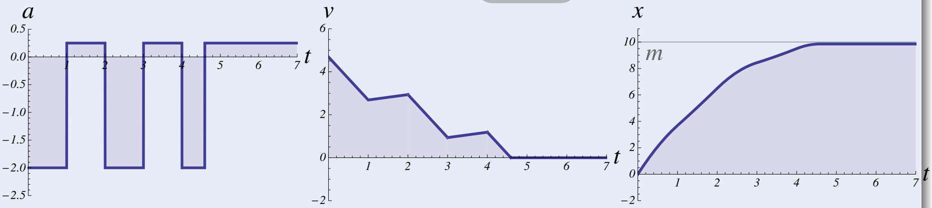
Concept (Differential Dynamic Logic) (JAR'08,LICS'12)



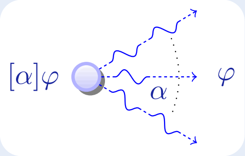


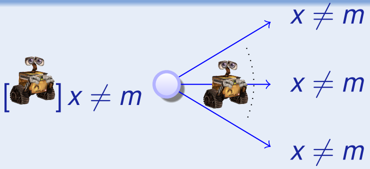
$$\underbrace{x \neq m \wedge b > 0}_{\text{init}} \rightarrow \big[\big((\text{if}(SB(x,m))\quad a := -b)\;;\; x' = v, v' = a\big)^*\big]\underbrace{x \neq m}_{\text{post}}$$

all runs



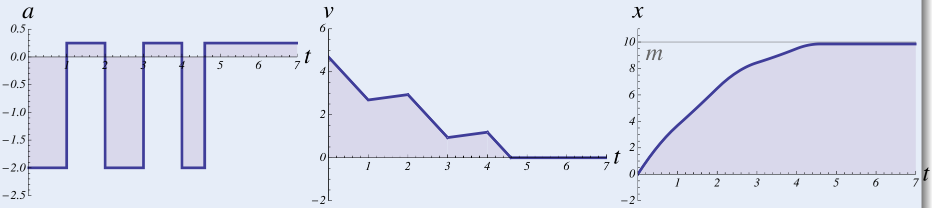
Concept (Differential Dynamic Logic) (JAR'08,LICS'12)



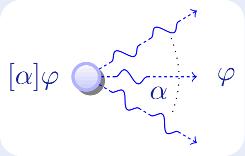


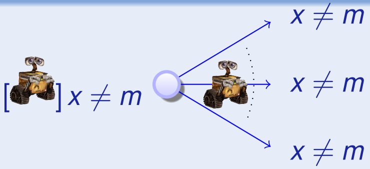
nondet. choice

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



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

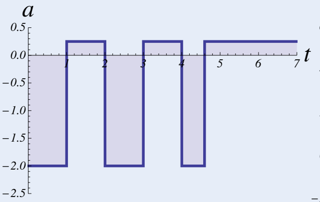


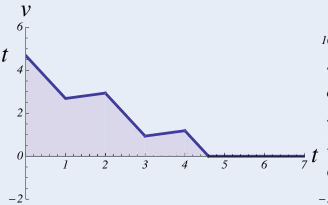


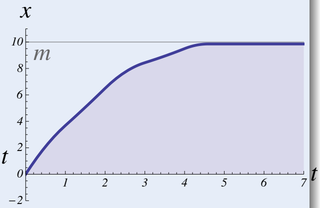
test

nondet. choice

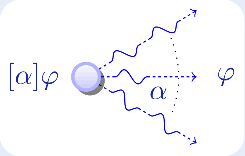
$$\underbrace{x \neq m \land b > 0}_{\text{init}} \rightarrow \left[\left(\left(?\neg SB(x,m) \cup a := -b\right);\ x' = v, v' = a\right)^*\right] \underbrace{x \neq m}_{\text{post}}$$

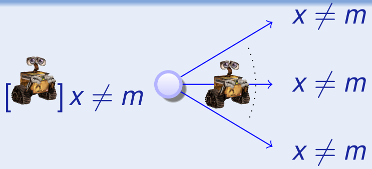






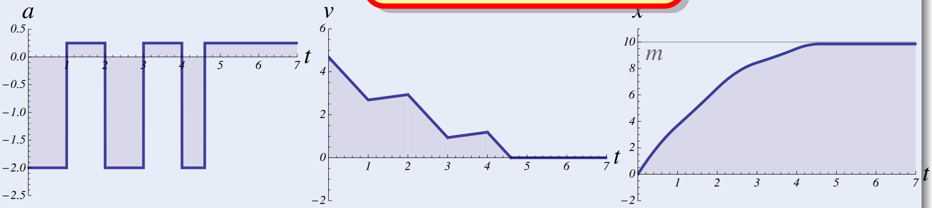
Concept (Differential Dynamic Logic) (JAR'08,LICS'12)





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

hybrid program dynamics



Outline (Modeling CPS)

Hybrid Programs: Syntax

Definition (Syntax of hybrid program α)

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

Hybrid Programs: Syntax

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

Hybrid Programs: Syntax

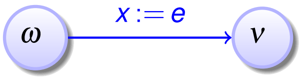
Definition (Syntax of hybrid program α)

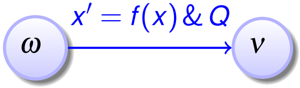
$$\alpha, \beta ::= x := e \mid ?Q \mid x' = f(x) \,\&\, Q \mid \alpha \cup \beta \mid \alpha ; \beta \mid \alpha^*$$

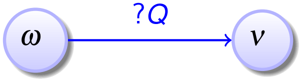
- $x := e$ — Discrete Assign
- $?Q$ — Test Condition
- $x' = f(x) \,\&\, Q$ — Differential Equation
- $\alpha \cup \beta$ — Nondet. Choice
- $\alpha ; \beta$ — Seq. Compose
- α^* — Nondet. Repeat

Like regular expressions. Everything nondeterministic

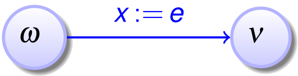
Hybrid Programs: Semantics

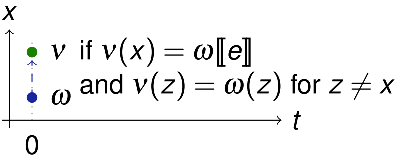


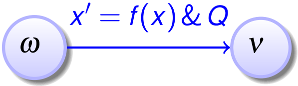


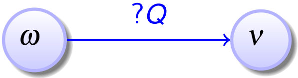


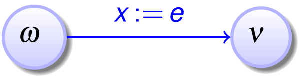
Hybrid Programs: Semantics

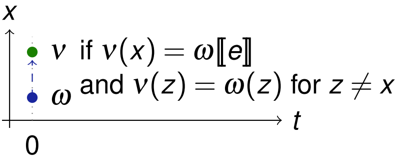


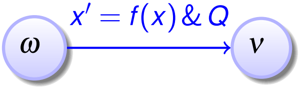


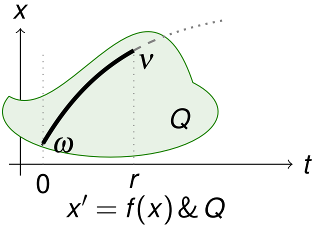


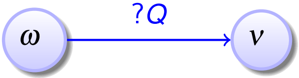


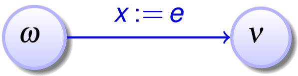

ω
$x := e$
ν


x
ν if $\nu(x) = \omega[\![e]\!]$
ω and $\nu(z) = \omega(z)$ for $z \neq x$
t
0

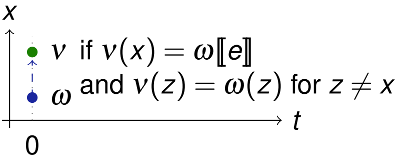

ω
$x' = f(x) \,\&\, Q$
ν


x
ν
Q
ω
t
0
r
$x' = f(x) \,\&\, Q$

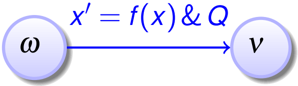

ω
$?Q$
ν



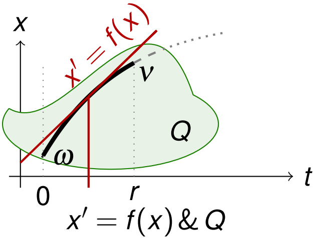
$x := e$
ω
ν



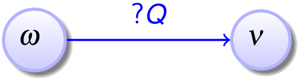
x
ν if $\nu(x) = \omega[\![e]\!]$
ω and $\nu(z) = \omega(z)$ for $z \neq x$
t
0



$x' = f(x) \,\&\, Q$
ω
ν

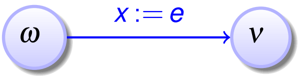


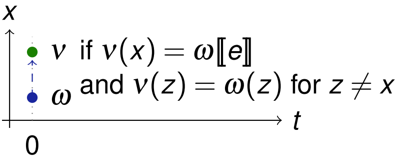
x
$x' = f(x)$
ν
Q
ω
t
0
r
$x' = f(x) \,\&\, Q$

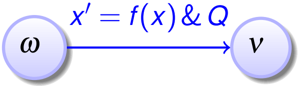


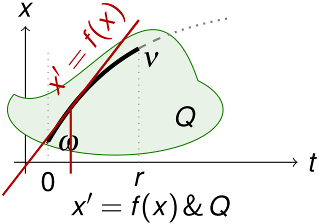
$?Q$
ω
ν

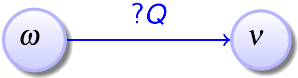
Hybrid Programs: Semantics



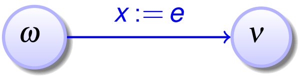


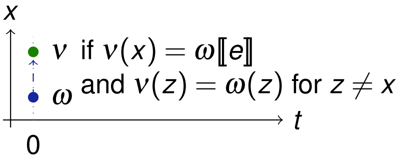


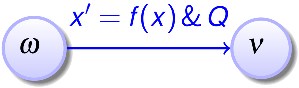


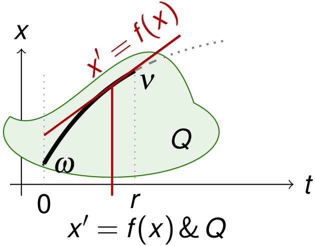


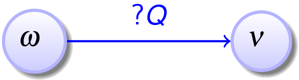
Hybrid Programs: Semantics



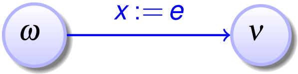


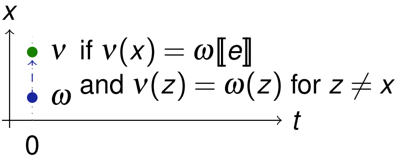


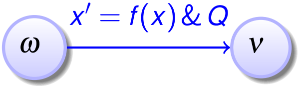


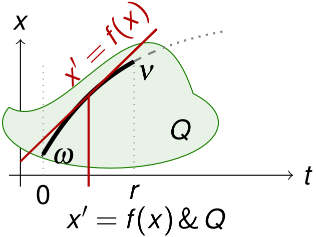


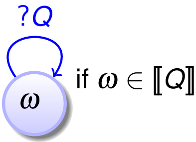
Hybrid Programs: Semantics

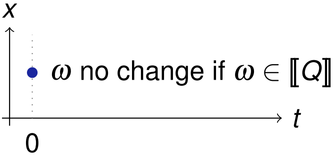




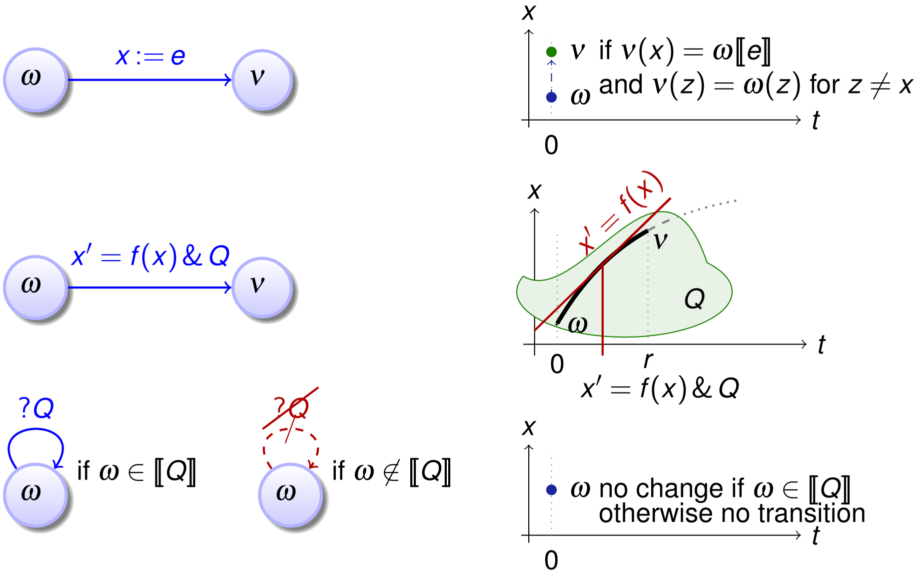


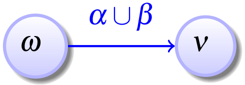


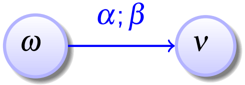


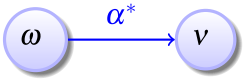


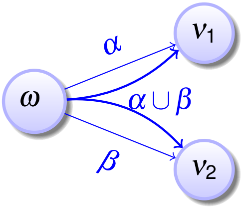
Hybrid Programs: Semantics

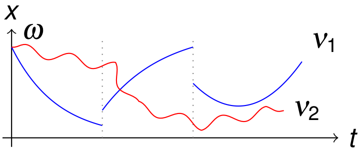


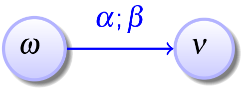

$\alpha \cup \beta$
ω
ν

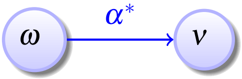

$\alpha;\beta$
ω
ν

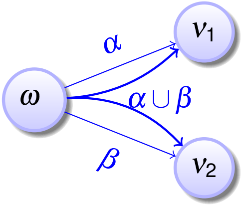

α^*
ω
ν

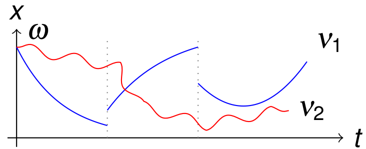

α
ν_1
ω
$\alpha \cup \beta$
β
ν_2

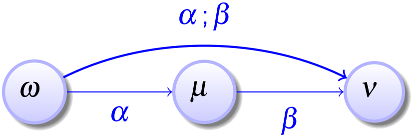

x
ω
ν_1
ν_2
t

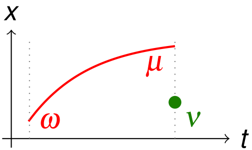

$\alpha;\beta$
ω
ν

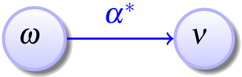

α^*
ω
ν

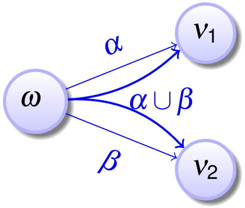

α
ω
ν_1
$\alpha \cup \beta$
β
ν_2


x
ω
ν_1
ν_2
t

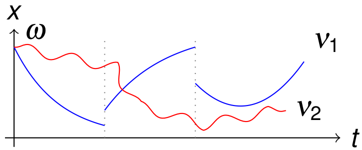

$\alpha ; \beta$
ω
μ
ν
α
β


x
μ
ω
ν
t

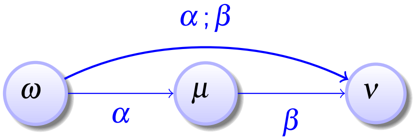

α^*
ω
ν



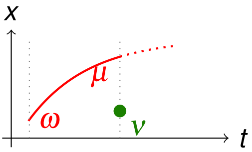
α
ν_1
ω
$\alpha \cup \beta$
β
ν_2



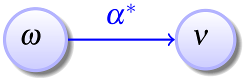
x
ω
ν_1
ν_2
t



$\alpha ; \beta$
ω
μ
ν
α
β

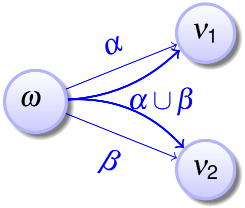


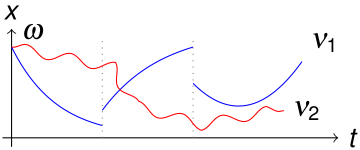
x
μ
ω
ν
t

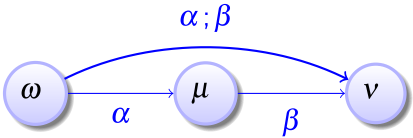


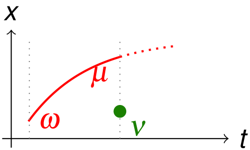
α^*
ω
ν

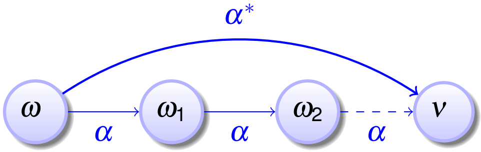
Hybrid Programs: Semantics

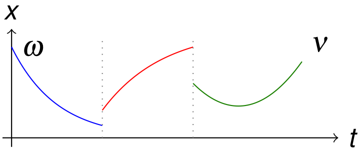




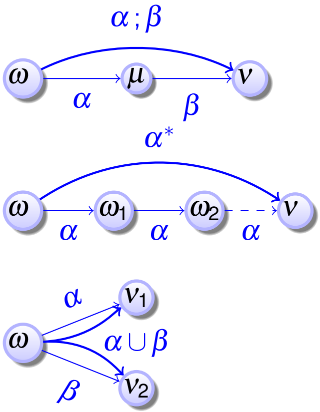


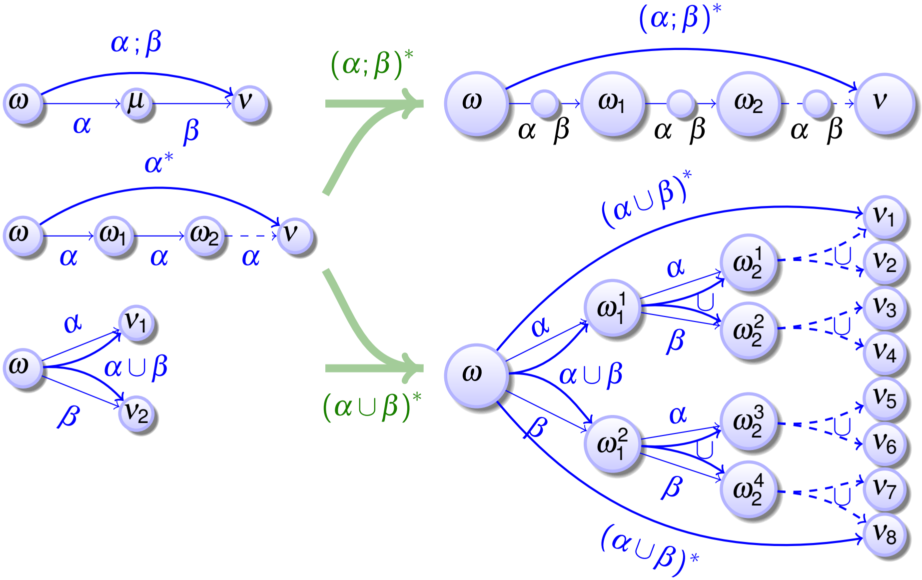






Plug-in for Semantics of Composed Hybrid Programs




$\alpha;\beta$
ω
μ
ν
α
β
α^*
ω_1
ω_2
$\alpha \cup \beta$
ν_1
ν_2
$(\alpha;\beta)^*$
$(\alpha\cup\beta)^*$
ω_1^1
ω_1^2
ω_2^1
ω_2^2
ω_2^3
ω_2^4
$\cup$
ν_3
ν_4
ν_5
ν_6
ν_7
ν_8

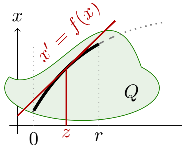
Definition (Syntax of hybrid program α)

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

Definition (Semantics of hybrid programs) $([\![\cdot]\!] : \mathrm{HP} \to \wp(\mathscr{S} \times \mathscr{S}))$

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

compositional



Hybrid Programs: Syntax & Semantics

Definition (Syntax of hybrid program α)

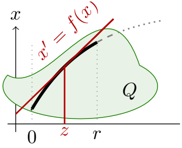
$$\alpha, \beta \ ::= \ x := e \mid ?Q \mid x' = f(x) \,\&\, Q \mid \alpha \cup \beta \mid \alpha ; \beta \mid \alpha^*$$

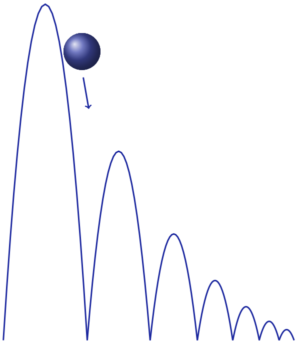
Definition (Semantics of hybrid programs) $([\![\cdot]\!] : \mathrm{HP} \to \wp(\mathscr{S} \times \mathscr{S}))$

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

compositional

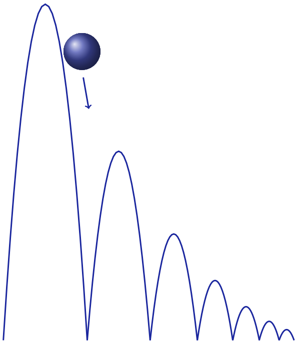
1. $\varphi(z)(x') = \frac{\mathrm{d}\varphi(t)(x)}{\mathrm{d}t}(z)$ exists at all times $0 \leq z \leq r$
2. $\varphi(z) \in [\![x' = f(x) \wedge Q]\!]$ for all times $0 \leq z \leq r$
3. $\varphi(z) = \varphi(0)$ except at x, x'





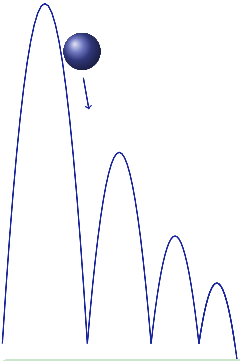
Example (Quantum the Bouncing Ball)

Quantum the Acrophobic Bouncing Ball



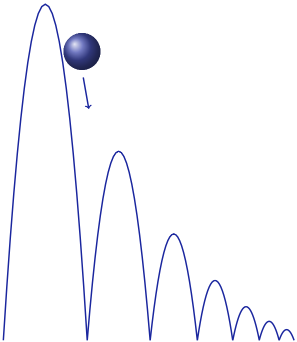
Example (Quantum the Bouncing Ball)

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



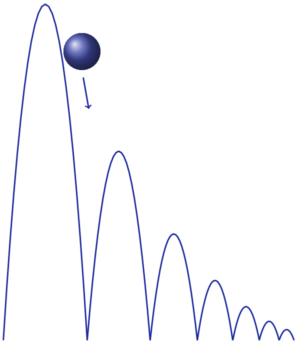
Example (Quantum the Bouncing Ball)

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



Example (Quantum the Bouncing Ball)

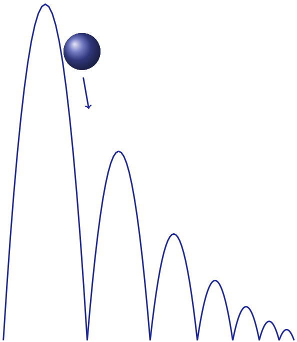
$$\{x' = v, v' = -g \,\&\, x \geq 0\}$$



Example (Quantum the Bouncing Ball)

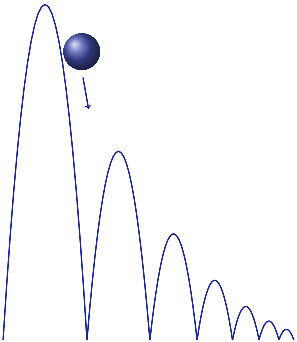
$$\{x' = v, v' = -g \,\&\, x \geq 0\};$$
$$\text{if}(x = 0)\ \ v := -cv$$

Quantum the Acrophobic Bouncing Ball



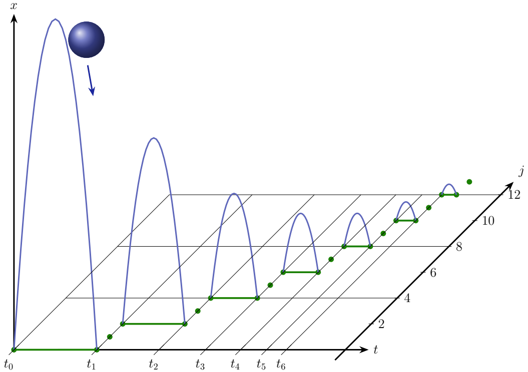
Example (Quantum the Bouncing Ball)

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



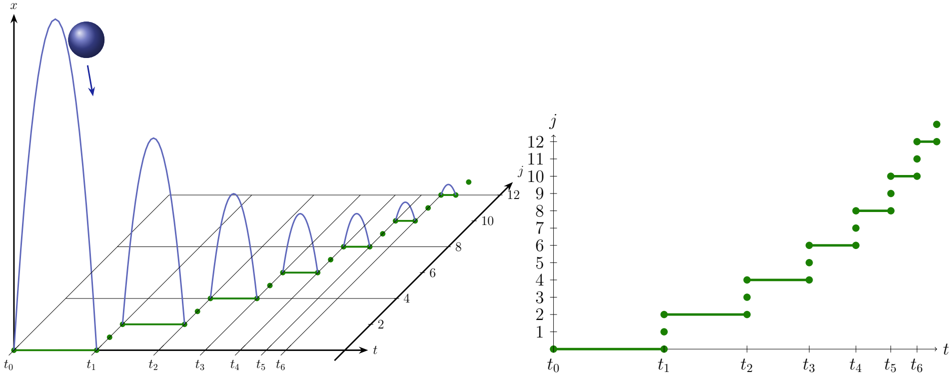
Example (Quantum the Bouncing Ball)

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



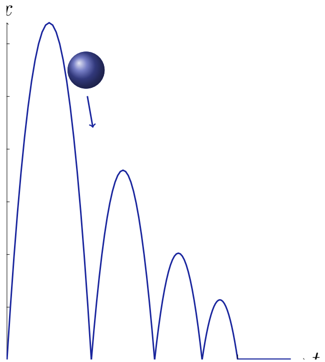
Example (Quantum the Bouncing Ball)

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



Example (Quantum the Bouncing Ball)

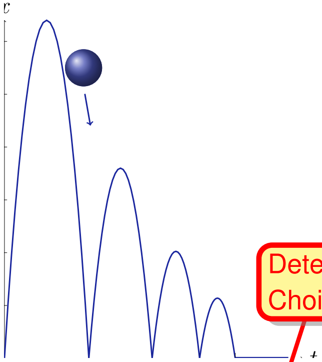
$$\big(\{x' = v, v' = -g \,\&\, x \geq 0\};$$
$$\text{if}(x = 0)\;\; v := -cv\big)^*$$



$\text{if}(Q)\,\alpha\,\text{else}\,\beta \equiv$

Example (Quantum the Bouncing Ball)

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



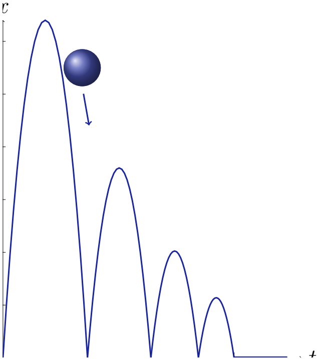
$$\text{if}(Q)\,\alpha\,\text{else}\,\beta \equiv (?Q;\alpha) \cup (?\neg Q;\beta)$$

Determ. Choice

Nondet. Choice

Example (Quantum the Bouncing Ball)

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

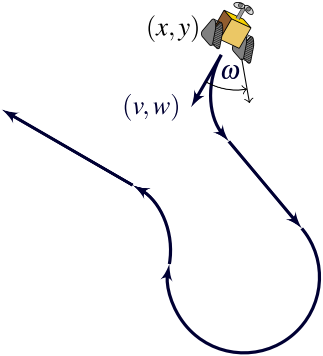


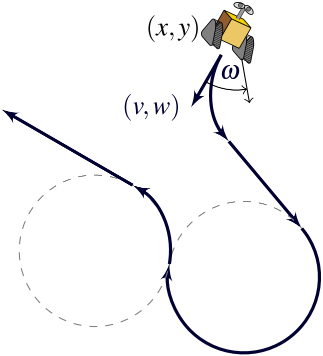
Nondet. Assign

Test Limits

Example (Quantum the Bouncing Ball)

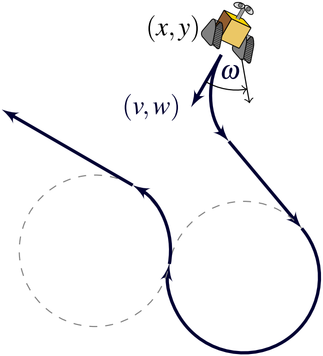
$$\Big(\{x' = v, v' = -g \,\&\, x \geq 0\};$$
$$\text{if}(x = 0)\,(c := *; ?c \geq 0; v := -cv)\Big)^*$$


(x,y)
ω
(v,w)



Example (Runaround Robot)

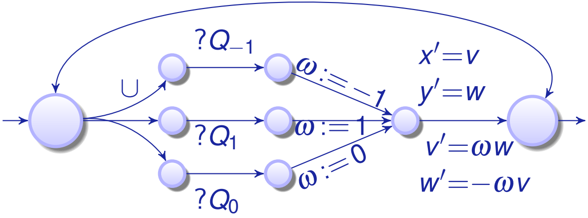
$$\big((\omega := -1 \cup \omega := 1 \cup \omega := 0);$$
$$\{x' = v, y' = w, v' = \omega w, w' = -\omega v\}\big)^*$$

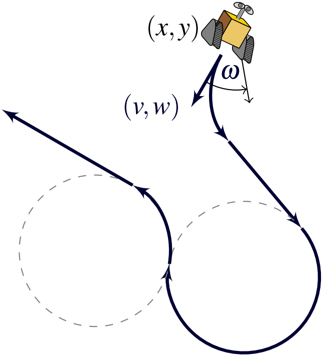


Example (Runaround Robot)

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

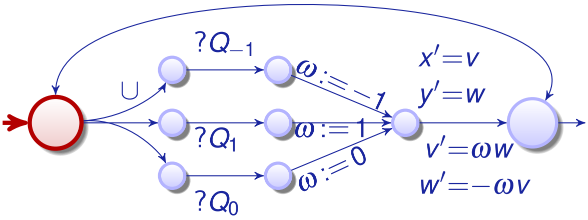
Runaround Robot

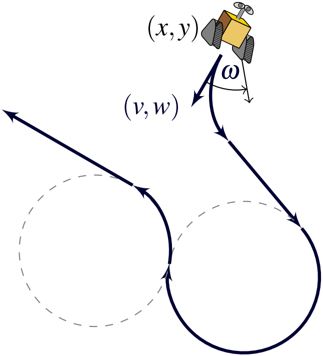




Example (Runaround Robot)

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

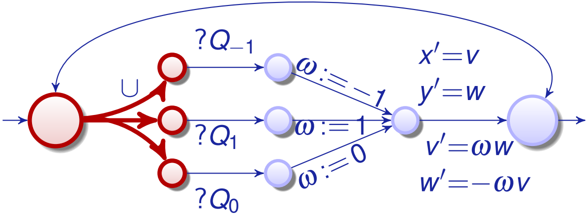


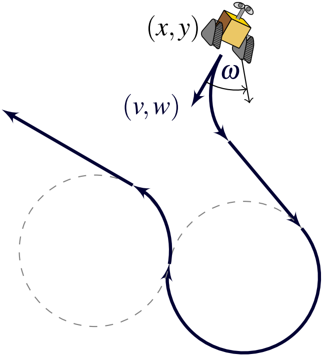


Example (Runaround Robot)

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

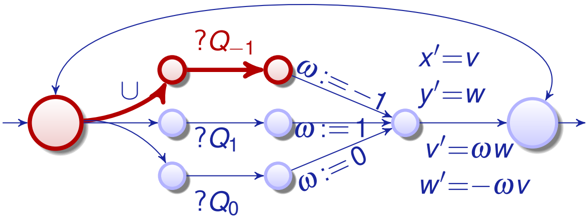
Runaround Robot

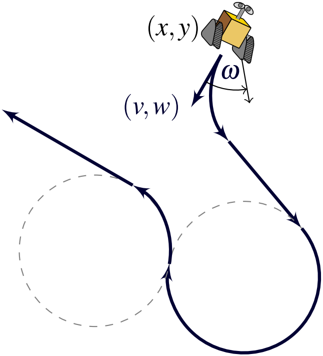




Example (Runaround Robot)

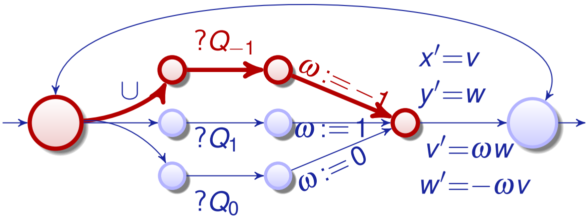
$$\Big(\big(?Q_{-1}; \omega := -1 \cup ?Q_1; \omega := 1 \cup ?Q_0; \omega := 0\big); \\ \{x' = v, y' = w, v' = \omega w, w' = -\omega v\}\Big)^*$$

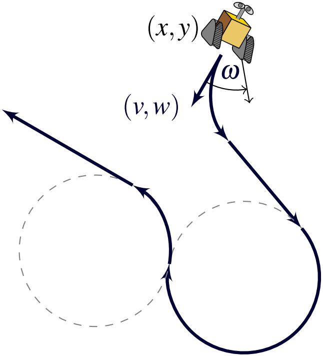




Example (Runaround Robot)

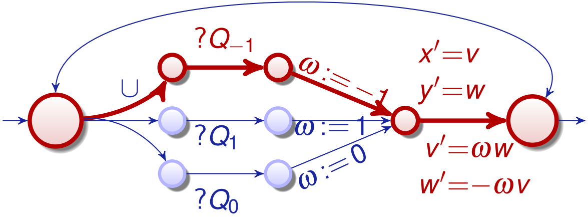
$$\Big(\big(?Q_{-1}; \omega := -1 \cup ?Q_1; \omega := 1 \cup ?Q_0; \omega := 0\big);$$
$$\{x' = v, y' = w, v' = \omega w, w' = -\omega v\}\Big)^*$$

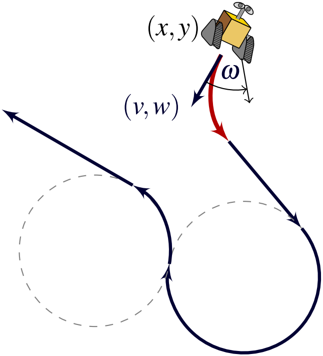




Example (Runaround Robot)

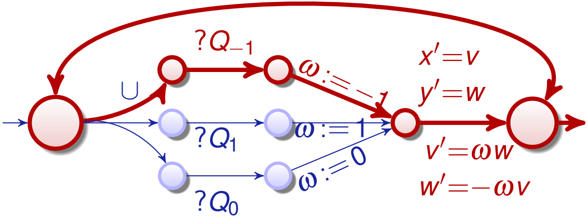
$$\Big(\big(?Q_{-1};\, \omega := -1 \cup ?Q_1;\, \omega := 1 \cup ?Q_0;\, \omega := 0\big);$$
$$\{x' = v, y' = w, v' = \omega w, w' = -\omega v\}\Big)^*$$

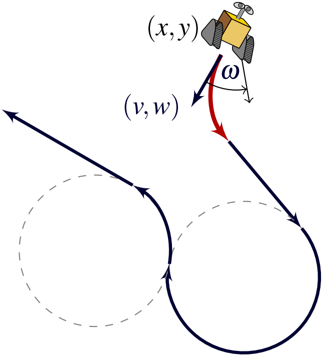




Example (Runaround Robot)

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

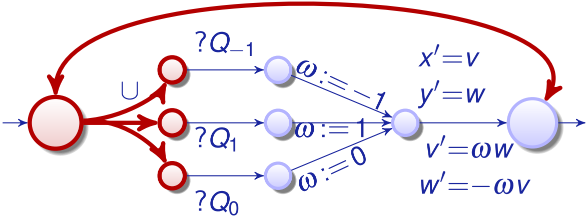


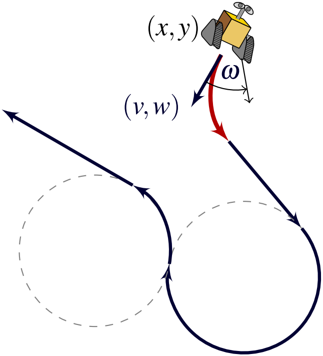


Example (Runaround Robot)

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

Runaround Robot

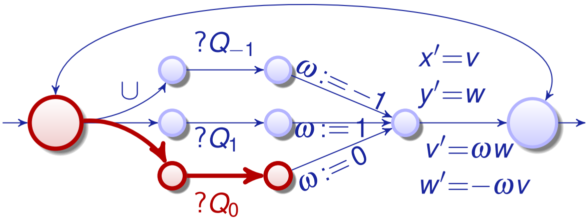


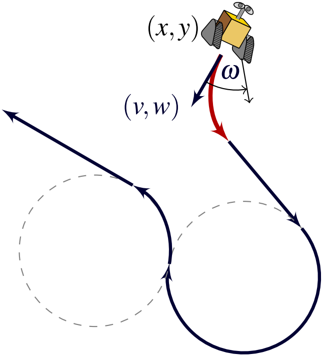


Example (Runaround Robot)

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

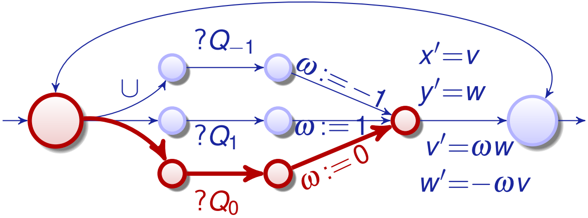
Runaround Robot

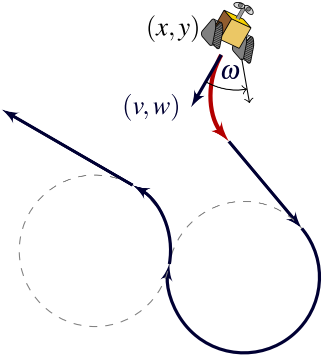




Example (Runaround Robot)

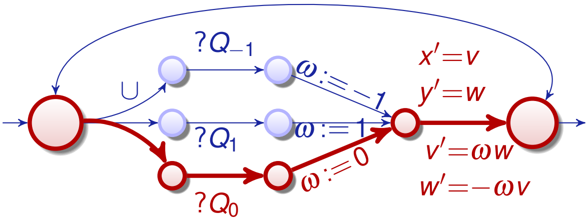
$$\Big(\big(?Q_{-1}; \omega := -1 \cup ?Q_1; \omega := 1 \cup ?Q_0; \omega := 0\big);$$
$$\{x' = v, y' = w, v' = \omega w, w' = -\omega v\}\Big)^*$$

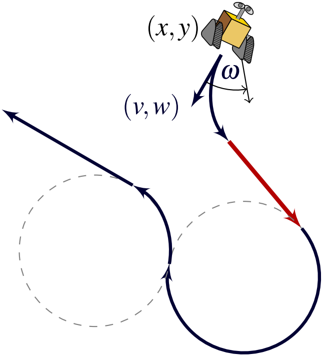




Example (Runaround Robot)

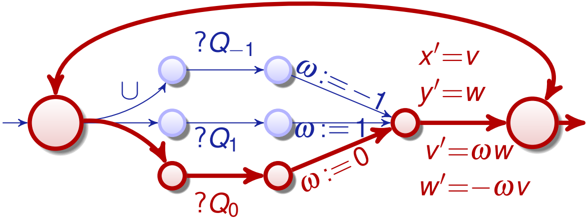
$$\big((?Q_{-1};\omega:=-1 \cup ?Q_1;\omega:=1 \cup ?Q_0;\omega:=0);$$
$$\{x'=v, y'=w, v'=\omega w, w'=-\omega v\}\big)^*$$

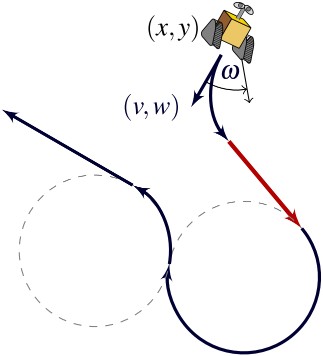




Example (Runaround Robot)

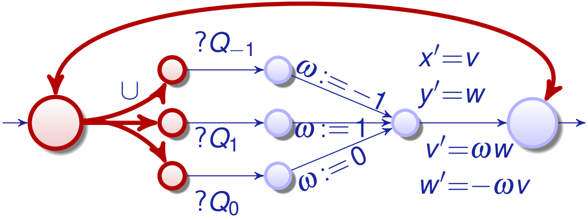
$$\Big(\big(?Q_{-1}; \omega := -1 \cup ?Q_1; \omega := 1 \cup ?Q_0; \omega := 0\big); \{x' = v, y' = w, v' = \omega w, w' = -\omega v\}\Big)^*$$

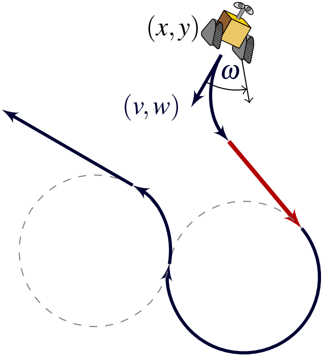




Example (Runaround Robot)

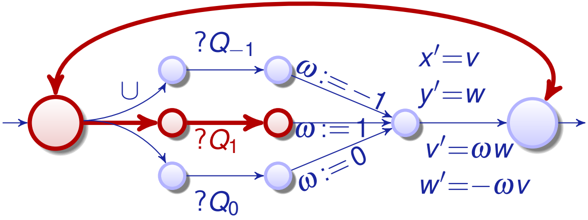
$$\big((?Q_{-1};\omega := -1 \cup ?Q_1;\omega := 1 \cup ?Q_0;\omega := 0);$$
$$\{x' = v, y' = w, v' = \omega w, w' = -\omega v\}\big)^*$$

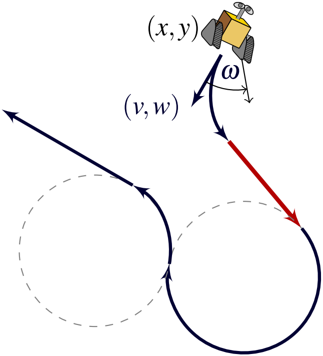




Example (Runaround Robot)

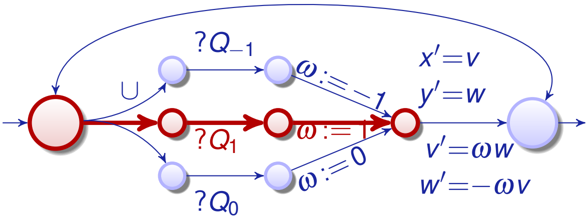
$$\big((?Q_{-1}; \omega := -1 \cup ?Q_1; \omega := 1 \cup ?Q_0; \omega := 0);$$
$$\{x' = v, y' = w, v' = \omega w, w' = -\omega v\}\big)^*$$

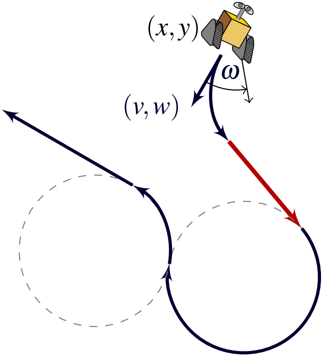




Example (Runaround Robot)

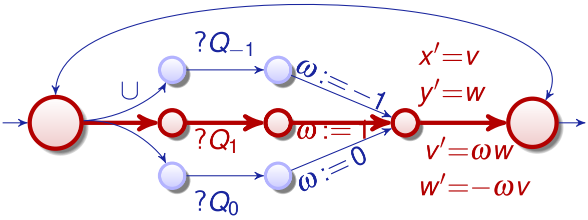
$$\big((?Q_{-1};\omega:=-1 \cup ?Q_1;\omega:=1 \cup ?Q_0;\omega:=0);$$
$$\{x'=v, y'=w, v'=\omega w, w'=-\omega v\}\big)^*$$

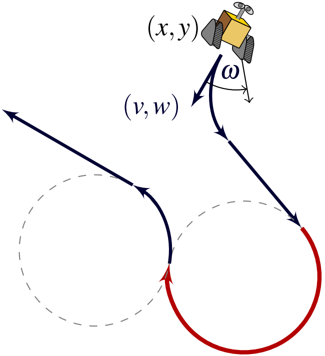




Example (Runaround Robot)

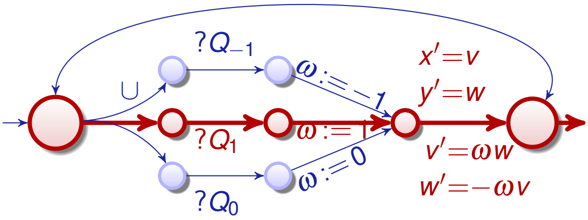
$$\big((?Q_{-1};\omega := -1 \cup ?Q_1;\omega := 1 \cup ?Q_0;\omega := 0);\\ \{x' = v, y' = w, v' = \omega w, w' = -\omega v\}\big)^*$$

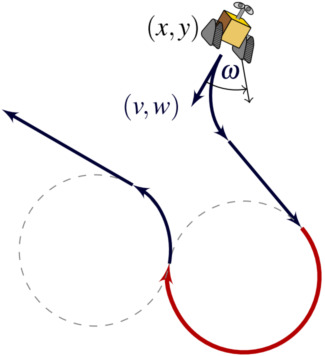




Example (Runaround Robot)

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





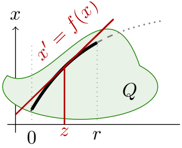
Example (Runaround Robot)

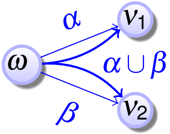
$$\big((?Q_{-1}; \omega := -1 \cup ?Q_1; \omega := 1 \cup ?Q_0; \omega := 0);$$
$$\{x' = v, y' = w, v' = \omega w, w' = -\omega v\}\big)^*$$

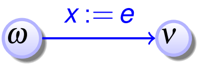
Summary: Modeling CPS

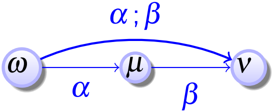
Definition (Hybrid program)

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

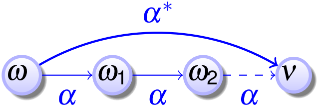








if $\omega \in [\![Q]\!]$

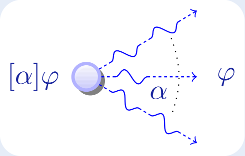


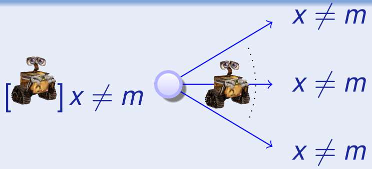
Programming CPS $\neq$ program cyber $\|$ program physics (mutual ignorance)

Outline (Specifying CPS)

CPS Analysis

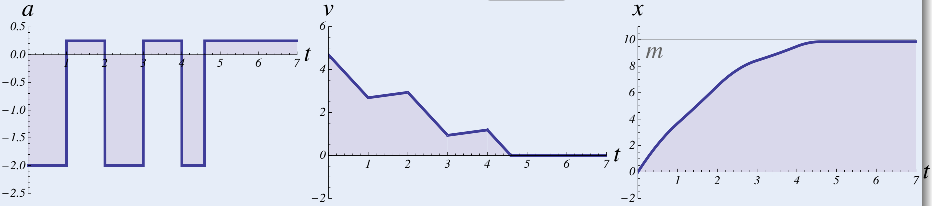
Concept (Differential Dynamic Logic) (JAR'08,LICS'12)





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

all runs



Differential Dynamic Logic: Syntax

Definition (Syntax of differential dynamic logic)

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

$$P, Q ::= e \geq \tilde{e} \mid \neg P \mid P \land Q \mid P \lor Q \mid P \to Q \mid \forall x\, P \mid \exists x\, P \mid [\alpha]P \mid \langle\alpha\rangle P$$

Definition (Syntax of differential dynamic logic)

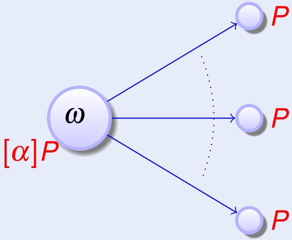
The *formulas* of *differential dynamic logic* are defined by the grammar:

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

Not | And | Or | Imply | All reals | Some real | All runs | Some runs

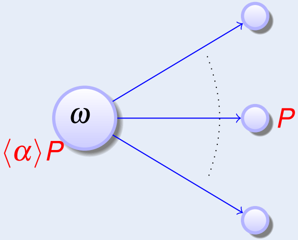
Differential Dynamic Logic dL: Semantics

Definition (dL Formulas)

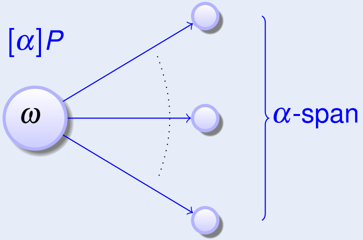


Differential Dynamic Logic dL: Semantics

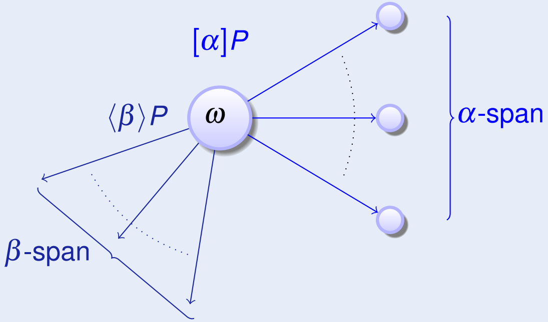
Definition (dL Formulas)



Definition (dL Formulas)

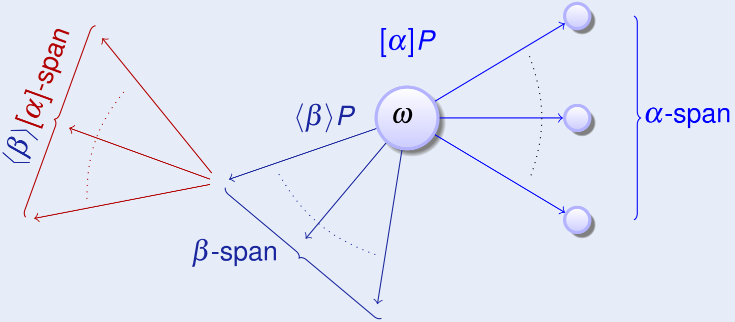


Definition (dL Formulas)



Differential Dynamic Logic dL: Semantics

Definition (dL Formulas)



Differential Dynamic Logic: Syntax & Semantics

Definition (Syntax of differential dynamic logic)

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

$$P, Q ::= e \geq \tilde{e} \mid \neg P \mid P \land Q \mid P \lor Q \mid P \to Q \mid \forall x\, P \mid \exists x\, P \mid [\alpha]P \mid \langle\alpha\rangle P$$

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

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

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

Differential Dynamic Logic: Syntax & Semantics

$[\![P]\!]$ the set of states in which formula P is true

$\omega \models P$ formula P is true in state ω, alias $\omega \in [\![P]\!]$

$\models P$ formula P is valid, i.e., true in all states ω, i.e., $[\![P]\!] = \mathscr{S}$

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

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

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

Differential Dynamic Logic: Syntax & Semantics

$[\![P]\!]$ the set of states in which formula P is true

$\omega \models P$ formula P is true in state ω, alias $\omega \in [\![P]\!]$

$\models P$ formula P is valid, i.e., true in all states ω, i.e., $[\![P]\!] = \mathscr{S}$

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

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

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

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

Differential Dynamic Logic: Syntax & Semantics

$[\![P]\!]$ the set of states in which formula P is true

$\omega \models P$ formula P is true in state ω, alias $\omega \in [\![P]\!]$

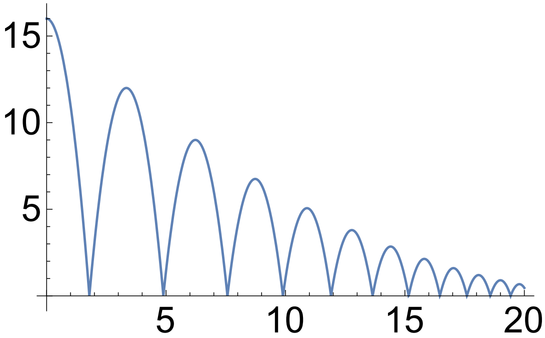
$\models P$ formula P is valid, i.e., true in all states ω, i.e., $[\![P]\!] = \mathscr{S}$

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

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

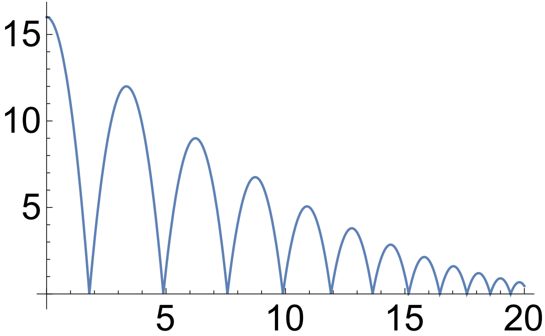
$$
\begin{aligned}
[\![e \geq \tilde{e}]\!] &= \{\omega : \omega[\![e]\!] \geq \omega[\![\tilde{e}]\!]\} \\
[\![\neg P]\!] &= [\![P]\!]^{\complement} = \mathscr{S} \setminus [\![P]\!] \\
[\![P \land Q]\!] &= [\![P]\!] \cap [\![Q]\!] \\
[\![P \lor Q]\!] &= [\![P]\!] \cup [\![Q]\!] \\
[\![P \to Q]\!] &=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

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



Example (Bouncing Ball)

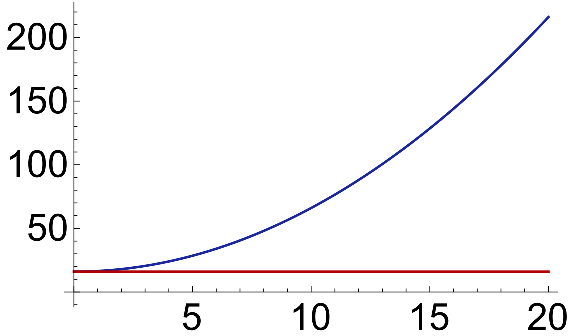
$$\big(\{x' = v, v' = -g \,\&\, x \geq 0\};\ \mathrm{if}(x = 0)\, v := -cv\big)^*$$



Example (Bouncing Ball)

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

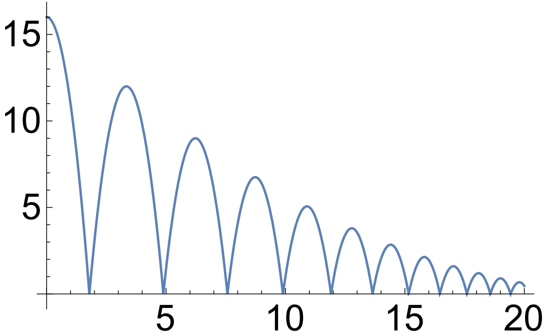
Quantum the Acrophobic Bouncing Ball



Not if $g < 0$ in anti-gravity

Example (Bouncing Ball)

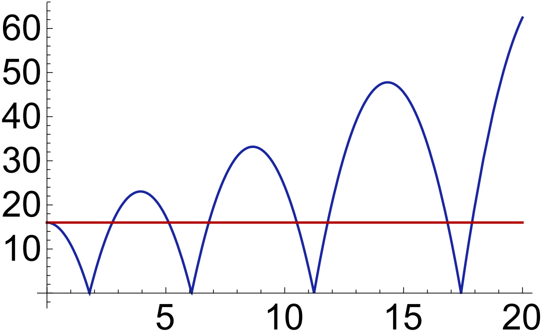
$$H=x\geq 0 \rightarrow [(\{x'=v, v'=-g \,\&\, x\geq 0\}; \text{if}(x=0)\, v:=-cv)^*]\, 0\leq x\leq H$$



Example (Bouncing Ball)

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

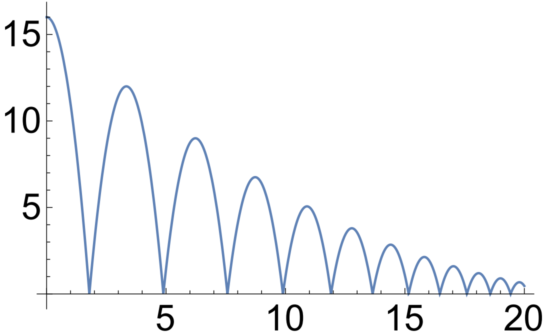
Quantum the Acrophobic Bouncing Ball



Not if $c > 1$ for anti-damping

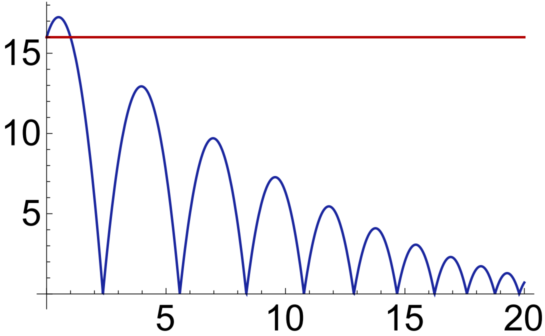
Example (Bouncing Ball)

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



Example (Bouncing Ball)

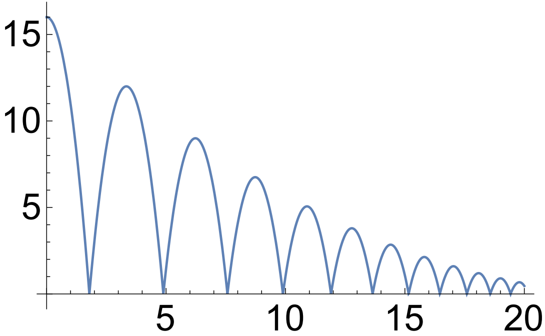
$$1 \geq c \geq 0 \land H = x \geq 0 \land g > 0 \rightarrow \left[\left(\{x' = v, v' = -g \,\&\, x \geq 0\}; \right.\right.$$
$$\left.\left. \text{if}(x = 0)\, v := -cv \right)^* \right] 0 \leq x \leq H$$



Not if $v > 0$ initial climbing

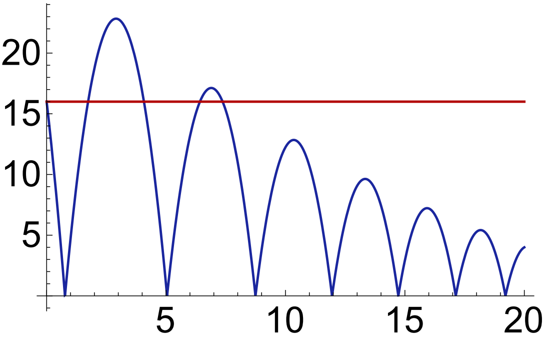
Example (Bouncing Ball)

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



Example (Bouncing Ball)

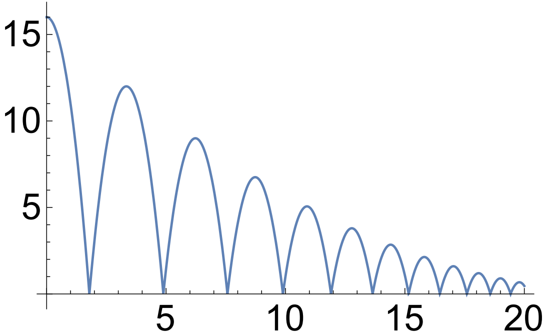
$$\color{red}{v \le 0 \land}\ 1 \ge c \ge 0 \land H = x \ge 0 \land g > 0 \to \left[\left(\{x' = v, v' = -g \,\&\, x \ge 0\};\ \text{if}(x = 0)\, v := -cv\right)^*\right] 0 \le x \le H$$



Not if $v \ll 0$ initial dribbling

Example (Bouncing Ball)

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



Example (Bouncing Ball)

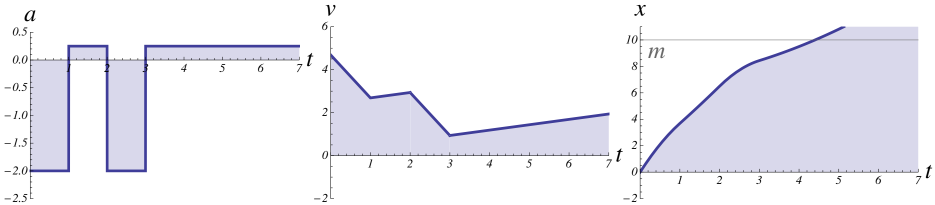
$$v=0 \land 1\geq c\geq 0 \land H=x\geq 0 \land g>0 \rightarrow \left[\left(\{x' = v, v' = -g \,\&\, x \geq 0\};\ \text{if}(x=0)\, v := -cv\right)^*\right] 0\leq x\leq H$$

Ex: Car Control Programs

Repeat control decisions

Example (Single car car_s)

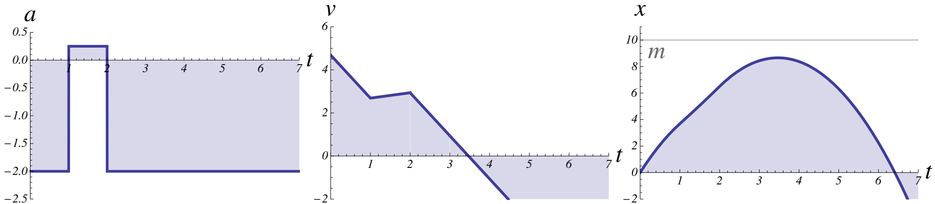
$$\big((a := A \cup a := -b);\ \{x' = v, v' = a\}\big)^*$$



How does this model brake?

Example (Single car car_s)

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

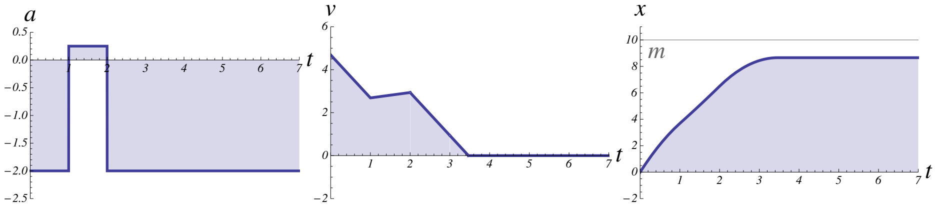


Ex: Car Control Programs

Velocity bound $v \geq 0$ in evolution domain

Example (▸ Single car car_s)

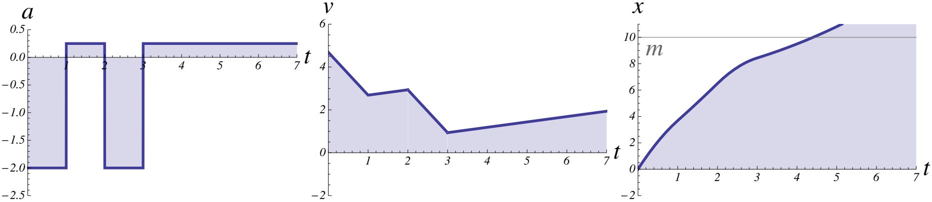
$$\big((\ a := A\ \cup a := -b);\ \{x' = v, v' = a \,\&\, v \geq 0\}\big)^*$$



Acceleration not always safe

Example (Single car car_s)

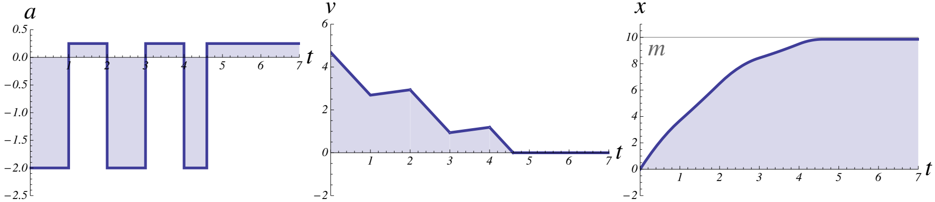
$$\big((\; a := A \;\cup a := -b);\; \{x' = v, v' = a \,\&\, v \geq 0\}\big)^*$$



Acceleration condition $?Q$

Example (Single car car_s)

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



Ex: Car Control Properties

time-triggered

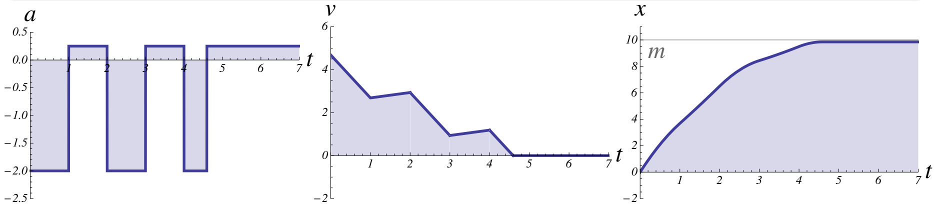
$Q \equiv$

Example (Single car car_ε time-triggered)

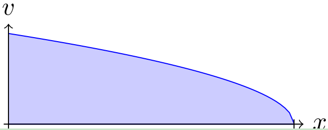
$$\Big(\big((?Q; a := A) \cup a := -b\big); t := 0; \{x' = v, v' = a, t' = 1 \,\&\, v \geq 0 \land t \leq \varepsilon\}\Big)^*$$

Example (Safely stays before traffic light m)

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



$Q \equiv$

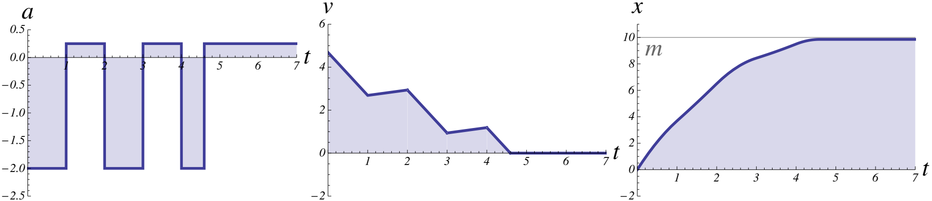


Example (Single car car_ε time-triggered)

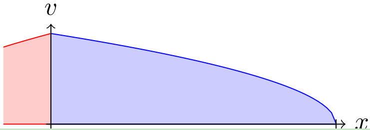
$$\Big(\big((?Q; a := A) \cup a := -b\big); t := 0; \{x' = v, v' = a, t' = 1 \,\&\, v \geq 0 \land t \leq \varepsilon\}\Big)^*$$

Example (▶ Safely stays before traffic light m)

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



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

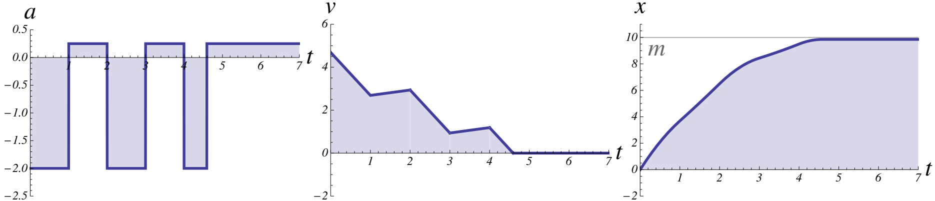


Example (Single car car_ε time-triggered)

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

Example (Safely stays before traffic light m)

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



Ex: Car Control Properties

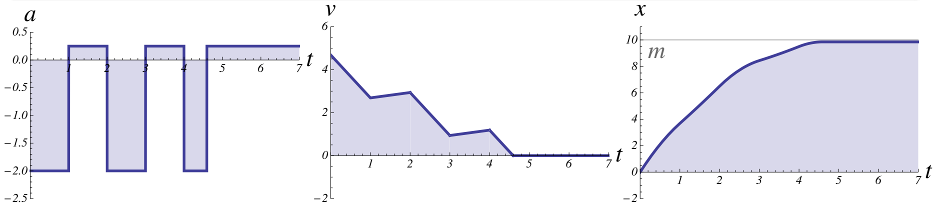
$$Q \equiv 2b(m-x) \geq v^2 + \big(A+b\big)\big(A\varepsilon^2 + 2\varepsilon v\big)$$

Example (Single car car_ε time-triggered)

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

Example (Live, can move everywhere)

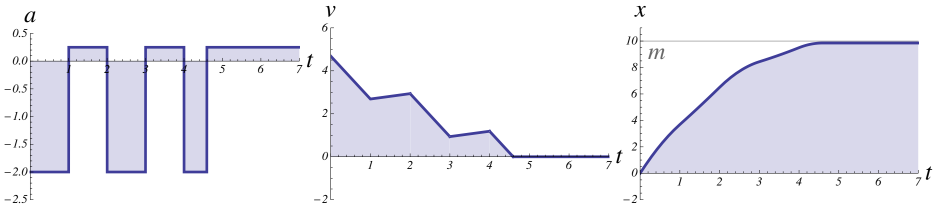
$$\varepsilon > 0 \land A > 0 \land b > 0 \rightarrow \forall p \exists m \langle car_\varepsilon \rangle\, x \geq p$$



Example (dL-based model-predictive control design)

$$\_\_\_\_\_\_\_\_ \wedge v \geq 0 \wedge A \geq 0 \wedge b > 0 \rightarrow$$

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

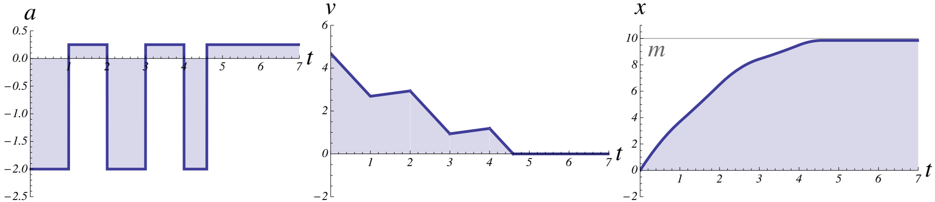


Example (dL-based model-predictive control design)

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

$$[((\ (?\underline{\qquad\qquad\qquad\qquad\qquad\qquad};\ a := A) \cup a := -b);$$

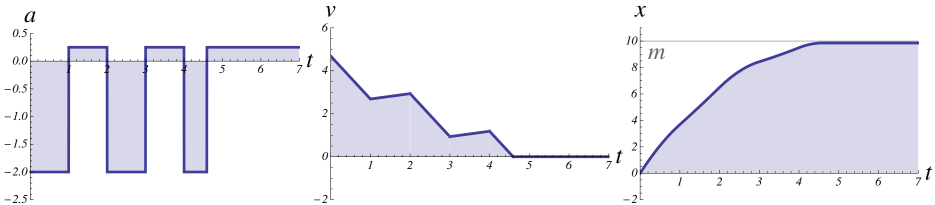
$$t := 0;\ \{x' = v, v' = a, t' = 1 \,\&\, v \geq 0 \land t \leq \varepsilon\})^*]\, x \leq m$$



Example (dL-based model-predictive control design)

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

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



Example (dL-based model-predictive control design)

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

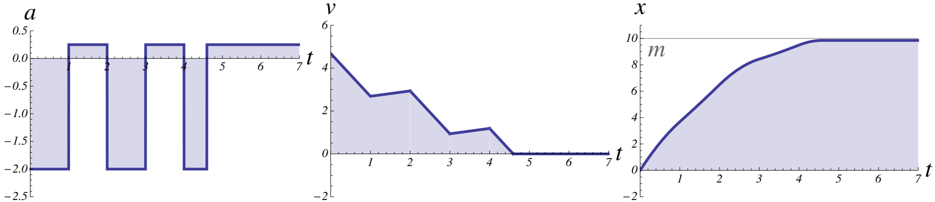
$$\Big[\Big(\Big($$

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

$$a := A)$$

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

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



Example (dL-based model-predictive control design)

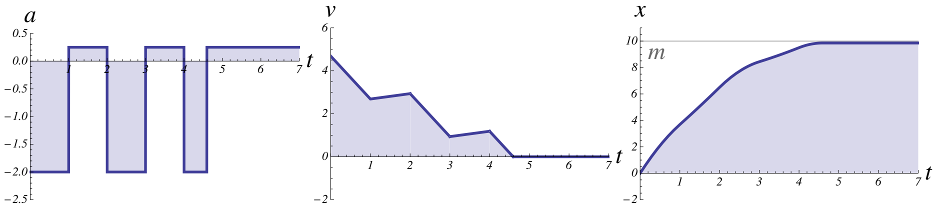
$$\frac{[x'=v,v'=-b]x\le m}{} \land v\ge 0 \land A\ge 0\land b>0 \rightarrow$$

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

$$a:=A\big)$$

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

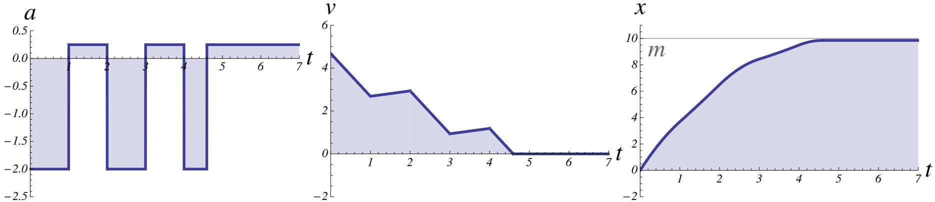
$$t:=0;\ \{x'=v,v'=a,t'=1\,\&\,v\ge 0\land t\le\varepsilon\}\Big)^*\Big]\,x\le m$$



Example (dL-based model-predictive control design)

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

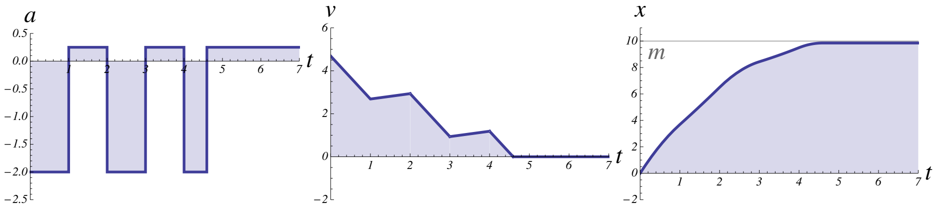
$$\Big[\big(\big((?\underline{[t := 0; x' = v, v' = A, t' = 1 \,\&\, v \geq 0 \land t \leq \varepsilon][x' = v, v' = -b]x \leq m}; \; a := A) \cup a := -b); \; t := 0; \; \{x' = v, v' = a, t' = 1 \,\&\, v \geq 0 \land t \leq \varepsilon\}\big)^*\Big]\, x \leq m$$



Example (dL-based model-predictive control design)

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

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

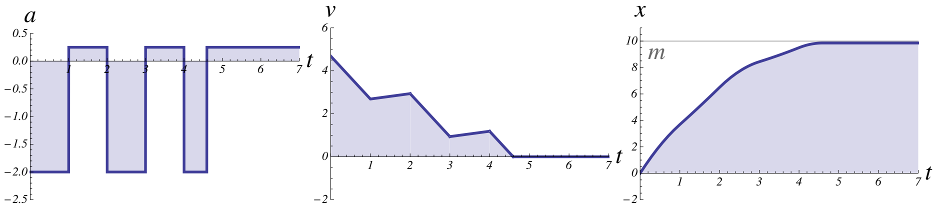


Example (dL-based model-predictive control design)

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

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

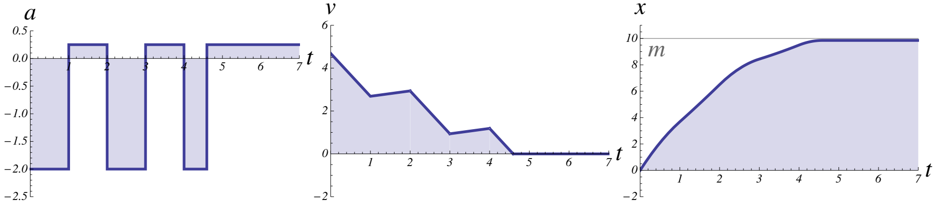
$$t:=0;\; \{x'=v, v'=a, t'=1 \,\&\, v \ge 0 \land t \le \varepsilon\})^*]\, x \le m$$



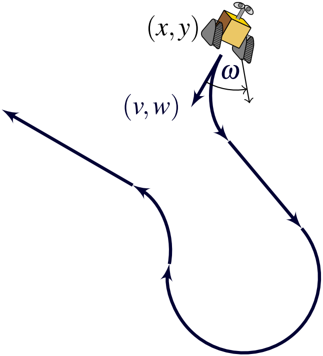
Example (dL-based model-predictive control design)

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

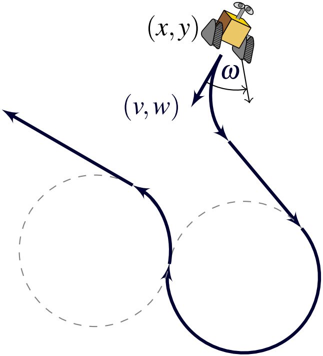
$$\Big[\Big(\Big(\big(?\underline{\color{red}{2b(m-x) \ge v^2 + (A+b)(A\varepsilon^2 + 2\varepsilon v)}};\ a := A\big) \cup a := -b\big);\ t := 0;\ \{x' = v, v' = a, t' = 1 \,\&\, v \ge 0 \land t \le \varepsilon\}\Big)^*\Big]\, x \le m$$



Exercise: Runaround Robot

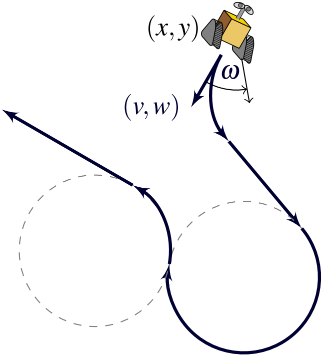


Exercise: Runaround Robot



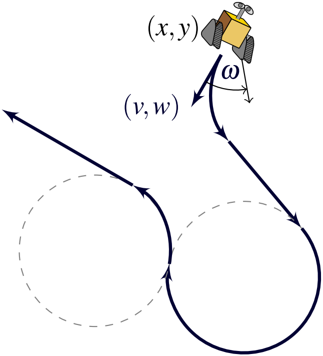
Example (Runaround Robot)

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



Example (Runaround Robot)

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



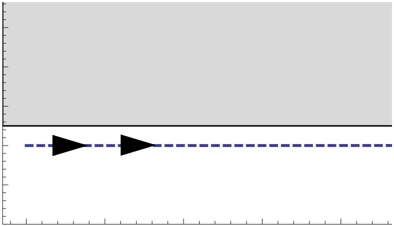
Example (Runaround Robot)

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

Exercise: TwoCar Control One Car to Follow Another

Model two cars and control one car to safely follow the leader car.

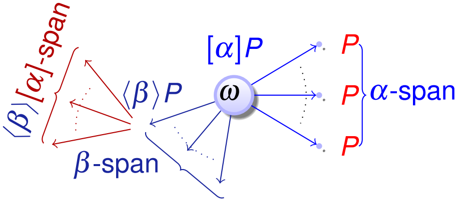
- A maximum acceleration (magnitude)
- B maximum braking (magnitude)
- T maximum reaction time
- x, v, a position, velocity, acceleration of follower car to be controlled
- likewise for lead car, uncontrolled
- motion on a straight line



Summary: Specifying CPS

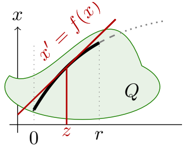
Definition (Differential dynamic logic)

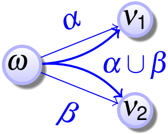
$$P, Q ::= e \geq \tilde{e} \mid \neg P \mid P \wedge Q \mid P \vee Q \mid P \rightarrow Q \mid \forall x\, P \mid \exists x\, P \mid [\alpha]P \mid \langle\alpha\rangle P$$

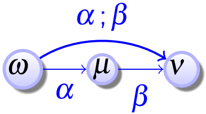


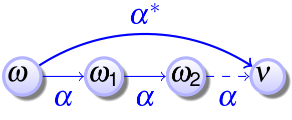
Definition (Hybrid program)

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







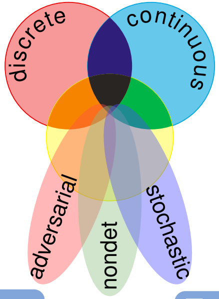


Outline (Proving CPS)

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

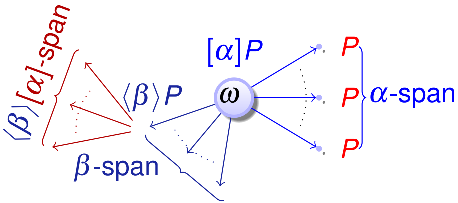
Exploiting compositionality tames CPS complexity.

Analytic simplification

Summary: Specifying CPS

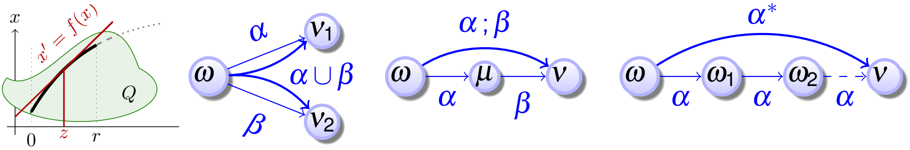
Definition (Differential dynamic logic)

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



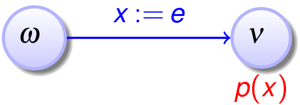
Definition (Hybrid program)

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

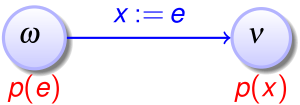


Dynamic Axioms for Dynamical Systems

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

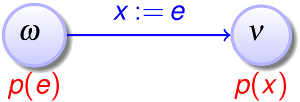


$$[:=]\quad [x := e]p(x) \leftrightarrow p(e)$$

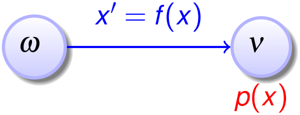


Dynamic Axioms for Dynamical Systems

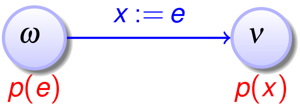
$[:=]\ \ [x := e]p(x) \leftrightarrow p(e)$



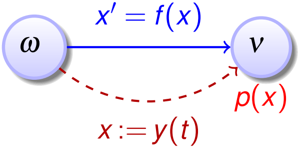
$[']\ \ [x' = f(x)]p(x) \leftrightarrow$



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

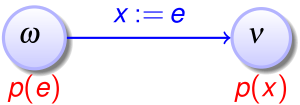


$['] \ [x' = f(x)]p(x) \leftrightarrow \qquad [x := y(t)]p(x)$

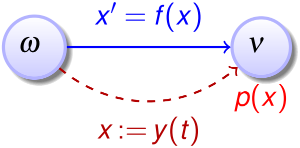


Dynamic Axioms for Dynamical Systems

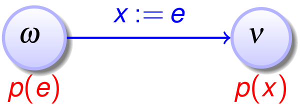
$[:=]\ [x := e]p(x) \leftrightarrow p(e)$

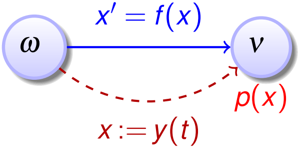


$[']\ [x' = f(x)]p(x) \leftrightarrow \forall t \geq 0\, [x := y(t)]p(x)$



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

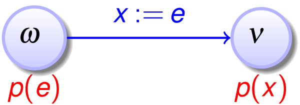


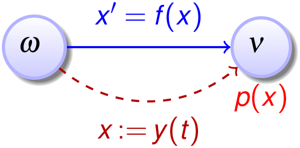


['] $[x' = f(x)]p(x) \leftrightarrow \forall t \geq 0\, [x := y(t)]p(x)$

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

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



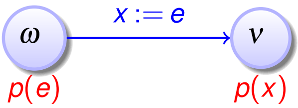


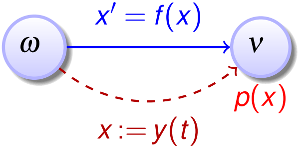
$['\,]\ [x' = f(x)]p(x) \leftrightarrow \forall t{\geq}0\, [x := y(t)]p(x)$

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

Dynamic Axioms for Dynamical Systems

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

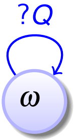




$['\,]\ [x' = f(x)]p(x) \leftrightarrow \forall t{\geq}0\, [x := y(t)]p(x)$

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

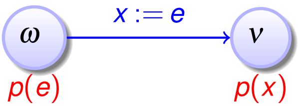
$[?]\ [?Q]P \leftrightarrow$

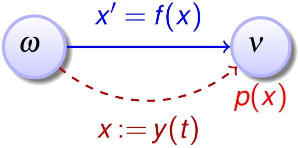


if $\omega \in [\![Q]\!]$

Dynamic Axioms for Dynamical Systems

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

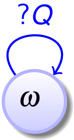




$[']$ $[x' = f(x)]p(x) \leftrightarrow \forall t \geq 0\, [x := y(t)]p(x)$

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

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

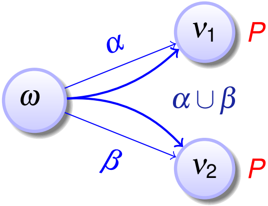


if $\omega \in [\![Q]\!]$

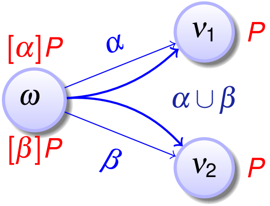
Dynamic Axioms for Dynamical Systems

compositional semantics $\Rightarrow$ compositional proofs

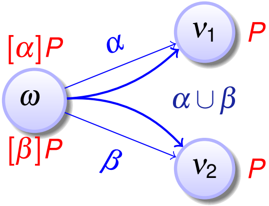
[∪] $[\alpha \cup \beta]P \leftrightarrow$



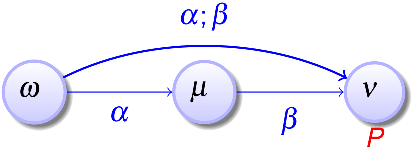
$[\cup]$ $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$



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

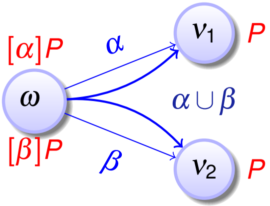


[;] $[\alpha;\beta]P \leftrightarrow$

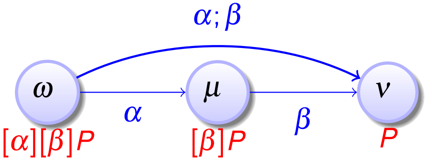


Dynamic Axioms for Dynamical Systems

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

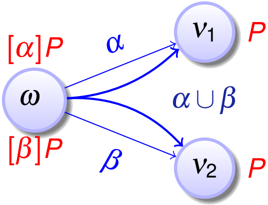


[;] $[\alpha;\beta]P \leftrightarrow [\alpha][\beta]P$

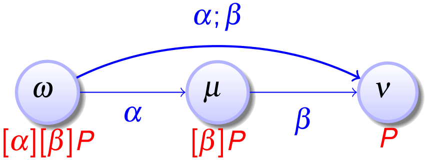


Dynamic Axioms for Dynamical Systems

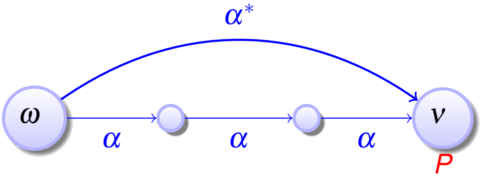
$[\cup]$ $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \land [\beta]P$



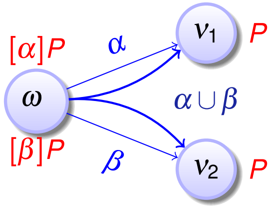
$[;]$ $[\alpha;\beta]P \leftrightarrow [\alpha][\beta]P$



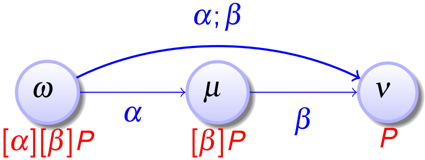
$[^*]$ $[\alpha^*]P \leftrightarrow$



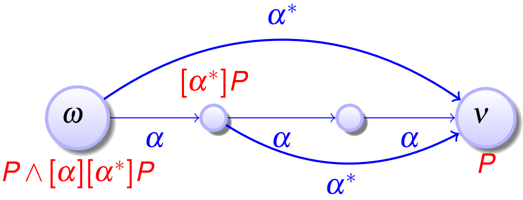
$[\cup]$ $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \land [\beta]P$



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

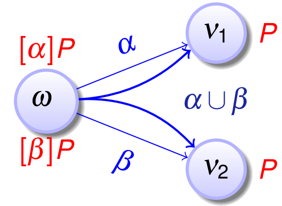


$[^*]$ $[\alpha^*]P \leftrightarrow P \land [\alpha][\alpha^*]P$

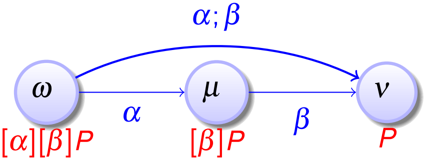


Dynamic Axioms for Dynamical Systems

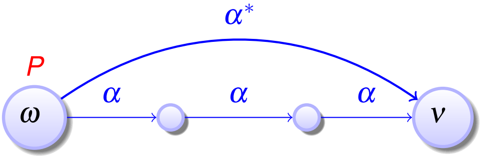
[∪] $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$



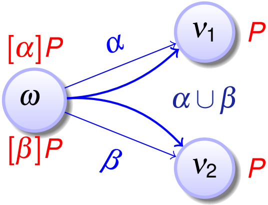
[;] $[\alpha;\beta]P \leftrightarrow [\alpha][\beta]P$



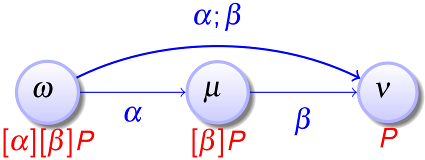
I $[\alpha^*]P \leftrightarrow P \wedge$



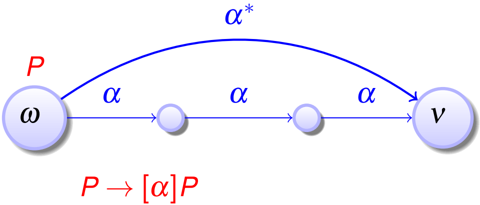
[∪] $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$



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

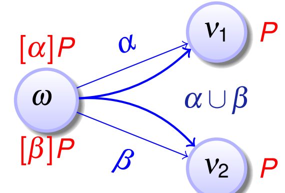


I $[\alpha^*]P \leftrightarrow P \wedge \qquad (P \rightarrow [\alpha]P)$

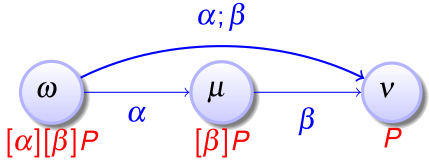


Dynamic Axioms for Dynamical Systems

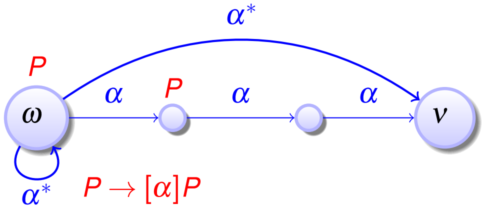
$[\cup]$ $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$



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

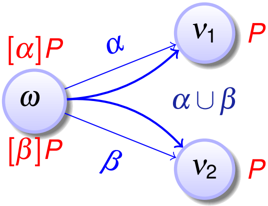


I $[\alpha^*]P \leftrightarrow P \wedge [\alpha^*](P \rightarrow [\alpha]P)$

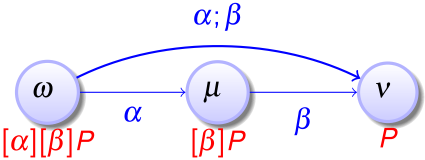


Dynamic Axioms for Dynamical Systems

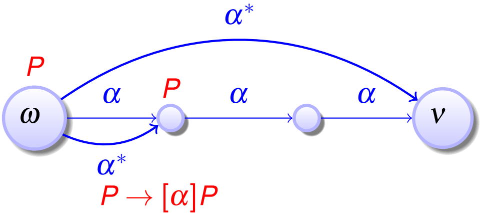
[∪] $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$



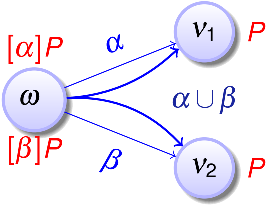
[;] $[\alpha;\beta]P \leftrightarrow [\alpha][\beta]P$



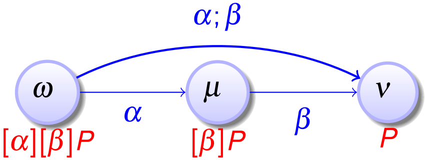
I $[\alpha^*]P \leftrightarrow P \wedge [\alpha^*](P \rightarrow [\alpha]P)$



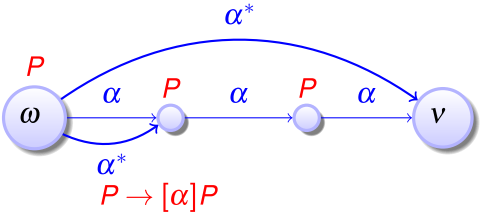
[∪] $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \land [\beta]P$



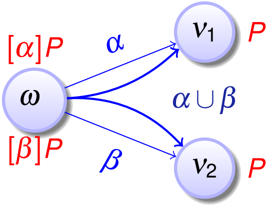
[;] $[\alpha;\beta]P \leftrightarrow [\alpha][\beta]P$



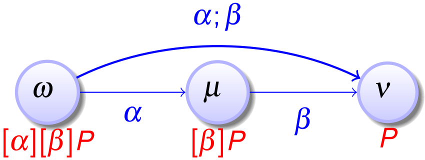
I $[\alpha^*]P \leftrightarrow P \land [\alpha^*](P \rightarrow [\alpha]P)$



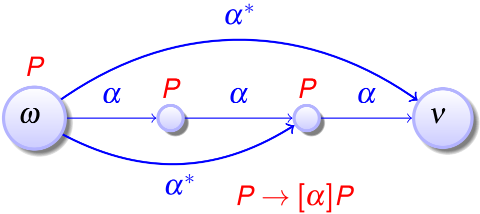
[∪] $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$



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

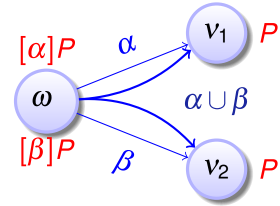


I $[\alpha^*]P \leftrightarrow P \wedge [\alpha^*](P \rightarrow [\alpha]P)$

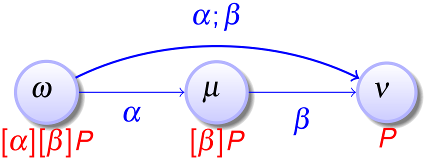


Dynamic Axioms for Dynamical Systems

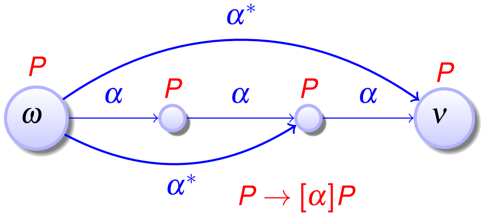
$[\cup]$ $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$



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

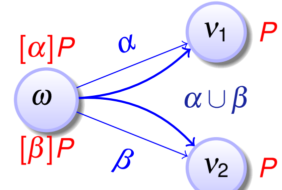


I $[\alpha^*]P \leftrightarrow P \wedge [\alpha^*](P \rightarrow [\alpha]P)$

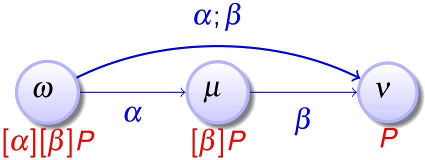


Dynamic Axioms for Dynamical Systems

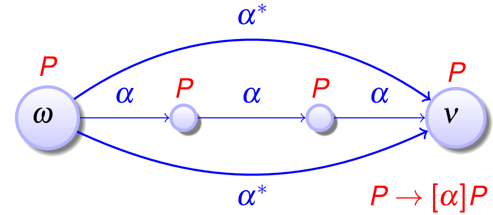
$[\cup]$ $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$



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



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

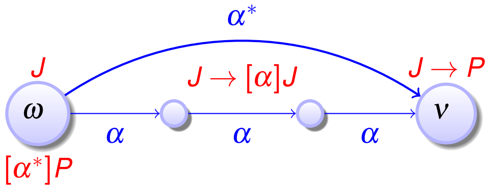


Proof Rule: Loop Invariants

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

Lemma (Loop invariant rule is derived syntactically)

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



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

Proof Rule: Loop Invariants

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

Lemma (Loop invariant rule is derived syntactically)

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

Proof (Derived rule).

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

□

Proof Rule: Loop Invariants

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

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).

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

□

Finding invariant J can be a challenge.

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

Differential Dynamic Logic: Axiomatization

equations of truth

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

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

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

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

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

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

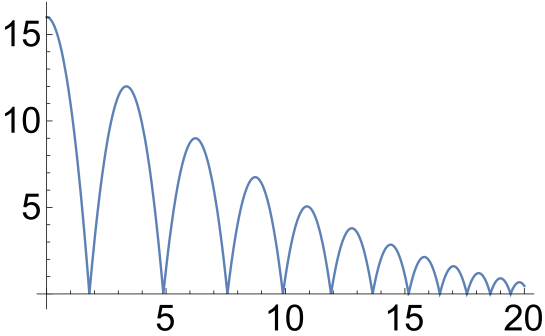
K $[\alpha](P \rightarrow Q) \rightarrow ([\alpha]P \rightarrow [\alpha]Q)$

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

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

LICS'12,JAR'17

Quantum the Acrophobic Bouncing Ball



Example (Bouncing Ball)

$$v{=}0 \land 1{\geq}c{\geq}0 \land H{=}x{\geq}0 \land g{>}0 \to \Big[\Big(\{x' = v, v' = -g \,\&\, x \geq 0\};$$
$$\text{if}(x = 0)\, v := -cv\Big)^*\Big]\, 0{\leq}x{\leq}H$$

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

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

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

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

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

$$\text{loop}\ \dfrac{A \to \mathrm{j}(x,v) \qquad \dfrac{\mathrm{j}(x,v) \to [\mathrm{grav}; (?x{=}0; v{:=}{-}cv \cup ?x{\neq}0)]\mathrm{j}(x,v)}{\mathrm{j}(x,v) \to [\mathrm{grav}; (?x{=}0; v{:=}{-}cv \cup ?x{\neq}0)]\mathrm{j}(x,v)} \qquad \mathrm{j}(x,v) \to B(x,v)}{A \to [\big(\mathrm{grav}; (?x{=}0; v{:=}{-}cv \cup ?x{\neq}0)\big)^*]B(x,v)}$$

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

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

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

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

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

$$A \equiv 0 \le x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \ge c \ge 0$$

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

$$\mathrm{grav} \equiv \{x' = v, v' = -g \,\&\, x \ge 0\}$$

$$\dfrac{\dfrac{\dfrac{\text{j}(x,v)\rightarrow[\text{grav}]\text{j}(x,v) \qquad \dfrac{}{\text{j}(x,v)\rightarrow[?x=0;\, v:=-cv \cup ?x\neq 0]\text{j}(x,v)}}{\text{j}(x,v)\rightarrow[\text{grav}][?x=0;\, v:=-cv \cup ?x\neq 0]\text{j}(x,v)}\;\text{MR}}{\text{j}(x,v)\rightarrow[\text{grav};(?x=0;\, v:=-cv \cup ?x\neq 0)]\text{j}(x,v)}\;[;]}{}$$

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

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

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

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

$$
\text{loop}\;\dfrac{A\to \text{j}(x,v) \qquad \dfrac{[;]\;\dfrac{\text{MR}\;\dfrac{\text{j}(x,v)\to[\text{grav}]\text{j}(x,v) \qquad [\cup]\;\dfrac{\dfrac{}{\text{j}(x,v)\to[?x=0;v:=-cv]\text{j}(x,v)\land[?x\neq0]\text{j}(x,v)}}{\text{j}(x,v)\to[?x=0;v:=-cv\cup ?x\neq0]\text{j}(x,v)}}{\text{j}(x,v)\to[\text{grav}][?x=0;v:=-cv\cup ?x\neq0]\text{j}(x,v)}}{\text{j}(x,v)\to[\text{grav};(?x=0;v:=-cv\cup ?x\neq0)]\text{j}(x,v)}}{\text{j}(x,v)\to[\text{grav};(?x=0;v:=-cv\cup ?x\neq0)]\text{j}(x,v)} \qquad \text{j}(x,v)\to B(x,v)}{A\to\left[\left(\text{grav};(?x=0;v:=-cv\cup ?x\neq0)\right)^*\right]B(x,v)}
$$

$$A \equiv 0\le x\land x=H\land v=0\land g>0\land 1\ge c\ge 0$$

$$B(x,v)\equiv 0\le x\land x\le H$$

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

$$
\dfrac{A \to j(x,v) \qquad \dfrac{\dfrac{j(x,v) \to [\text{grav}]j(x,v) \quad [\cup]\dfrac{\wedge R\dfrac{\overline{j(x,v) \to [?x=0; v:=-cv]j(x,v)} \qquad \overline{j(x,v) \to [?x\neq 0]j(x,v)}}{j(x,v) \to [?x=0; v:=-cv]j(x,v) \wedge [?x\neq 0]j(x,v)}}{j(x,v) \to [?x=0; v:=-cv \cup ?x\neq 0]j(x,v)}}{\text{MR}\; j(x,v) \to [\text{grav}][?x=0; v:=-cv \cup ?x\neq 0]j(x,v)}}{[;]\; \dfrac{j(x,v) \to [\text{grav}; (?x=0; v:=-cv \cup ?x\neq 0)]j(x,v)}{j(x,v) \to [\text{grav}; (?x=0; v:=-cv \cup ?x\neq 0)]j(x,v)}} \qquad j(x,v) \to B(x,v)}{\text{loop}\; A \to [\big(\text{grav}; (?x=0; v:=-cv \cup ?x\neq 0)\big)^*]B(x,v)}
$$

$$A \equiv 0 \le x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \ge c \ge 0$$

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

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

$$
\text{loop}\;\dfrac{A\to \mathrm{j}(x,v) \qquad [;]\,\dfrac{\text{MR}\,\dfrac{\mathrm{j}(x,v)\to[\mathrm{grav}]\mathrm{j}(x,v) \qquad [\cup]\,\dfrac{\wedge\text{R}\,\dfrac{[;]\,\dfrac{\dfrac{}{\mathrm{j}(x,v)\to[?x=0][v:=-cv]\mathrm{j}(x,v)}}{\mathrm{j}(x,v)\to[?x=0;\,v:=-cv]\mathrm{j}(x,v)} \qquad \dfrac{}{\mathrm{j}(x,v)\to[?x\neq0]\mathrm{j}(x,v)}}{\mathrm{j}(x,v)\to[?x=0;\,v:=-cv]\mathrm{j}(x,v)\wedge[?x\neq0]\mathrm{j}(x,v)}}{\mathrm{j}(x,v)\to[?x=0;\,v:=-cv\cup ?x\neq0]\mathrm{j}(x,v)}}{\mathrm{j}(x,v)\to[\mathrm{grav}][?x=0;\,v:=-cv\cup ?x\neq0]\mathrm{j}(x,v)}}{\dfrac{\mathrm{j}(x,v)\to[\mathrm{grav};(?x=0;\,v:=-cv\cup ?x\neq0)]\mathrm{j}(x,v)}{\mathrm{j}(x,v)\to[\mathrm{grav};(?x=0;\,v:=-cv\cup ?x\neq0)]\mathrm{j}(x,v)}} \qquad \mathrm{j}(x,v)\to B(x,v)}{A\to\left[\left(\mathrm{grav};(?x=0;\,v:=-cv\cup ?x\neq0)\right)^*\right]B(x,v)}
$$

$$A \equiv 0\le x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \ge c \ge 0$$

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

$$\mathrm{grav} \equiv \{x' = v, v' = -g \,\&\, x \ge 0\}$$

$$
\text{loop}\;\dfrac{A\rightarrow \mathrm{j}(x,v) \qquad \dfrac{\text{[;]}\;\dfrac{\text{MR}\;\dfrac{\mathrm{j}(x,v)\rightarrow[\mathrm{grav}]\mathrm{j}(x,v) \qquad [\cup]\;\dfrac{\wedge\text{R}\;\dfrac{\text{[;]}\;\dfrac{[?],\rightarrow\text{R}\;\dfrac{\dfrac{}{\mathrm{j}(x,v),\, x=0\rightarrow[v:=-cv]\mathrm{j}(x,v)}}{\mathrm{j}(x,v)\rightarrow[?x=0][v:=-cv]\mathrm{j}(x,v)}}{\mathrm{j}(x,v)\rightarrow[?x=0;\, v:=-cv]\mathrm{j}(x,v)} \qquad \dfrac{}{\mathrm{j}(x,v)\rightarrow[?x\neq 0]\mathrm{j}(x,v)}}{\mathrm{j}(x,v)\rightarrow[?x=0;\, v:=-cv]\mathrm{j}(x,v)\wedge[?x\neq 0]\mathrm{j}(x,v)}}{\mathrm{j}(x,v)\rightarrow[?x=0;\, v:=-cv\cup ?x\neq 0]\mathrm{j}(x,v)}}{\mathrm{j}(x,v)\rightarrow[\mathrm{grav}][?x=0;\, v:=-cv\cup ?x\neq 0]\mathrm{j}(x,v)}}{\mathrm{j}(x,v)\rightarrow[\mathrm{grav};(?x=0;\, v:=-cv\cup ?x\neq 0)]\mathrm{j}(x,v)}}{\mathrm{j}(x,v)\rightarrow[\mathrm{grav};(?x=0;\, v:=-cv\cup ?x\neq 0)]\mathrm{j}(x,v)} \qquad \mathrm{j}(x,v)\rightarrow B(x,v)}{A\rightarrow\left[\left(\mathrm{grav};(?x=0;\, v:=-cv\cup ?x\neq 0)\right)^*\right]B(x,v)}
$$

$$A \equiv 0 \le x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \ge c \ge 0$$

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

$$\mathrm{grav} \equiv \{x' = v, v' = -g \,\&\, x \ge 0\}$$

$$\dfrac{A \to \text{j}(x,v) \qquad \dfrac{\dfrac{\text{j}(x,v) \to [\text{grav}]\text{j}(x,v) \quad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\text{j}(x,v), x{=}0 \to \text{j}(x,-cv)}{\text{j}(x,v), x{=}0 \to [v{:=}{-cv}]\text{j}(x,v)}[:=]}{\text{j}(x,v) \to [?x{=}0][v{:=}{-cv}]\text{j}(x,v)}[?],\to R}{\text{j}(x,v) \to [?x{=}0; v{:=}{-cv}]\text{j}(x,v)}[;] \qquad \text{j}(x,v) \to [?x{\neq}0]\text{j}(x,v)}{\text{j}(x,v) \to [?x{=}0; v{:=}{-cv}]\text{j}(x,v) \land [?x{\neq}0]\text{j}(x,v)}\land R}{\text{j}(x,v) \to [?x{=}0; v{:=}{-cv} \cup ?x{\neq}0]\text{j}(x,v)}[\cup]}{\text{j}(x,v) \to [\text{grav}][?x{=}0; v{:=}{-cv} \cup ?x{\neq}0]\text{j}(x,v)}\text{MR}}{\text{j}(x,v) \to [\text{grav}; (?x{=}0; v{:=}{-cv} \cup ?x{\neq}0)]\text{j}(x,v)}[;] \qquad \text{j}(x,v) \to B(x,v)}{A \to [\big(\text{grav}; (?x{=}0; v{:=}{-cv} \cup ?x{\neq}0)\big)^*]B(x,v)}\text{loop}$$

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

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

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

$$
\dfrac{
  A \rightarrow \mathrm{j}(x,v)
  \quad
  \dfrac{
    \dfrac{
      \mathrm{j}(x,v) \rightarrow [grav]\mathrm{j}(x,v)
      \quad
      \dfrac{
        \dfrac{
          \dfrac{
            \dfrac{
              \dfrac{\mathrm{j}(x,v), x{=}0 \rightarrow \mathrm{j}(x,-cv)}{\mathrm{j}(x,v), x{=}0 \rightarrow [v:=-cv]\mathrm{j}(x,v)}[:=]
            }{\mathrm{j}(x,v) \rightarrow [?x{=}0][v:=-cv]\mathrm{j}(x,v)}[?],\rightarrow R
          }{\mathrm{j}(x,v) \rightarrow [?x{=}0;v:=-cv]\mathrm{j}(x,v)}[;]
          \quad
          \dfrac{\mathrm{j}(x,v), x{\neq}0 \rightarrow \mathrm{j}(x,v)}{\mathrm{j}(x,v) \rightarrow [?x{\neq}0]\mathrm{j}(x,v)}[?]
        }{\mathrm{j}(x,v) \rightarrow [?x{=}0;v:=-cv]\mathrm{j}(x,v) \land [?x{\neq}0]\mathrm{j}(x,v)}\land R
      }{\mathrm{j}(x,v) \rightarrow [?x{=}0;v:=-cv \cup ?x{\neq}0]\mathrm{j}(x,v)}[\cup]
    }{\mathrm{j}(x,v) \rightarrow [grav][?x{=}0;v:=-cv \cup ?x{\neq}0]\mathrm{j}(x,v)}MR
  }{
    \dfrac{\mathrm{j}(x,v) \rightarrow [grav;(?x{=}0;v:=-cv \cup ?x{\neq}0)]\mathrm{j}(x,v)}{\mathrm{j}(x,v) \rightarrow [grav;(?x{=}0;v:=-cv \cup ?x{\neq}0)]\mathrm{j}(x,v)}
  }[;]
  \quad
  \mathrm{j}(x,v) \rightarrow B(x,v)
}{A \rightarrow [\big(grav;(?x{=}0;v:=-cv \cup ?x{\neq}0)\big)^*]B(x,v)}loop
$$

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

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

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

$$
\text{loop}\ \dfrac{A \to j(x,v) \qquad \dfrac{\text{MR}\ \dfrac{j(x,v)\to[\mathrm{grav}]j(x,v) \quad [\cup]\ \dfrac{\wedge R\ \dfrac{[;]\ \dfrac{[?],\to R\ \dfrac{[:=]\ \dfrac{j(x,v), x{=}0 \to j(x,-cv)}{j(x,v), x{=}0 \to [v:=-cv]j(x,v)}}{j(x,v)\to[?x{=}0][v:=-cv]j(x,v)}}{j(x,v)\to[?x{=}0;\, v:=-cv]j(x,v)} \quad [?]\ \dfrac{j(x,v), x{\neq}0 \to j(x,v)}{j(x,v)\to[?x{\neq}0]j(x,v)}}{j(x,v)\to[?x{=}0;\, v:=-cv]j(x,v) \wedge [?x{\neq}0]j(x,v)}}{j(x,v)\to[?x{=}0;\, v:=-cv \cup ?x{\neq}0]j(x,v)}}{[;]\ \dfrac{j(x,v)\to[\mathrm{grav}][?x{=}0;\, v:=-cv \cup ?x{\neq}0]j(x,v)}{j(x,v)\to[\mathrm{grav};(?x{=}0;\, v:=-cv \cup ?x{\neq}0)]j(x,v)}}}{j(x,v)\to[\mathrm{grav};(?x{=}0;\, v:=-cv \cup ?x{\neq}0)]j(x,v)} \qquad j(x,v)\to B(x,v)}{A \to [\big(\mathrm{grav};(?x{=}0;\, v:=-cv \cup ?x{\neq}0)\big)^*]B(x,v)}
$$

$$A \equiv 0 \le x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \ge c \ge 0$$

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

$$\mathrm{grav} \equiv \{x' = v, v' = -g \,\&\, x \ge 0\}$$

$A \to \mathrm{j}(x,v)$

$\mathrm{j}(x,v) \to [\mathrm{grav}](\mathrm{j}(x,v))$

$\mathrm{j}(x,v), x=0 \to \mathrm{j}(x,(-cv))$

$\mathrm{j}(x,v), x\neq 0 \to \mathrm{j}(x,v)$

$\mathrm{j}(x,v) \to B(x,v)$

$$A \equiv 0 \le x \land x = H \land v = 0 \land g > 0 \land 1 \ge c \ge 0$$

$$B(x,v) \equiv 0 \le x \land x \le H$$

$$\mathrm{grav} \equiv \{x' = v, v' = -g \,\&\, x \ge 0\}$$

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

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

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

$\mathrm{j}(x,v), x\neq 0 \rightarrow \mathrm{j}(x,v)$

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

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

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

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

$0 \le x \land x = H \land v = 0 \land g > 0 \land 1 \ge c \ge 0 \rightarrow j(x,v)$

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

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

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

$j(x,v) \rightarrow 0 \le x \land x \le H$

2. $j(x,v) \equiv 0 \le x \land x \le H$

$$A \equiv 0 \le x \land x = H \land v = 0 \land g > 0 \land 1 \ge c \ge 0$$

$$B(x,v) \equiv 0 \le x \land x \le H$$

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

$0 \le x \land x = H \land v = 0 \land g > 0 \land 1 \ge c \ge 0 \to j(x,v)$

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

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

$j(x,v), x \ne 0 \to j(x,v)$

$j(x,v) \to 0 \le x \land x \le H$

2. $j(x,v) \equiv 0 \le x \land x \le H$ weak: fails ODE if $v \gg 0$

$$A \equiv 0 \le x \land x = H \land v = 0 \land g > 0 \land 1 \ge c \ge 0$$

$$B(x,v) \equiv 0 \le x \land x \le H$$

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

Proving Quantum the Acrophobic Bouncing Ball

$0 \le x \land x = H \land v = 0 \land g > 0 \land 1 \ge c \ge 0 \rightarrow j(x,v)$

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

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

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

$j(x,v) \rightarrow 0 \le x \land x \le H$

1. $j(x,v) \equiv x \ge 0$
2. $j(x,v) \equiv 0 \le x \land x \le H$ — weak: fails ODE if $v \gg 0$

$$A \equiv 0 \le x \land x = H \land v = 0 \land g > 0 \land 1 \ge c \ge 0$$

$$B(x,v) \equiv 0 \le x \land x \le H$$

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

$$0 \le x \land x = H \land v = 0 \land g > 0 \land 1 \ge c \ge 0 \rightarrow j(x,v)$$
$$j(x,v) \rightarrow [\{x'=v, v'=-g \,\&\, x \ge 0\}](j(x,v))$$
$$j(x,v), x=0 \rightarrow j(x,(-cv))$$
$$j(x,v), x \ne 0 \rightarrow j(x,v)$$
$$j(x,v) \rightarrow 0 \le x \land x \le H$$

1. $j(x,v) \equiv x \ge 0$ — weaker: fails postcondition if $x > H$
2. $j(x,v) \equiv 0 \le x \land x \le H$ — weak: fails ODE if $v \gg 0$

$$A \equiv 0 \le x \land x = H \land v = 0 \land g > 0 \land 1 \ge c \ge 0$$
$$B(x,v) \equiv 0 \le x \land x \le H$$
$$\text{grav} \equiv \{x' = v, v' = -g \,\&\, x \ge 0\}$$

$$0 \le x \land x = H \land v = 0 \land g > 0 \land 1 \ge c \ge 0 \rightarrow j(x,v)$$
$$j(x,v) \rightarrow [\{x'=v, v'=-g \,\&\, x \ge 0\}](j(x,v))$$
$$j(x,v), x=0 \rightarrow j(x,(-cv))$$
$$j(x,v), x \ne 0 \rightarrow j(x,v)$$
$$j(x,v) \rightarrow 0 \le x \land x \le H$$

1. $j(x,v) \equiv x \ge 0$ — weaker: fails postcondition if $x > H$
2. $j(x,v) \equiv 0 \le x \land x \le H$ — weak: fails ODE if $v \gg 0$
3. $j(x,v) \equiv x = 0 \land v = 0$

$$A \equiv 0 \le x \land x = H \land v = 0 \land g > 0 \land 1 \ge c \ge 0$$
$$B(x,v) \equiv 0 \le x \land x \le H$$
$$\text{grav} \equiv \{x' = v, v' = -g \,\&\, x \ge 0\}$$

$$0 \leq x \land x = H \land v = 0 \land g > 0 \land 1 \geq c \geq 0 \rightarrow j(x,v)$$
$$j(x,v) \rightarrow [\{x'=v, v'=-g \,\&\, x \geq 0\}](j(x,v))$$
$$j(x,v), x=0 \rightarrow j(x,(-cv))$$
$$j(x,v), x \neq 0 \rightarrow j(x,v)$$
$$j(x,v) \rightarrow 0 \leq x \land x \leq H$$

1. $j(x,v) \equiv x \geq 0$ — weaker: fails postcondition if $x > H$
2. $j(x,v) \equiv 0 \leq x \land x \leq H$ — weak: fails ODE if $v \gg 0$
3. $j(x,v) \equiv x = 0 \land v = 0$ — strong: fails initial condition if $x > 0$

$$A \equiv 0 \leq x \land x = H \land v = 0 \land g > 0 \land 1 \geq c \geq 0$$
$$B(x,v) \equiv 0 \leq x \land x \leq H$$
$$\text{grav} \equiv \{x' = v, v' = -g \,\&\, x \geq 0\}$$

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

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

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

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

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

1. $j(x,v) \equiv x \ge 0$ — weaker: fails postcondition if $x > H$
2. $j(x,v) \equiv 0 \le x \wedge x \le H$ — weak: fails ODE if $v \gg 0$
3. $j(x,v) \equiv x = 0 \wedge v = 0$ — strong: fails initial condition if $x > 0$
4. $j(x,v) \equiv x = 0 \vee x = H \wedge v = 0$

$$A \equiv 0 \le x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \ge c \ge 0$$

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

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

$0 \le x \land x = H \land v = 0 \land g > 0 \land 1 \ge c \ge 0 \rightarrow \mathrm{j}(x,v)$

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

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

$\mathrm{j}(x,v), x \ne 0 \rightarrow \mathrm{j}(x,v)$

$\mathrm{j}(x,v) \rightarrow 0 \le x \land x \le H$

1. $\mathrm{j}(x,v) \equiv x \ge 0$ — weaker: fails postcondition if $x > H$
2. $\mathrm{j}(x,v) \equiv 0 \le x \land x \le H$ — weak: fails ODE if $v \gg 0$
3. $\mathrm{j}(x,v) \equiv x = 0 \land v = 0$ — strong: fails initial condition if $x > 0$
4. $\mathrm{j}(x,v) \equiv x = 0 \lor x = H \land v = 0$ — no space for intermediate states

$$A \equiv 0 \le x \land x = H \land v = 0 \land g > 0 \land 1 \ge c \ge 0$$

$$B(x,v) \equiv 0 \le x \land x \le H$$

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

$$0 \le x \land x = H \land v = 0 \land g > 0 \land 1 \ge c \ge 0 \rightarrow j(x,v)$$
$$j(x,v) \rightarrow [\{x'=v, v'=-g \,\&\, x\ge 0\}](j(x,v))$$
$$j(x,v), x=0 \rightarrow j(x,(-cv))$$
$$j(x,v), x\ne 0 \rightarrow j(x,v)$$
$$j(x,v) \rightarrow 0 \le x \land x \le H$$

1. $j(x,v) \equiv x \ge 0$ — weaker: fails postcondition if $x > H$
2. $j(x,v) \equiv 0 \le x \land x \le H$ — weak: fails ODE if $v \gg 0$
3. $j(x,v) \equiv x = 0 \land v = 0$ — strong: fails initial condition if $x > 0$
4. $j(x,v) \equiv x = 0 \lor x = H \land v = 0$ — no space for intermediate states
5. $j(x,v) \equiv 2gx = 2gH - v^2 \land x \ge 0$

$$A \equiv 0 \le x \land x = H \land v = 0 \land g > 0 \land 1 \ge c \ge 0$$
$$B(x,v) \equiv 0 \le x \land x \le H$$
$$\text{grav} \equiv \{x' = v, v' = -g \,\&\, x \ge 0\}$$

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

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

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

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

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

1. $j(x,v) \equiv x \geq 0$ — weaker: fails postcondition if $x > H$
2. $j(x,v) \equiv 0 \leq x \wedge x \leq H$ — weak: fails ODE if $v \gg 0$
3. $j(x,v) \equiv x = 0 \wedge v = 0$ — strong: fails initial condition if $x > 0$
4. $j(x,v) \equiv x = 0 \vee x = H \wedge v = 0$ — no space for intermediate states
5. $j(x,v) \equiv 2gx = 2gH - v^2 \wedge x \geq 0$ — works: implicitly links v and x

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

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

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

$$0 \le x \land x = H \land v = 0 \land g > 0 \land 1 \ge c \ge 0 \rightarrow 2gx = 2gH - v^2 \land x \ge 0$$
$$2gx = 2gH - v^2 \land x \ge 0 \rightarrow [\{x' = v, v' = -g \,\&\, x \ge 0\}](2gx = 2gH - v^2 \land x \ge 0)$$
$$2gx = 2gH - v^2 \land x \ge 0, x = 0 \rightarrow 2gx = 2gH - (-cv)^2 \land x \ge 0$$
$$2gx = 2gH - v^2 \land x \ge 0, x \ne 0 \rightarrow 2gx = 2gH - v^2 \land x \ge 0$$
$$2gx = 2gH - v^2 \land x \ge 0 \rightarrow 0 \le x \land x \le H$$

1.
2.
3.
4.
5. $\mathrm{j}(x,v) \equiv 2gx = 2gH - v^2 \land x \ge 0$ works: implicitly links v and x

$$0 \le x \land x = H \land v = 0 \land g > 0 \land 1 \ge c \ge 0 \rightarrow 2gx{=}2gH{-}v^2 \land x{\ge}0$$

$$2gx{=}2gH{-}v^2 \land x{\ge}0 \rightarrow [\{x'{=}v, v'{=}{-}g \,\&\, x{\ge}0\}](2gx{=}2gH{-}v^2 \land x{\ge}0)$$

$$2gx{=}2gH{-}v^2 \land x{\ge}0, x{=}0 \rightarrow 2gx{=}2gH{-}(-cv)^2 \land x{\ge}0$$

$$2gx{=}2gH{-}v^2 \land x{\ge}0, x{\ne}0 \rightarrow 2gx{=}2gH{-}v^2 \land x{\ge}0$$

$$2gx{=}2gH{-}v^2 \land x{\ge}0 \rightarrow 0 \le x \land x \le H$$

1.
2.
3.
4.
5. $j(x,v) \equiv 2gx{=}2gH{-}v^2 \land x{\ge}0$ works: implicitly links v and x

$0 \le x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \ge c \ge 0 \rightarrow 2gx{=}2gH{-}v^2 \wedge x{\ge}0$

$2gx{=}2gH{-}v^2 \wedge x{\ge}0 \rightarrow [\{x'{=}v, v'{=}{-}g \,\&\, x{\ge}0\}](2gx{=}2gH{-}v^2 \wedge x{\ge}0)$

✓ $2gx{=}2gH{-}v^2 \wedge x{\ge}0, x{=}0 \rightarrow 2gx{=}2gH{-}({-}cv)^2 \wedge x{\ge}0$ if $c = 1 \ldots$

$2gx{=}2gH{-}v^2 \wedge x{\ge}0, x{\ne}0 \rightarrow 2gx{=}2gH{-}v^2 \wedge x{\ge}0$

$2gx{=}2gH{-}v^2 \wedge x{\ge}0 \rightarrow 0 \le x \wedge x \le H$

1.
2.
3.
4.
5. $\mathrm{j}(x,v) \equiv 2gx{=}2gH{-}v^2 \wedge x{\ge}0$ works: implicitly links v and x

$0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0 \rightarrow 2gx{=}2gH{-}v^2 \wedge x{\geq}0$

$2gx{=}2gH{-}v^2 \wedge x{\geq}0 \rightarrow [\{x'{=}v, v'{=}{-}g \,\&\, x{\geq}0\}](2gx{=}2gH{-}v^2 \wedge x{\geq}0)$

✓ $2gx{=}2gH{-}v^2 \wedge x{\geq}0, x{=}0 \rightarrow 2gx{=}2gH{-}(-cv)^2 \wedge x{\geq}0$ if $c = 1 \ldots$

$2gx{=}2gH{-}v^2 \wedge x{\geq}0, x{\neq}0 \rightarrow 2gx{=}2gH{-}v^2 \wedge x{\geq}0$

$2gx{=}2gH{-}v^2 \wedge x{\geq}0 \rightarrow 0 \leq x \wedge x \leq H$

1.
2.
3.
4.
5. $\mathrm{j}(x,v) \equiv 2gx{=}2gH{-}v^2 \wedge x{\geq}0$ works: implicitly links v and x

$0 \le x \land x = H \land v = 0 \land g > 0 \land 1 \ge c \ge 0 \to 2gx = 2gH - v^2 \land x \ge 0$

$2gx = 2gH - v^2 \land x \ge 0 \to [\{x' = v, v' = -g \,\&\, x \ge 0\}](2gx = 2gH - v^2 \land x \ge 0)$

✓ $2gx = 2gH - v^2 \land x \ge 0, x = 0 \to 2gx = 2gH - (-cv)^2 \land x \ge 0$ if $c = 1 \ldots$

✓ $2gx = 2gH - v^2 \land x \ge 0, x \ne 0 \to 2gx = 2gH - v^2 \land x \ge 0$

$2gx = 2gH - v^2 \land x \ge 0 \to 0 \le x \land x \le H$

1.
2.
3.
4.
5. $j(x,v) \equiv 2gx = 2gH - v^2 \land x \ge 0$ works: implicitly links v and x

$0 \leq x \land x = H \land v = 0 \land g > 0 \land 1 \geq c \geq 0 \rightarrow 2gx{=}2gH{-}v^2 \land x{\geq}0$

$2gx{=}2gH{-}v^2 \land x{\geq}0 \rightarrow [\{x'{=}v, v'{=}{-}g \,\&\, x{\geq}0\}](2gx{=}2gH{-}v^2 \land x{\geq}0)$

✓ $2gx{=}2gH{-}v^2 \land x{\geq}0, x{=}0 \rightarrow 2gx{=}2gH{-}({-}cv)^2 \land x{\geq}0$ if $c = 1 \ldots$

✓ $2gx{=}2gH{-}v^2 \land x{\geq}0, x{\neq}0 \rightarrow 2gx{=}2gH{-}v^2 \land x{\geq}0$

$2gx{=}2gH{-}v^2 \land x{\geq}0 \rightarrow 0 \leq x \land x \leq H$

1.
2.
3.
4.
5. $\mathrm{j}(x,v) \equiv 2gx{=}2gH{-}v^2 \land x{\geq}0$ works: implicitly links v and x

$0 \le x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \ge c \ge 0 \rightarrow 2gx = 2gH - v^2 \wedge x \ge 0$

$2gx = 2gH - v^2 \wedge x \ge 0 \rightarrow [\{x' = v, v' = -g \,\&\, x \ge 0\}](2gx = 2gH - v^2 \wedge x \ge 0)$

✓ $2gx = 2gH - v^2 \wedge x \ge 0, x = 0 \rightarrow 2gx = 2gH - (-cv)^2 \wedge x \ge 0$ if $c = 1 \ldots$

✓ $2gx = 2gH - v^2 \wedge x \ge 0, x \ne 0 \rightarrow 2gx = 2gH - v^2 \wedge x \ge 0$

✓ $2gx = 2gH - v^2 \wedge x \ge 0 \rightarrow 0 \le x \wedge x \le H$ because $g > 0$

1.
2.
3.
4.
5. $\mathrm{j}(x,v) \equiv 2gx = 2gH - v^2 \wedge x \ge 0$ works: implicitly links v and x

$0 \le x \land x = H \land v = 0 \land g > 0 \land 1 \ge c \ge 0 \to 2gx = 2gH - v^2 \land x \ge 0$

$2gx = 2gH - v^2 \land x \ge 0 \to [\{x' = v, v' = -g \,\&\, x \ge 0\}](2gx = 2gH - v^2 \land x \ge 0)$

✓ $2gx = 2gH - v^2 \land x \ge 0, x = 0 \to 2gx = 2gH - (-cv)^2 \land x \ge 0$ if $c = 1 \ldots$

✓ $2gx = 2gH - v^2 \land x \ge 0, x \ne 0 \to 2gx = 2gH - v^2 \land x \ge 0$

✓ $2gx = 2gH - v^2 \land x \ge 0 \to 0 \le x \land x \le H$ because $g > 0$

1.
2.
3.
4.
5. $\mathrm{j}(x,v) \equiv 2gx = 2gH - v^2 \land x \ge 0$ works: implicitly links v and x

✓ $0 \leq x \land x = H \land v = 0 \land g > 0 \land 1 \geq c \geq 0 \rightarrow 2gx{=}2gH{-}v^2 \land x{\geq}0$

$2gx{=}2gH{-}v^2 \land x{\geq}0 \rightarrow [\{x'{=}v, v'{=}{-}g \,\&\, x{\geq}0\}](2gx{=}2gH{-}v^2 \land x{\geq}0)$

✓ $2gx{=}2gH{-}v^2 \land x{\geq}0, x{=}0 \rightarrow 2gx{=}2gH{-}(-cv)^2 \land x{\geq}0$ if $c = 1 \ldots$

✓ $2gx{=}2gH{-}v^2 \land x{\geq}0, x{\neq}0 \rightarrow 2gx{=}2gH{-}v^2 \land x{\geq}0$

✓ $2gx{=}2gH{-}v^2 \land x{\geq}0 \rightarrow 0 \leq x \land x \leq H$ because $g > 0$

1.
2.
3.
4.
5. $\mathrm{j}(x,v) \equiv 2gx{=}2gH{-}v^2 \land x{\geq}0$ works: implicitly links v and x

$x(t) = H - \frac{g}{2}t^2$ $v(t) = -gt$

✓ $0 \le x \land x = H \land v = 0 \land g > 0 \land 1 \ge c \ge 0 \to 2gx{=}2gH{-}v^2 \land x{\ge}0$

$2gx{=}2gH{-}v^2 \land x{\ge}0 \to [\{x'{=}v, v'{=}{-}g \,\&\, x{\ge}0\}](2gx{=}2gH{-}v^2 \land x{\ge}0)$

✓ $2gx{=}2gH{-}v^2 \land x{\ge}0, x{=}0 \to 2gx{=}2gH{-}({-}cv)^2 \land x{\ge}0$ if $c = 1 \ldots$

✓ $2gx{=}2gH{-}v^2 \land x{\ge}0, x{\ne}0 \to 2gx{=}2gH{-}v^2 \land x{\ge}0$

✓ $2gx{=}2gH{-}v^2 \land x{\ge}0 \to 0 \le x \land x \le H$ because $g > 0$

1.
2.
3.
4.
5. $\mathrm{j}(x,v) \equiv 2gx{=}2gH{-}v^2 \land x{\ge}0$ works: implicitly links v and x

$$x(t) = H - \frac{g}{2}t^2 \rightsquigarrow 2gx(t) = 2gH - g^2t^2 \qquad v(t)^2 = g^2t^2 \leftsquigarrow v(t) = -gt$$

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

$$\dfrac{\dfrac{}{\text{j}(x,v) \rightarrow \forall t{\geq}0\, [x:=H-\frac{g}{2}t^2; v:=-gt](x{\geq}0 \rightarrow \text{j}(x,v))}\;[;]}{\text{j}(x,v) \rightarrow [x'=v, v'=-g \,\&\, x{\geq}0]\text{j}(x,v)}\;[']$$

$$\dfrac{\dfrac{[:=]\quad \mathrm{j}(x,v) \rightarrow \forall t{\ge}0\,[x:=H-\frac{g}{2}t^2][v:=-gt](x{\ge}0 \rightarrow \mathrm{j}(x,v))}{[;]\quad \mathrm{j}(x,v) \rightarrow \forall t{\ge}0\,[x:=H-\frac{g}{2}t^2;\, v:=-gt](x{\ge}0 \rightarrow \mathrm{j}(x,v))}}{[']\quad \mathrm{j}(x,v) \rightarrow [x'=v, v'=-g\,\&\,x{\ge}0]\mathrm{j}(x,v)}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\mathrm{j}(x,v) \rightarrow \forall t{\geq}0\,[x{:=}H-\frac{g}{2}t^2](x{\geq}0 \rightarrow \mathrm{j}(x,-gt))}[{:=}]}{\mathrm{j}(x,v) \rightarrow \forall t{\geq}0\,[x{:=}H-\frac{g}{2}t^2][v{:=}-gt](x{\geq}0 \rightarrow \mathrm{j}(x,v))}[{:=}]}{\mathrm{j}(x,v) \rightarrow \forall t{\geq}0\,[x{:=}H-\frac{g}{2}t^2;\, v{:=}-gt](x{\geq}0 \rightarrow \mathrm{j}(x,v))}[;]}{\mathrm{j}(x,v) \rightarrow [x'{=}v, v'{=}-g\,\&\,x{\geq}0]\mathrm{j}(x,v)}[']$$

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\text{j}(x,v) \rightarrow \forall t{\geq}0\,\big(H-\frac{g}{2}t^2{\geq}0 \rightarrow \text{j}(H-\frac{g}{2}t^2,-gt)\big)}\;\forall\text{R}}{\text{j}(x,v) \rightarrow \forall t{\geq}0\,[x{:=}H-\frac{g}{2}t^2]\big(x{\geq}0 \rightarrow \text{j}(x,-gt)\big)}\;[:=]}{\text{j}(x,v) \rightarrow \forall t{\geq}0\,[x{:=}H-\frac{g}{2}t^2][v{:=}-gt]\big(x{\geq}0 \rightarrow \text{j}(x,v)\big)}\;[:=]}{\text{j}(x,v) \rightarrow \forall t{\geq}0\,[x{:=}H-\frac{g}{2}t^2;\, v{:=}-gt]\big(x{\geq}0 \rightarrow \text{j}(x,v)\big)}\;[;]}{\text{j}(x,v) \rightarrow [x'{=}v, v'{=}-g\,\&\,x{\geq}0]\text{j}(x,v)}\;[']
$$

$$
\dfrac{
\dfrac{
\dfrac{
\dfrac{
\dfrac{
\dfrac{}{j(x,v) \rightarrow t\geq 0 \rightarrow H-\frac{g}{2}t^2\geq 0 \rightarrow j(H-\frac{g}{2}t^2, -gt)}\rightarrow\text{R}
}{j(x,v) \rightarrow \forall t\geq 0\, (H-\frac{g}{2}t^2\geq 0 \rightarrow j(H-\frac{g}{2}t^2, -gt))}\forall\text{R}
}{j(x,v) \rightarrow \forall t\geq 0\, [x:=H-\frac{g}{2}t^2](x\geq 0 \rightarrow j(x, -gt))}[:=]
}{j(x,v) \rightarrow \forall t\geq 0\, [x:=H-\frac{g}{2}t^2][v:=-gt](x\geq 0 \rightarrow j(x,v))}[:=]
}{j(x,v) \rightarrow \forall t\geq 0\, [x:=H-\frac{g}{2}t^2; v:=-gt](x\geq 0 \rightarrow j(x,v))}[;]
}{j(x,v) \rightarrow [x'=v, v'=-g \,\&\, x\geq 0]j(x,v)}['']
$$

Proving Quantum the Acrophobic Bouncing Ball

$$\mathrm{j}(x,v),\, t\geq 0,\, H-\frac{g}{2}t^2\geq 0 \rightarrow \mathrm{j}(H-\tfrac{g}{2}t^2, -gt)$$

$\rightarrow$R

$$\mathrm{j}(x,v) \rightarrow t\geq 0 \rightarrow H-\frac{g}{2}t^2\geq 0 \rightarrow \mathrm{j}(H-\tfrac{g}{2}t^2, -gt)$$

$\forall$R

$$\mathrm{j}(x,v) \rightarrow \forall t\geq 0\, \Big(H-\frac{g}{2}t^2\geq 0 \rightarrow \mathrm{j}(H-\tfrac{g}{2}t^2, -gt)\Big)$$

$[:=]$

$$\mathrm{j}(x,v) \rightarrow \forall t\geq 0\, [x:=H-\frac{g}{2}t^2]\big(x\geq 0 \rightarrow \mathrm{j}(x, -gt)\big)$$

$[:=]$

$$\mathrm{j}(x,v) \rightarrow \forall t\geq 0\, [x:=H-\frac{g}{2}t^2][v:=-gt]\big(x\geq 0 \rightarrow \mathrm{j}(x,v)\big)$$

$[;]$

$$\mathrm{j}(x,v) \rightarrow \forall t\geq 0\, [x:=H-\frac{g}{2}t^2;\, v:=-gt]\big(x\geq 0 \rightarrow \mathrm{j}(x,v)\big)$$

$[']$

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

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

$$2gx=2gH-v^2\land x\geq 0, H-\frac{g}{2}t^2\geq 0 \rightarrow 2g(H-\frac{g}{2}t^2)=2gH-(gt)^2\land(H-\frac{g}{2}t^2)\geq 0$$

$$j(x,v), t\geq 0, H-\frac{g}{2}t^2\geq 0 \rightarrow j(H-\frac{g}{2}t^2, -gt)$$

$\rightarrow$R
$$j(x,v) \rightarrow t\geq 0 \rightarrow H-\frac{g}{2}t^2\geq 0 \rightarrow j(H-\frac{g}{2}t^2, -gt)$$

$\forall$R
$$j(x,v) \rightarrow \forall t\geq 0\,(H-\frac{g}{2}t^2\geq 0 \rightarrow j(H-\frac{g}{2}t^2, -gt))$$

$[:=]$
$$j(x,v) \rightarrow \forall t\geq 0\,[x:=H-\frac{g}{2}t^2](x\geq 0 \rightarrow j(x,-gt))$$

$[:=]$
$$j(x,v) \rightarrow \forall t\geq 0\,[x:=H-\frac{g}{2}t^2][v:=-gt](x\geq 0 \rightarrow j(x,v))$$

$[;]$
$$j(x,v) \rightarrow \forall t\geq 0\,[x:=H-\frac{g}{2}t^2; v:=-gt](x\geq 0 \rightarrow j(x,v))$$

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

$$\wedge R \; \dfrac{2gx{=}2gH{-}v^2 \to 2g(H{-}\frac{g}{2}t^2){=}2gH{-}(gt)^2 \qquad H{-}\frac{g}{2}t^2{\geq}0 \to H{-}\frac{g}{2}t^2{\geq}0}{2gx{=}2gH{-}v^2 \wedge x{\geq}0,\, H{-}\frac{g}{2}t^2{\geq}0 \to 2g(H{-}\frac{g}{2}t^2){=}2gH{-}(gt)^2 \wedge (H{-}\frac{g}{2}t^2){\geq}0}$$

$$\mathrm{j}(x,v),\, t{\geq}0,\, H{-}\tfrac{g}{2}t^2{\geq}0 \to \mathrm{j}(H{-}\tfrac{g}{2}t^2, -gt)$$

$$\to R \quad \mathrm{j}(x,v) \to t{\geq}0 \to H{-}\tfrac{g}{2}t^2{\geq}0 \to \mathrm{j}(H{-}\tfrac{g}{2}t^2, -gt)$$

$$\forall R \quad \mathrm{j}(x,v) \to \forall t{\geq}0\, (H{-}\tfrac{g}{2}t^2{\geq}0 \to \mathrm{j}(H{-}\tfrac{g}{2}t^2, -gt))$$

$$[:=] \quad \mathrm{j}(x,v) \to \forall t{\geq}0\, [x{:=}H{-}\tfrac{g}{2}t^2](x{\geq}0 \to \mathrm{j}(x, -gt))$$

$$[:=] \quad \mathrm{j}(x,v) \to \forall t{\geq}0\, [x{:=}H{-}\tfrac{g}{2}t^2][v{:=}{-}gt](x{\geq}0 \to \mathrm{j}(x,v))$$

$$[;] \quad \mathrm{j}(x,v) \to \forall t{\geq}0\, [x{:=}H{-}\tfrac{g}{2}t^2;\, v{:=}{-}gt](x{\geq}0 \to \mathrm{j}(x,v))$$

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

$$*$$

$$\mathbb{R}\ \frac{}{2gx=2gH-v^2 \rightarrow 2g(H-\frac{g}{2}t^2)=2gH-(gt)^2} \qquad \frac{}{H-\frac{g}{2}t^2\geq 0 \rightarrow H-\frac{g}{2}t^2\geq 0}$$

$$\wedge R\ \ 2gx=2gH-v^2 \wedge x\geq 0, H-\frac{g}{2}t^2\geq 0 \rightarrow 2g(H-\frac{g}{2}t^2)=2gH-(gt)^2 \wedge (H-\frac{g}{2}t^2)\geq 0$$

$$j(x,v), t\geq 0, H-\frac{g}{2}t^2\geq 0 \rightarrow j(H-\frac{g}{2}t^2, -gt)$$

$$\rightarrow R\ \ j(x,v) \rightarrow t\geq 0 \rightarrow H-\frac{g}{2}t^2\geq 0 \rightarrow j(H-\frac{g}{2}t^2, -gt)$$

$$\forall R\ \ j(x,v) \rightarrow \forall t\geq 0\, (H-\frac{g}{2}t^2\geq 0 \rightarrow j(H-\frac{g}{2}t^2, -gt))$$

$$[:=]\ \ j(x,v) \rightarrow \forall t\geq 0\, [x:=H-\frac{g}{2}t^2](x\geq 0 \rightarrow j(x,-gt))$$

$$[:=]\ \ j(x,v) \rightarrow \forall t\geq 0\, [x:=H-\frac{g}{2}t^2][v:=-gt](x\geq 0 \rightarrow j(x,v))$$

$$[;]\ \ j(x,v) \rightarrow \forall t\geq 0\, [x:=H-\frac{g}{2}t^2; v:=-gt](x\geq 0 \rightarrow j(x,v))$$

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

Proving Quantum the Acrophobic Bouncing Ball

$$
\dfrac{\dfrac{\dfrac{*}{2gx=2gH-v^2\rightarrow 2g(H-\frac{g}{2}t^2)=2gH-(gt)^2}\,\mathbb{R} \qquad \dfrac{*}{H-\frac{g}{2}t^2\geq 0\rightarrow H-\frac{g}{2}t^2\geq 0}\,\text{id}}{2gx=2gH-v^2\wedge x\geq 0, H-\frac{g}{2}t^2\geq 0\rightarrow 2g(H-\frac{g}{2}t^2)=2gH-(gt)^2\wedge(H-\frac{g}{2}t^2)\geq 0}\,\wedge\text{R}}{}
$$

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\text{j}(x,v), t\geq 0, H-\frac{g}{2}t^2\geq 0 \rightarrow \text{j}(H-\frac{g}{2}t^2,-gt)}{\text{j}(x,v) \rightarrow t\geq 0 \rightarrow H-\frac{g}{2}t^2\geq 0 \rightarrow \text{j}(H-\frac{g}{2}t^2,-gt)}\,\rightarrow\text{R}}{\text{j}(x,v) \rightarrow \forall t\geq 0\,(H-\frac{g}{2}t^2\geq 0 \rightarrow \text{j}(H-\frac{g}{2}t^2,-gt))}\,\forall\text{R}}{\text{j}(x,v) \rightarrow \forall t\geq 0\,[x:=H-\frac{g}{2}t^2](x\geq 0 \rightarrow \text{j}(x,-gt))}\,[:=]}{\text{j}(x,v) \rightarrow \forall t\geq 0\,[x:=H-\frac{g}{2}t^2][v:=-gt](x\geq 0 \rightarrow \text{j}(x,v))}\,[:=]}{\text{j}(x,v) \rightarrow \forall t\geq 0\,[x:=H-\frac{g}{2}t^2; v:=-gt](x\geq 0 \rightarrow \text{j}(x,v))}\,[;]}{\text{j}(x,v) \rightarrow [x'=v, v'=-g\,\&\,x\geq 0]\text{j}(x,v)}\,[']}{}
$$

$$\dfrac{\dfrac{\dfrac{*}{2gx=2gH-v^2\to 2g(H-\frac{g}{2}t^2)=2gH-(gt)^2}\,\mathbb{R}\qquad \dfrac{*}{H-\frac{g}{2}t^2\geq 0\to H-\frac{g}{2}t^2\geq 0}\,\text{id}}{2gx=2gH-v^2\wedge x\geq 0, H-\frac{g}{2}t^2\geq 0\to 2g(H-\frac{g}{2}t^2)=2gH-(gt)^2\wedge(H-\frac{g}{2}t^2)\geq 0}\,\wedge\text{R}}{}$$

$$\dfrac{j(x,v), t\geq 0, H-\frac{g}{2}t^2\geq 0 \to j(H-\frac{g}{2}t^2,-gt)}{j(x,v)\to t\geq 0\to H-\frac{g}{2}t^2\geq 0\to j(H-\frac{g}{2}t^2,-gt)}\,\to\text{R}$$

$$\dfrac{j(x,v)\to t\geq 0\to H-\frac{g}{2}t^2\geq 0\to j(H-\frac{g}{2}t^2,-gt)}{j(x,v)\to\forall t\geq 0\,(H-\frac{g}{2}t^2\geq 0\to j(H-\frac{g}{2}t^2,-gt))}\,\forall\text{R}$$

$$\dfrac{j(x,v)\to\forall t\geq 0\,(H-\frac{g}{2}t^2\geq 0\to j(H-\frac{g}{2}t^2,-gt))}{j(x,v)\to\forall t\geq 0\,[x:=H-\frac{g}{2}t^2](x\geq 0\to j(x,-gt))}\,[:=]$$

$$\dfrac{j(x,v)\to\forall t\geq 0\,[x:=H-\frac{g}{2}t^2](x\geq 0\to j(x,-gt))}{j(x,v)\to\forall t\geq 0\,[x:=H-\frac{g}{2}t^2][v:=-gt](x\geq 0\to j(x,v))}\,[:=]$$

$$\dfrac{j(x,v)\to\forall t\geq 0\,[x:=H-\frac{g}{2}t^2][v:=-gt](x\geq 0\to j(x,v))}{j(x,v)\to\forall t\geq 0\,[x:=H-\frac{g}{2}t^2; v:=-gt](x\geq 0\to j(x,v))}\,[;]$$

$$\dfrac{j(x,v)\to\forall t\geq 0\,[x:=H-\frac{g}{2}t^2; v:=-gt](x\geq 0\to j(x,v))}{j(x,v)\to[x'=v, v'=-g\,\&\,x\geq 0]j(x,v)}\,[']$$

- Oh no! These solutions assume $x = H, v = 0$ which $j(x,v)$ can't guarantee!

Proving Quantum the Acrophobic Bouncing Ball

$$\dfrac{\dfrac{*}{2gx{=}2gH{-}v^2 \to 2g(H{-}\frac{g}{2}t^2){=}2gH{-}(gt)^2}\,\mathbb{R} \qquad \dfrac{*}{H{-}\frac{g}{2}t^2{\geq}0 \to H{-}\frac{g}{2}t^2{\geq}0}\,\text{id}}{2gx{=}2gH{-}v^2 \land x{\geq}0,\, H{-}\frac{g}{2}t^2{\geq}0 \to 2g(H{-}\frac{g}{2}t^2){=}2gH{-}(gt)^2 \land (H{-}\frac{g}{2}t^2){\geq}0}\,\land\text{R}$$

$$\mathrm{j}(x{,}v),\, t{\geq}0,\, H{-}\tfrac{g}{2}t^2{\geq}0 \to \mathrm{j}(H{-}\tfrac{g}{2}t^2, -gt)$$

$$\mathrm{j}(x{,}v) \to t{\geq}0 \to H{-}\tfrac{g}{2}t^2{\geq}0 \to \mathrm{j}(H{-}\tfrac{g}{2}t^2, -gt) \tag{$\to$R}$$

$$\mathrm{j}(x{,}v) \to \forall t{\geq}0\, (H{-}\tfrac{g}{2}t^2{\geq}0 \to \mathrm{j}(H{-}\tfrac{g}{2}t^2, -gt)) \tag{$\forall$R}$$

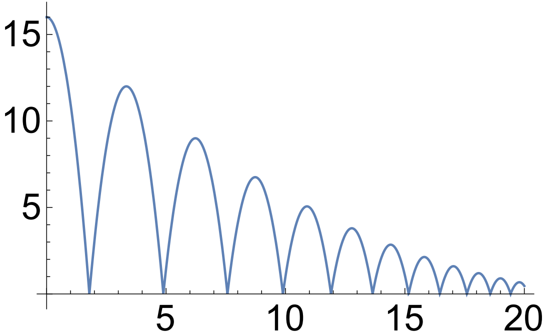
$$\mathrm{j}(x{,}v) \to \forall t{\geq}0\, [x{:=}H{-}\tfrac{g}{2}t^2](x{\geq}0 \to \mathrm{j}(x, -gt)) \tag{[:=]}$$

$$\mathrm{j}(x{,}v) \to \forall t{\geq}0\, [x{:=}H{-}\tfrac{g}{2}t^2][v{:=}{-}gt](x{\geq}0 \to \mathrm{j}(x{,}v)) \tag{[:=]}$$

$$\mathrm{j}(x{,}v) \to \forall t{\geq}0\, [x{:=}H{-}\tfrac{g}{2}t^2;\, v{:=}{-}gt](x{\geq}0 \to \mathrm{j}(x{,}v)) \tag{[;]}$$

$$\mathrm{j}(x{,}v) \to [x'{=}v, v'{=}{-}g\, \&\, x{\geq}0]\mathrm{j}(x{,}v) \tag{[′]}$$

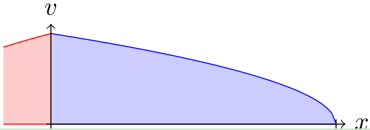
- Oh no! These solutions assume $x = H, v = 0$ which $\mathrm{j}(x{,}v)$ can't guarantee!
- Never use solutions without proof! ▸ Todo redo proof with true solution



Example (Bouncing Ball)

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

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

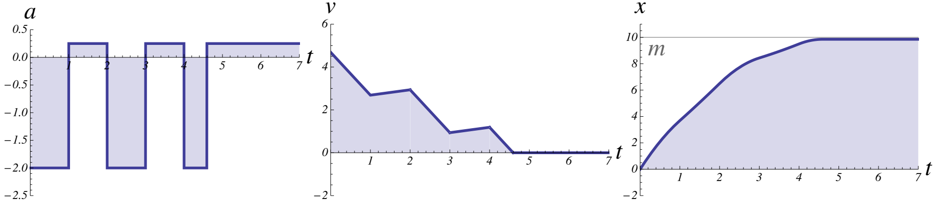


Example (Single car car_ε time-triggered)

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

Example (▶ Safely stays before traffic light m)

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

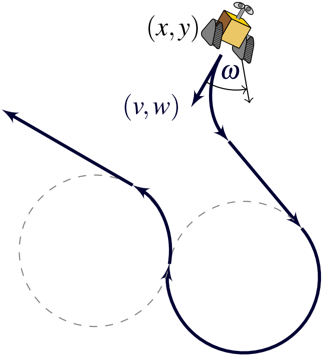


The lion's share of understanding comes from understanding what does change (variants/progress measures) and what doesn't change (invariants).

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)

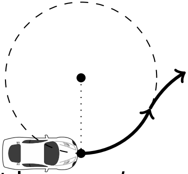
$$(x,y) \neq o \rightarrow \Big[\Big(\big(?Q_{-1};\, \omega{:=}{-1} \cup ?Q_1;\, \omega{:=}1 \cup ?Q_0;\, \omega{:=}0\big);$$
$$\{x' = v, y' = w, v' = \omega w, w' = -\omega v\}\Big)^*\Big]\,(x,y) \neq o$$

KeYmaera X aXiomatic Tactical Theorem Prover for CPS

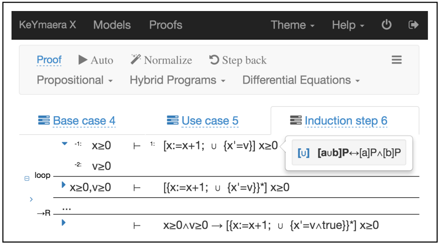
Proof search →

KeYmaera X

Model

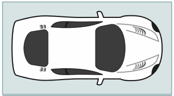


ctrl: $a := -b$;
plant: $x'' = a$



generates proofs

ModelPlex proof →



Model Safety

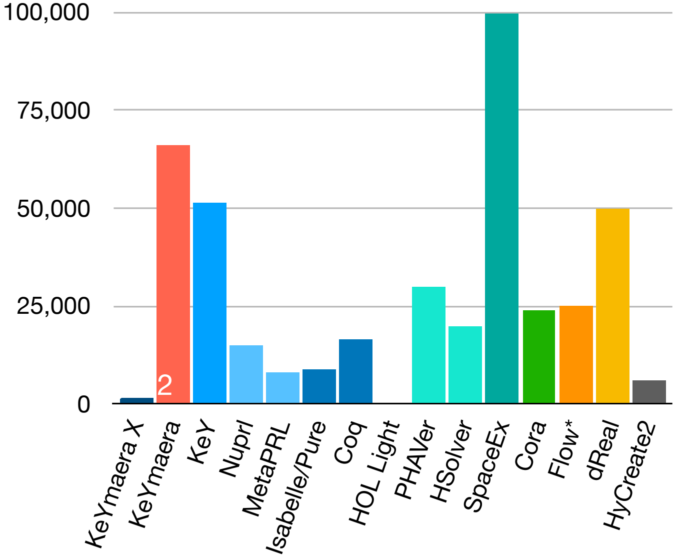
Compliance Monitor

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

Flexible
- Proof automation
- Interactive UI
- Programmable

Customizable
- Scala+Java API
- Command line
- REST API

KeYmaera X Small Kernel for Soundness 1 700 LOC



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

Uniform Substitution

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

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

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

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

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

Uniform Substitution

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 $U = \mathrm{BV}(\otimes(\cdot))$ of **no** operator $\otimes$
are free in the substitution on its argument θ (U-admissible)

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

Uniform Substitution

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

Modular interface: Prover vs. Logic

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

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

i.e. bound variables $U = \text{BV}(\otimes(\cdot))$ 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!

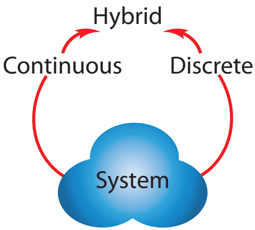
$$\frac{[v := f]p(v) \leftrightarrow p(f)}{[v := -x][x' = v]\,x \geq 0 \leftrightarrow [x' = -x]\,x \geq 0}$$

Clash

Complete Proof Theory of Hybrid Systems

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

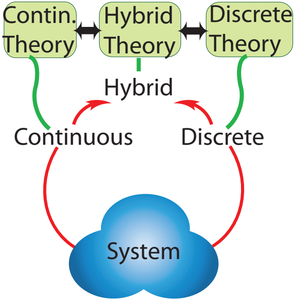
dL *calculus is a sound & complete axiomatization of hybrid systems relative to either differential equations* ***or*** *to discrete dynamics.*



Complete Proof Theory of Hybrid Systems

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

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



Summary: Proving CPS

equations of truth

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

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

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

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

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

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

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

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

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

LICS'12,JAR'17

Outline (Proving ODEs)

Summary: Proving CPS

equations of truth

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

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

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

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

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

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

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

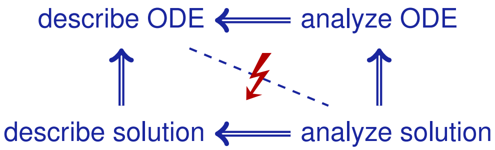
I $[\alpha^*]P \leftrightarrow P \land [\alpha^*](P \rightarrow [\alpha]P)$

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

LICS'12,JAR'17

Differential Equation Axiomatization

- 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!



Poincaré 1881

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

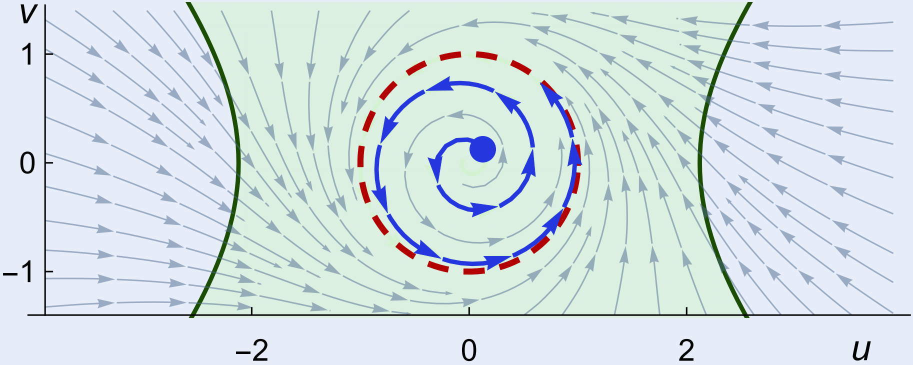
$$x'' = -x \qquad \text{has } x(t) = \sin(t) = t - \frac{t^3}{3!} + \frac{t^5}{5!} - \frac{t^7}{7!} + \frac{t^9}{9!} - \dots$$

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

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

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

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



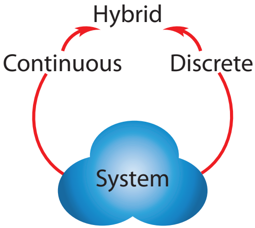
Differential Equation Axiomatization

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.*

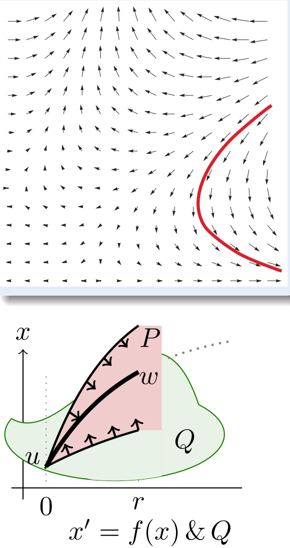
Theorem (Sound & Complete) (JAR'08, LICS'12, JAR'17)

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

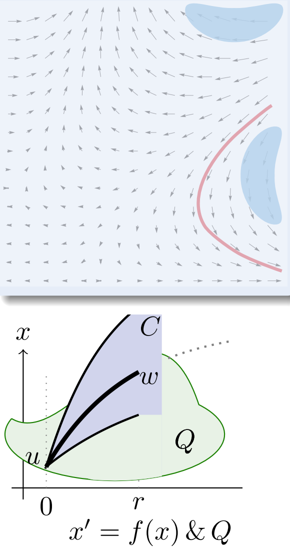


Differential Invariants for Differential Equations

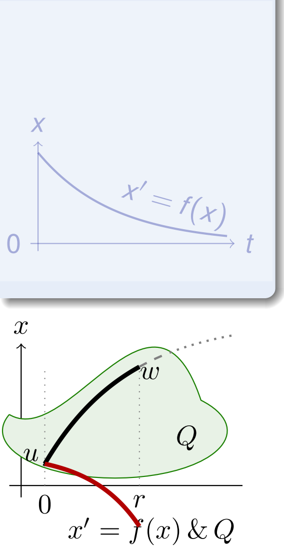
Differential Invariant



Differential Cut

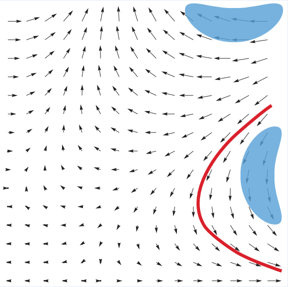


Differential Ghost

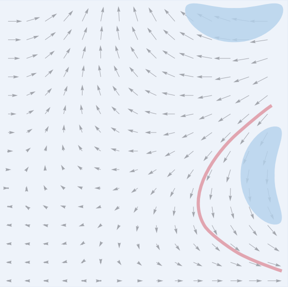


Differential Invariants for Differential Equations

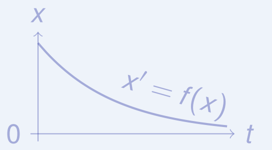
Differential Invariant

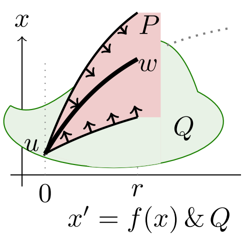


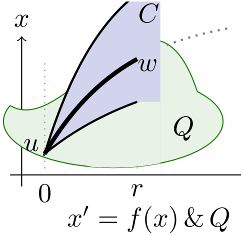
Differential Cut

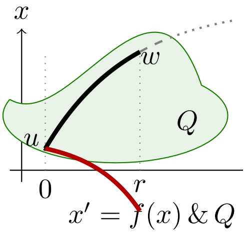


Differential Ghost







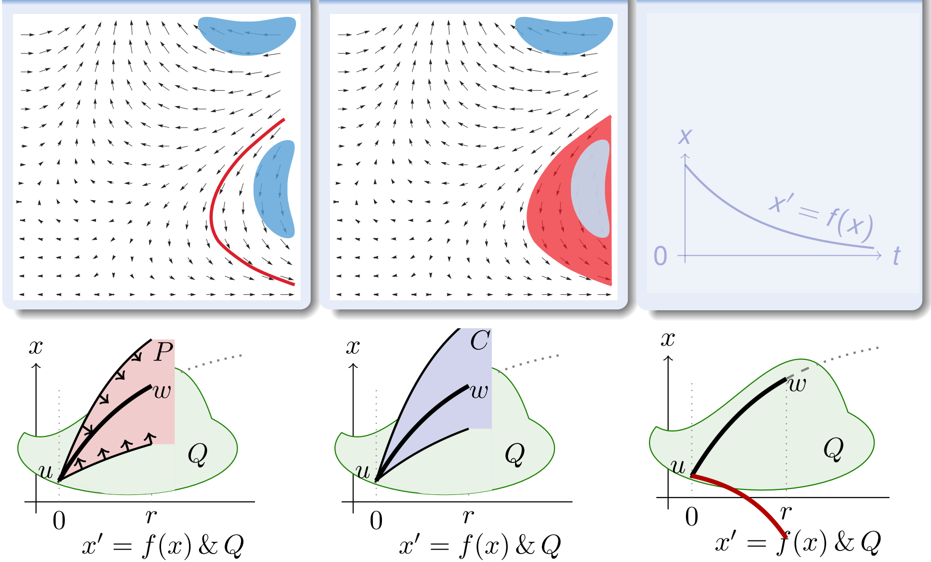


Differential Invariants for Differential Equations

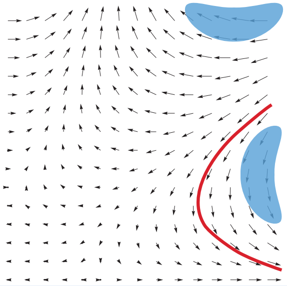
Differential Invariant

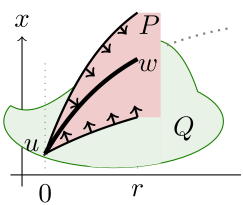
Differential Cut

Differential Ghost



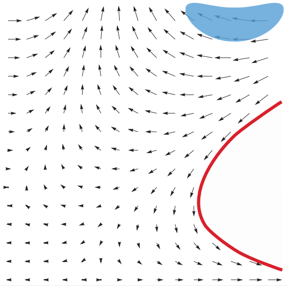
Differential Invariant

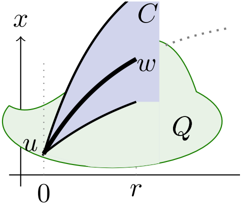




$x' = f(x) \,\&\, Q$

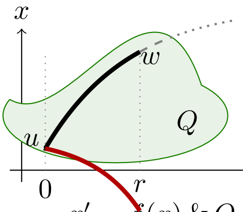
Differential Cut





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

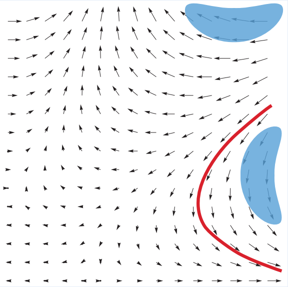
Differential Ghost

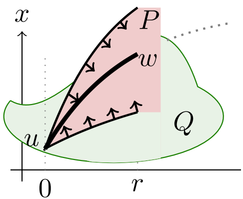


$x' = f(x) \,\&\, Q$

Differential Invariants for Differential Equations

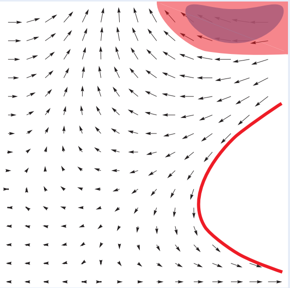
Differential Invariant

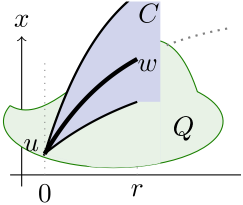




$x' = f(x) \,\&\, Q$

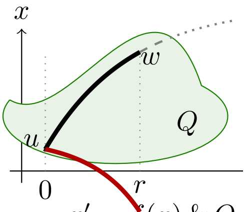
Differential Cut





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

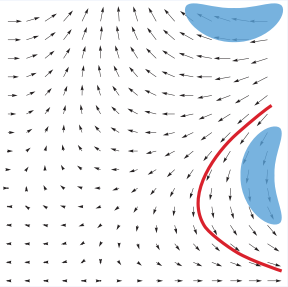
Differential Ghost



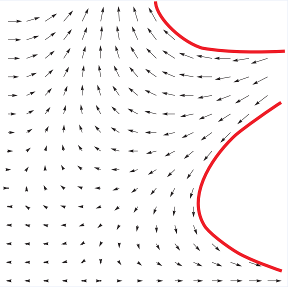
$x' = f(x) \,\&\, Q$

Differential Invariants for Differential Equations

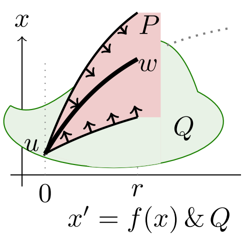
Differential Invariant

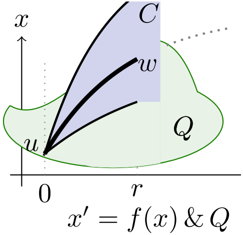


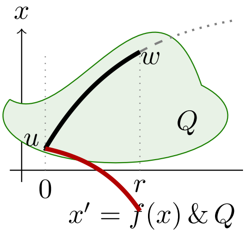
Differential Cut



Differential Ghost

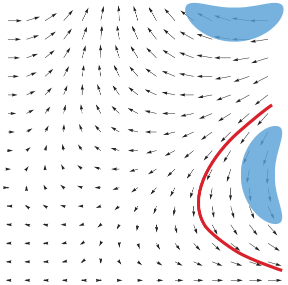




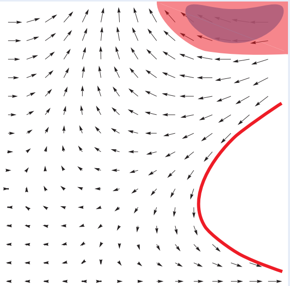


Differential Invariants for Differential Equations

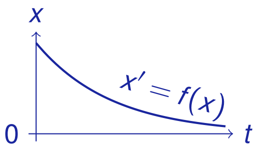
Differential Invariant

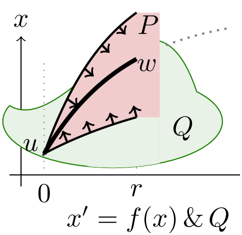


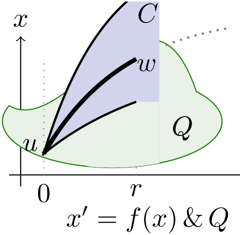
Differential Cut

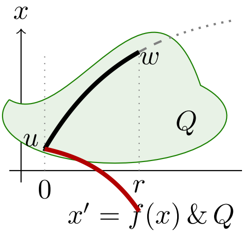


Differential Ghost



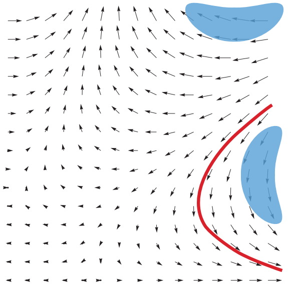




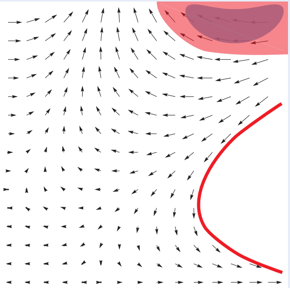


Differential Invariants for Differential Equations

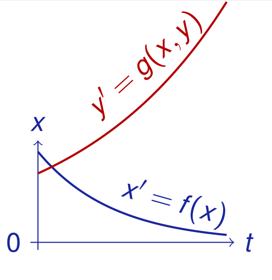
Differential Invariant

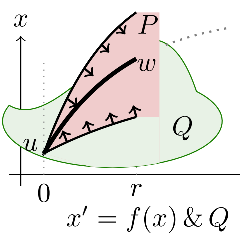


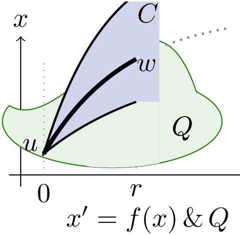
Differential Cut

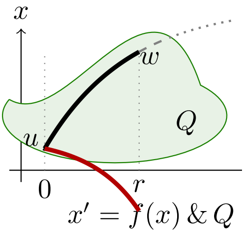


Differential Ghost



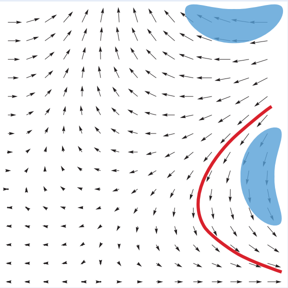




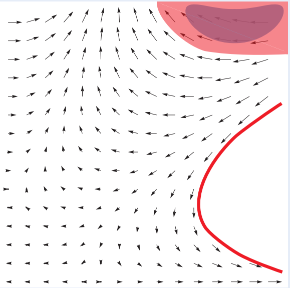


Differential Invariants for Differential Equations

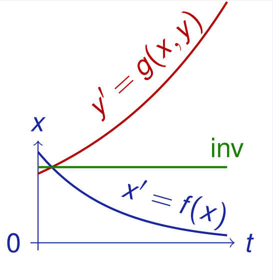
Differential Invariant

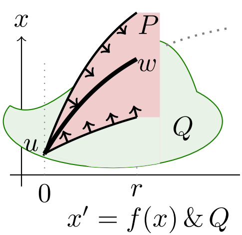


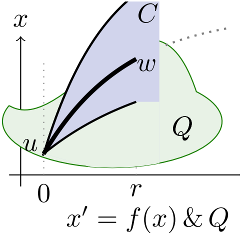
Differential Cut

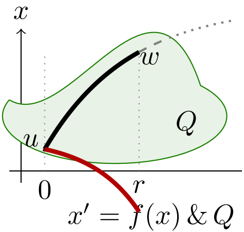


Differential Ghost









Differential Invariants for Differential Equations

Differential Invariant

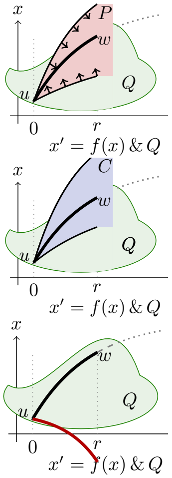
$$\frac{Q \to [x' := f(x)](P)'}{P \to [x' = f(x) \,\&\, Q]P}$$

Differential Cut

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

Differential Ghost

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



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

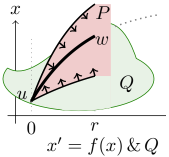
$$\omega[\![(e)']\!] = \sum_x \omega(x') \frac{\partial [\![e]\!]}{\partial x}(\omega)$$

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

Differential Invariants for Differential Equations

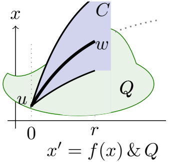
Differential Invariant

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



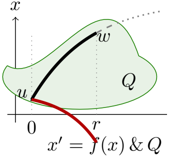
Differential Cut

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



Differential Ghost

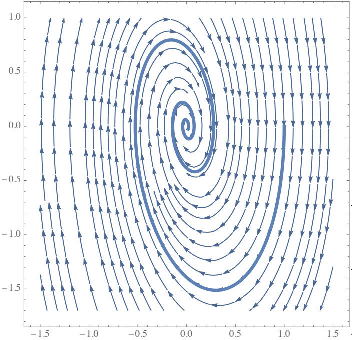
$$\frac{P \leftrightarrow \exists y\, G \quad G \rightarrow [x' = f(x), y' = g(x,y) \,\&\, Q]G}{P \rightarrow [x' = f(x) \,\&\, Q]P}$$

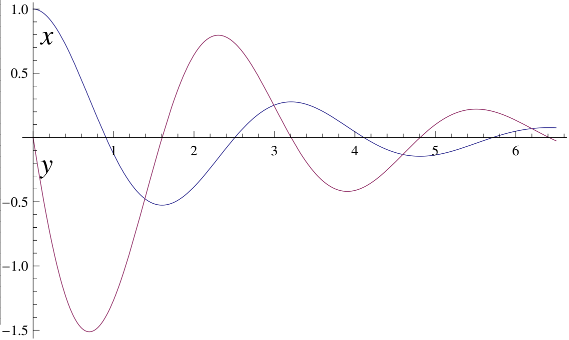


if $g(x,y) = a(x)y + b(x)$, so has long solution!

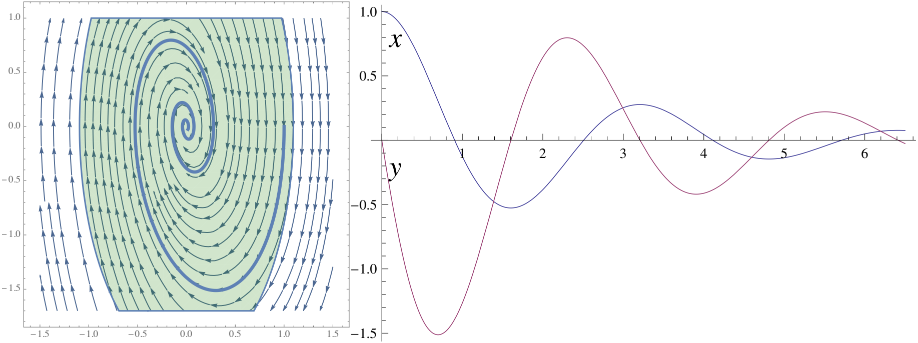
JLogComput'10,LMCS'12, LICS'12,JAR'17,LICS'18

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





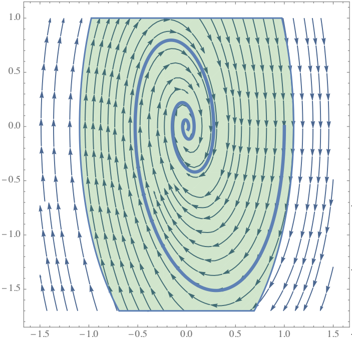
$$\frac{}{\omega^2x^2+y^2\le c^2 \rightarrow [x'=y, y'=-\omega^2x-2d\omega y \,\&\, \omega\ge 0 \wedge d\ge 0]\,\omega^2x^2+y^2\le c^2}$$

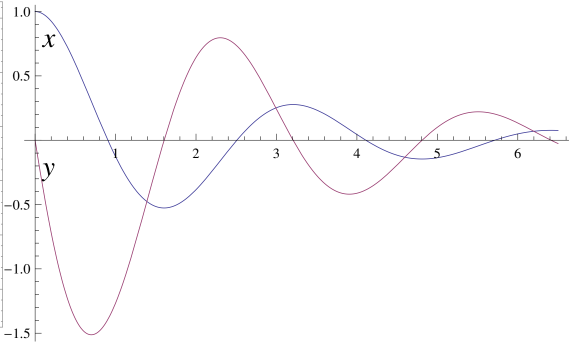


damped oscillator

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

$$\overline{{\color{green}\omega^2x^2+y^2\leq c^2} \rightarrow [x'=y, y'=-\omega^2 x - 2d\omega y \,\&\, \omega\geq 0 \land d\geq 0]\, {\color{green}\omega^2x^2+y^2\leq c^2}}$$



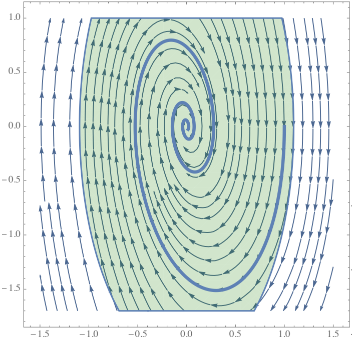


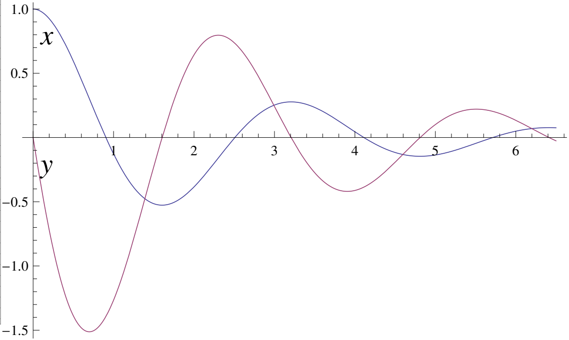
damped oscillator

$$\omega\geq0 \land d\geq0 \rightarrow 2\omega^2 x y + 2y(-\omega^2 x - 2d\omega y) \leq 0$$

$$\omega\geq0 \land d\geq0 \rightarrow [x':=y][y':=-\omega^2 x - 2d\omega y]\,2\omega^2 x x' + 2y y' \leq 0$$

$$\omega^2 x^2 + y^2 \leq c^2 \rightarrow [x' = y, y' = -\omega^2 x - 2d\omega y \,\&\, \omega\geq0 \land d\geq0]\,\omega^2 x^2 + y^2 \leq c^2$$





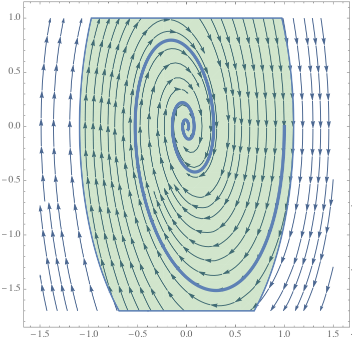
damped oscillator

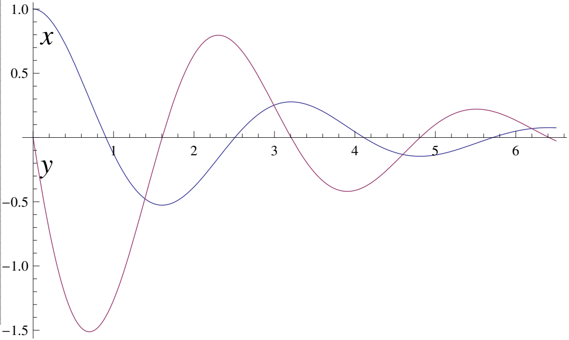
$$*$$

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

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

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

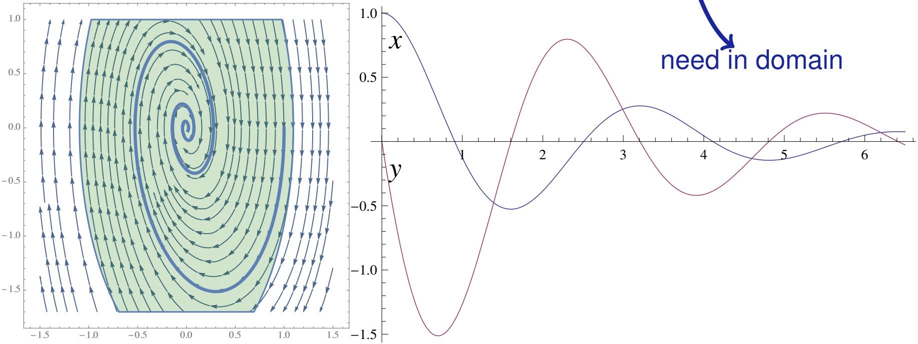




damped oscillator

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

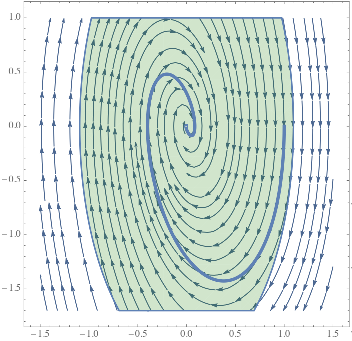
need in domain

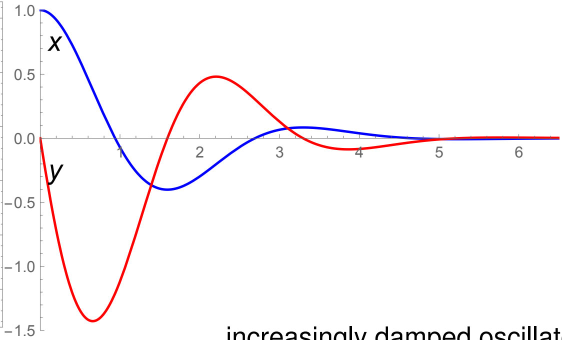


damped oscillator

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

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





increasingly damped oscillator

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

increasingly damped oscillator

Differential Cuts for Differential Equations

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

ask

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

increasingly damped oscillator

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

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

increasingly damped oscillator

$$\dfrac{\dfrac{}{\omega^2x^2+y^2\le c^2 \to [x'=y,y'=-\omega^2x-2d\omega y, d'=7 \,\&\, \omega\ge 0\wedge d\ge 0]\, \omega^2x^2+y^2\le c^2}}{\omega^2x^2+y^2\le c^2 \to [x'=y,y'=-\omega^2x-2d\omega y, d'=7 \,\&\, \omega\ge 0]\, \omega^2x^2+y^2\le c^2}$$

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

increasingly damped oscillator

Differential Cuts for Differential Equations

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

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

DC

$$*$$

$$\omega\ge 0 \rightarrow 7\ge 0$$

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

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

increasingly damped oscillator

$$\omega\ge0\land d\ge0 \to [x':=y][y':=-\omega^2x-2d\omega y]\,2\omega^2xx'+2yy'\le0$$

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

$$\omega^2x^2+y^2\le c^2 \to [x'=y,y'=-\omega^2x-2d\omega y,d'=7\,\&\,\omega\ge0]\,\omega^2x^2+y^2\le c^2$$

$$*$$

$$\omega\ge0\to7\ge0$$

$$\omega\ge0\to[d':=7]\,d'\ge0$$

$$d\ge0\to[x'=y,y'=-\omega^2x-2d\omega y,d'=7\,\&\,\omega\ge0]\,d\ge0$$

increasingly damped oscillator

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

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

increasingly damped oscillator

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

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

increasingly damped oscillator

Differential Cuts for Differential Equations

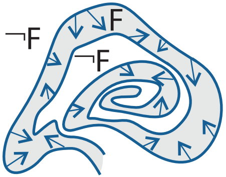
$$\dfrac{\dfrac{\dfrac{*}{\omega\geq 0\land d\geq 0 \rightarrow 2\omega^2xy+2y(-\omega^2x-2d\omega y)\leq 0}}{\omega\geq 0\land d\geq 0 \rightarrow [x':=y][y':=-\omega^2x-2d\omega y]\,2\omega^2xx'+2yy'\leq 0}}{\omega^2x^2+y^2\leq c^2 \rightarrow [x'=y,y'=-\omega^2x-2d\omega y,d'=7\,\&\,\omega\geq 0\land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

init

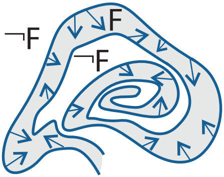
$$\dfrac{\dfrac{\dfrac{*}{\omega\geq 0 \rightarrow 7\geq 0}}{\omega\geq 0 \rightarrow [d':=7]\,d'\geq 0}}{d\geq 0 \rightarrow [x'=y,y'=-\omega^2x-2d\omega y,d'=7\,\&\,\omega\geq 0]\,d\geq 0}$$

Could repeatedly diffcut in formulas to help the proof

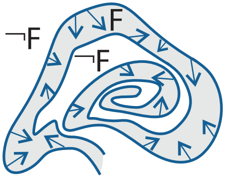
Assuming Differential Invariance

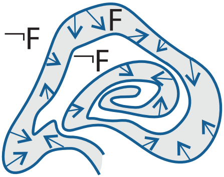


$$\frac{Q \rightarrow [x' := f(x)](F)'}{F \rightarrow [x' = f(x) \,\&\, Q]F}$$



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





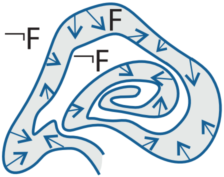
$$\frac{Q \rightarrow [x' := f(x)](F)'}{F \rightarrow [x' = f(x) \,\&\, Q]F}$$

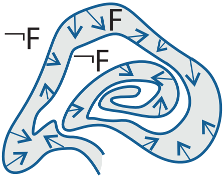
$$\frac{F \land Q \rightarrow [x' := f(x)](F)'}{F \rightarrow [x' = f(x) \,\&\, Q]F}$$

Example (Inductive hypothesis)

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

Assuming Differential Invariance



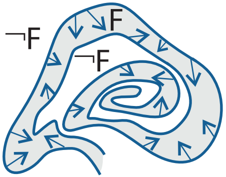


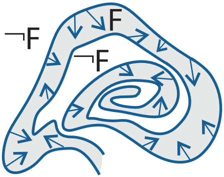
$$\frac{Q \rightarrow [x' := f(x)](F)'}{F \rightarrow [x' = f(x) \,\&\, Q]F}$$

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

Example (Inductive hypothesis)

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





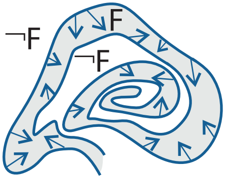
$$\frac{Q \rightarrow [x' := f(x)](F)'}{F \rightarrow [x' = f(x) \,\&\, Q]F}$$

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

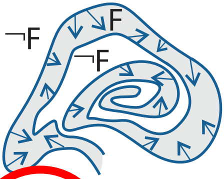
Example (Inductive hypothesis)

$$\cfrac{\cfrac{\cfrac{}{v^2 - 2v + 1 = 0 \rightarrow 2vw - 2w = 0}}{v^2 - 2v + 1 = 0 \rightarrow [v' := w][w' := -v]2vv' - 2v' = 0}}{v^2 - 2v + 1 = 0 \rightarrow [v' = w, w' = -v]v^2 - 2v + 1 = 0}$$

Assuming Differential Invariance



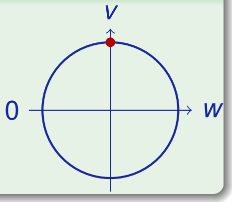
$$\frac{Q \rightarrow [x' := f(x)](F)'}{F \rightarrow [x' = f(x) \,\&\, Q]F}$$



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

Example (Inductive hypothesis is unsound!)

$$\frac{\frac{\frac{(\text{unsound})}{v^2 - 2v + 1 = 0 \rightarrow 2vw - 2w = 0}}{v^2 - 2v + 1 = 0 \rightarrow [v' := w][w' := -v]2vv' - 2v' = 0}}{v^2 - 2v + 1 = 0 \rightarrow [v' = w, w' = -v]v^2 - 2v + 1 = 0}$$

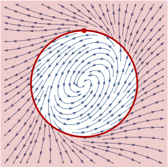


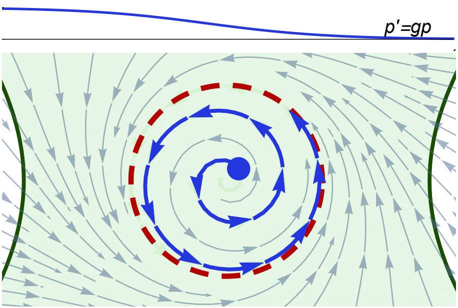
Induction for ODEs is subtle!

Example Proof Derived by Differential Ghosts

Darboux inequalities are DG

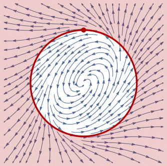
$$\frac{Q \to p^{\bullet} \geq gp}{p \succcurlyeq 0 \to [x' = f(x) \,\&\, Q] p \succcurlyeq 0} \quad (g \in \mathbb{R}[x])$$





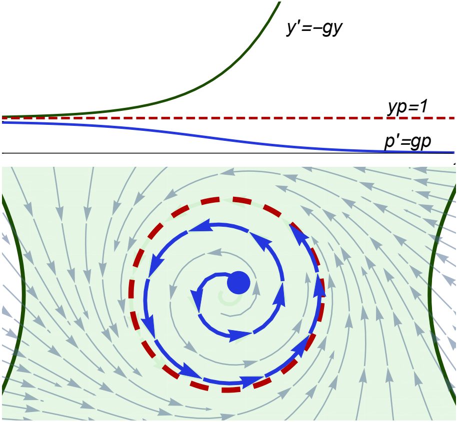
$$\frac{(1-u^2-v^2)^{\bullet} \geq -\frac{1}{2}(u^2+v^2)(1-u^2-v^2)}{\ldots \to \left[\begin{aligned} u' &= -v + \tfrac{u}{4}(1-u^2-v^2) \\ v' &= u + \tfrac{v}{4}(1-u^2-v^2) \end{aligned}\right] \underbrace{1-u^2-v^2 > 0}}$$

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



Darboux inequalities are DG

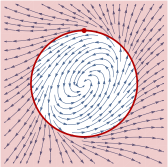
$$\frac{Q \rightarrow p^{\bullet} \geq gp}{p \succcurlyeq 0 \rightarrow [x' = f(x) \,\&\, Q]\, p \succcurlyeq 0} \quad (g \in \mathbb{R}[x])$$

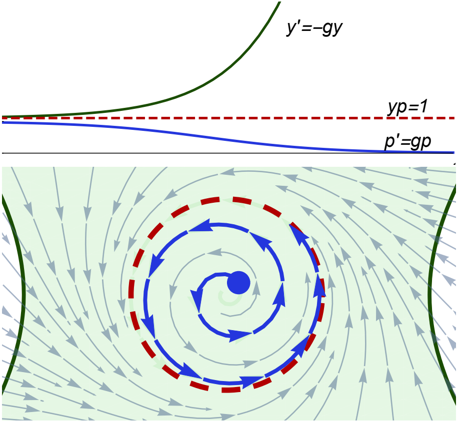


$$\dfrac{(1-u^2-v^2)^{\bullet} \geq -\tfrac{1}{2}(u^2+v^2)(1-u^2-v^2)}{\ldots \rightarrow \left[\begin{aligned} u' &= -v + \tfrac{u}{4}(1-u^2-v^2) \\ v' &= u + \tfrac{v}{4}(1-u^2-v^2) \\ y' &= \tfrac{1}{2}(u^2+v^2)y \end{aligned}\right] \underbrace{1-u^2-v^2 > 0}_{y(1-u^2-v^2)=1}}$$

Darboux inequalities are DG

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





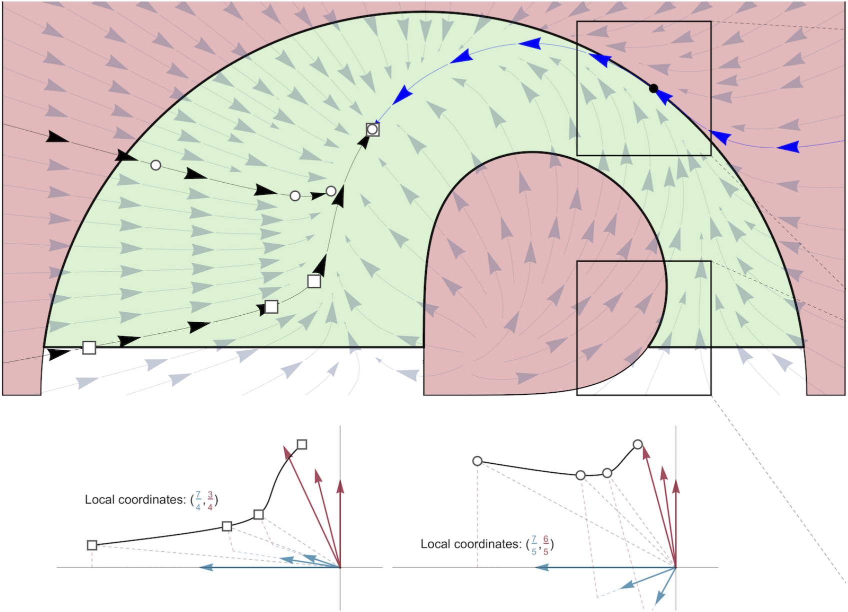
$$\frac{(1-u^2-v^2)^{\bullet} \geq -\frac{1}{2}(u^2+v^2)(1-u^2-v^2)}{\ldots \to \left[\begin{aligned} u' &= -v + \tfrac{u}{4}(1-u^2-v^2) \\ v' &= u + \tfrac{v}{4}(1-u^2-v^2) \\ y' &= \tfrac{1}{2}(u^2+v^2)y \\ z' &= -\tfrac{1}{4}(u^2+v^2)z \end{aligned}\right] \underbrace{1-u^2-v^2 > 0}_{y(1-u^2-v^2)=1}}$$

Example Proof Derived by Differential Ghosts

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

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{Q \rightarrow p^{\bullet} \geq gp \qquad \dfrac{*}{p^{\bullet} \geq gp, y > 0 \rightarrow p^{\bullet} y - gyp \geq 0}\ \mathbb{R}}{Q, y > 0 \rightarrow p^{\bullet} y - gyp \geq 0}\ \text{cut}}{p \succcurlyeq 0, y > 0 \rightarrow [x' = f(x), y' = -gy \,\&\, Q \land y > 0]py \succcurlyeq 0 \quad \triangleright}\ \text{dI}}{p \succcurlyeq 0, y > 0 \rightarrow [x' = f(x), y' = -gy \,\&\, Q](y > 0 \land py \succcurlyeq 0)}\ \text{dC}}{p \succcurlyeq 0 \rightarrow \exists y\,[x' = f(x), y' = -gy \,\&\, Q]p \succcurlyeq 0}\ \text{M}[\cdot],\exists\text{R}}{p \succcurlyeq 0 \rightarrow [x' = f(x) \,\&\, Q]p \succcurlyeq 0}\ \text{dG}
$$

Completeness for Differential Equation Invariants



LICS'18

Differential Equation Axiomatization

Theorem (Algebraic Completeness) (LICS'18)

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

Theorem (Semialgebraic Completeness) (LICS'18)

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

Differential Equation Axiomatization

Theorem (Algebraic Completeness) (LICS'18)

dL *calculus is a sound & complete axiomatization of algebraic invariants of polynomial differential equations. They are decidable with a derived axiom (on open Q for completeness):*

$$\text{DRI } [x' = f(x) \,\&\, Q]p = 0 \leftrightarrow \big(Q \rightarrow p^{\bullet(*)} = 0\big)$$

Theorem (Semialgebraic Completeness) (LICS'18)

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

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

Definable $p^{\bullet(*)}$ is short for *all/significant* Lie derivative w.r.t. ODE
Definable $p^{\bullet(-*)}$ is w.r.t. backwards ODE. Also for DNF P.

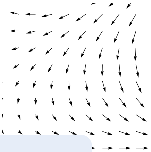
Differentials

Syntax

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

Semantics

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



Axioms

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

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

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

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

ODE

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

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

JAR'17

Differential Substitution Lemmas ⇝ Proofs

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

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

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

Lemma (Differential assignment) (Effect on Differentials)

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

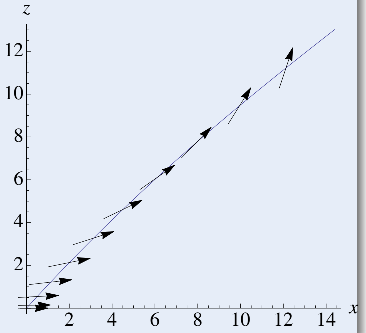
Lemma (Derivations) (Equations of Differentials)

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

Example: Longitudinal Dynamics of an Airplane

Study (6th Order Longitudinal Flight Equations)

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



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

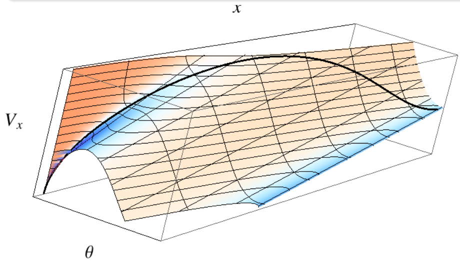
with Khalil Ghorbal TACAS'14

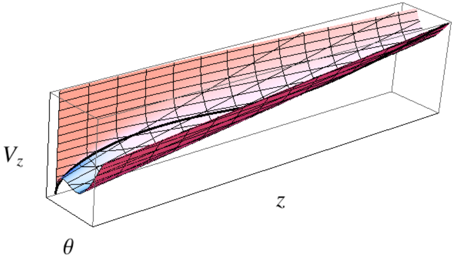
Result (DRI Automatically Generates Invariant Functions)

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

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

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



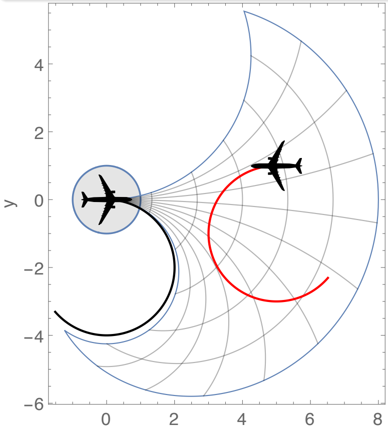


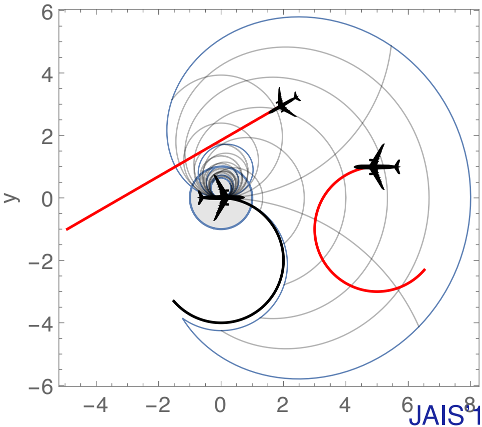
with Khalil Ghorbal TACAS'14

Result (DRI Automatically Generates Invariants)

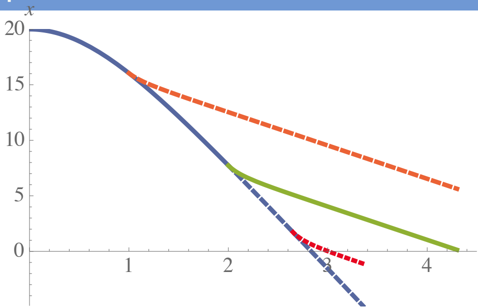
$$\omega_1 = 0 \land \omega_2 = 0 \rightarrow v_2 \sin\vartheta x = (v_2 \cos\vartheta - v_1) y > p(v_1 + v_2)$$

$$\omega_1 \neq 0 \lor \omega_2 \neq 0 \rightarrow -\omega_1\omega_2(x^2+y^2) + 2v_2\omega_1 \sin\vartheta x + 2(v_1\omega_2 - v_2\omega_1\cos\vartheta)y + 2v_1v_2\cos\vartheta > 2v_1v_2 + 2p(v_2|\omega_1| + v_1|\omega_2|) + p^2|\omega_1\omega_2|$$

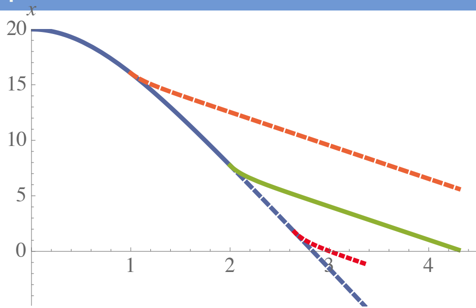




JAIS'14

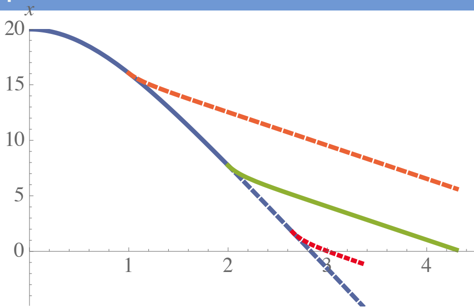

x
20
15
10
5
0
1
2
3
4

Ex: Parachute Open or Keep Closed



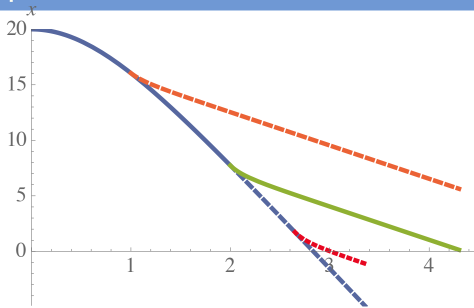
Example (Parachute)

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



Example (Parachute)

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

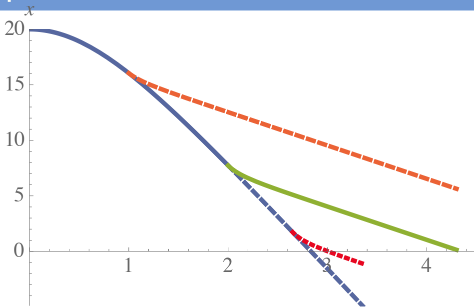


Example (Parachute)

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

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

Conservatively bounded next velocity above parachute's limit velocity.



Example (Parachute)

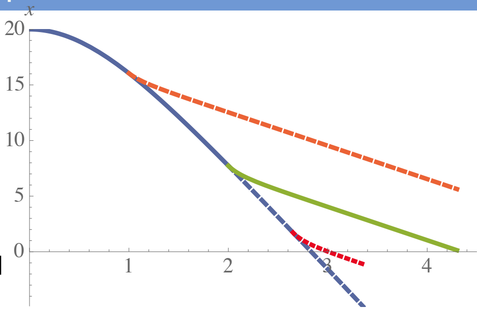
$$m < -\sqrt{g/p} \rightarrow \Big[\big((?(Q \land r = a) \cup r := p); t := 0;$$
$$\{x' = v, v' = -g + rv^2, t' = 1 \,\&\, t \leq T \land x \geq 0 \land v < 0\}\big)^*\Big]$$
$$(x = 0 \rightarrow v \geq m)$$

Ex: Parachute Open or Keep Closed

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

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

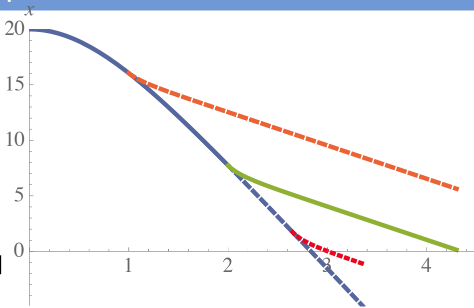
$$y' = -\frac{p}{2}(v - \sqrt{g/p}) \qquad y^2(\underbrace{v + \sqrt{g/p}}_{>0}) = 1$$



Example (Parachute)

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

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



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

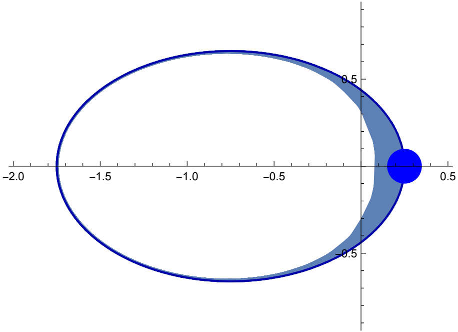
$$y' = -\frac{p}{2}(v - \sqrt{g/p}) \quad y^2(\underbrace{v + \sqrt{g/p}}_{>0}) = 1$$

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

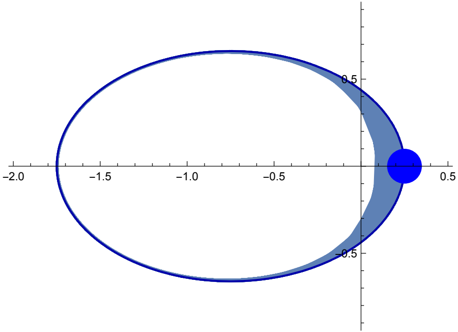
Example (Parachute)

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

Ex: Kepler Two Body Problem



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

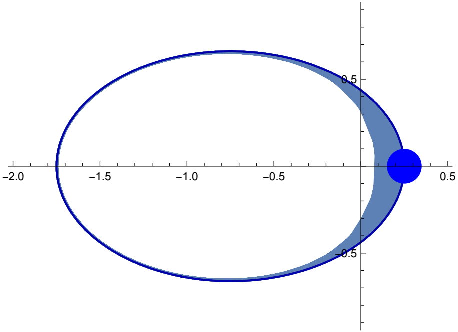


Example (Two Body Problem)

$$\left[x' = v, v' = -x/(x^2+y^2)^{3/2},\right.$$
$$\left. y' = w, w' = -y/(x^2+y^2)^{3/2}\right]$$

Ex: Kepler Two Body Problem

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

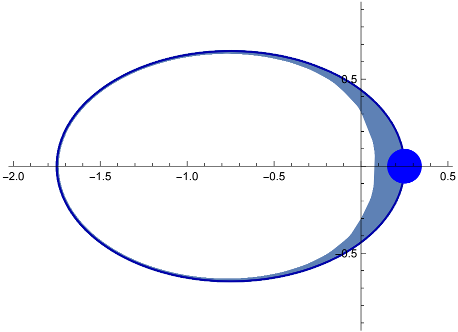


Example (Two Body Problem)

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

Ex: Kepler Two Body Problem

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

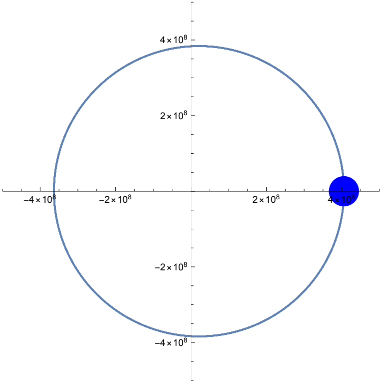


Example (Two Body Problem)

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

$\& \, x \neq 0 \lor y \neq 0$

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



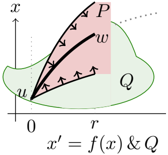
Example (Moon around Earth)

$$\cdots \rightarrow \left[x' = v, v' = -GMx/(x^2+y^2)^{3/2},\right.$$
$$\left. y' = w, w' = -GMy/(x^2+y^2)^{3/2} \,\&\, x \neq 0 \lor y \neq 0\right] \ldots$$

Summary: Proving ODEs

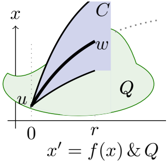
Differential Invariant

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



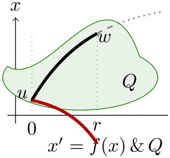
Differential Cut

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



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!

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

Outline (Logic for CPS)

Acknowledgments

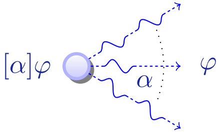
Logical Systems Lab at Carnegie Mellon University, Computer Science
Yong Kiam Tan, Brandon Bohrer, Nathan Fulton, Sarah Loos, Katherine Cordwell
Stefan Mitsch, Khalil Ghorbal, Jean-Baptiste Jeannin, Andrew Sogokon

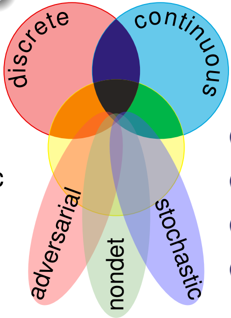
Unterstützt von / Supported by
Alexander von Humboldt
Stiftung / Foundation

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

differential dynamic logic

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





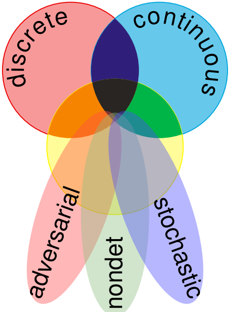
- Multi-dynamical systems
- Hybrid programs + dL logic
- Compositional proofs
- Decide invariant by dL

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

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

Numerous wonders remain to be discovered

- Verified CPS implementations by ModelPlex — FMSD'16
- Correct CPS execution — PLDI'18
- CPS proof and tactic languages+libraries — ITP'17
- Big CPS built from safe components — STTT'18
- Stochastic hybrid systems — CADE'11
- Invariant generation — FM'19
- Safe AI autonomy in CPS — AAAI'18 TACAS'19
- Correct model transformation — FM'14
- Refinement + system property proofs — LICS'16
- CPS information flow — LICS'18
- Hybrid games — TOCL'15



CPSs deserve proofs as safety evidence!

A. Platzer. *Logical Foundations of Cyber-Physical Systems*. Springer 2018

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

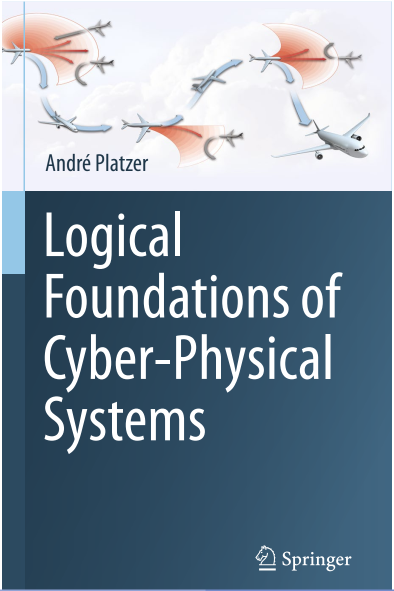
II Part: Differential Equations Analysis

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



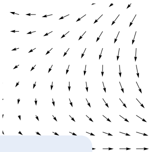
Outline

7. Appendix
   - Differentials
   - Differential Ghosts
   - Differential Radical Invariants

Differentials

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

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



$\to \mathbb{R}$

Axioms

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

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

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

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

ODE

$$[\![x' = f(x) \,\&\, Q]\!] = \{(\varphi(0)|_{\{x'\}^\complement}, \varphi(r)) : \varphi \models x' = f(x) \wedge Q$$

$$\text{for some } \varphi : [0,r] \to \mathcal{S}, \text{ some } r \in \mathbb{R}\}$$

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

JAR'17

Differential Substitution Lemmas

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

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

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

Lemma (Differential assignment) (Effect on Differentials)

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

Lemma (Derivations) (Equations of Differentials)

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

Differential Substitution Lemmas

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

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

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

Lemma (Differential assignment) (Effect on Differentials)

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

Lemma (Derivations) (Equations of Differentials)

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

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

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

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

Differential Substitution Lemmas

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

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

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

Lemma (Differential assignment) (Effect on Differentials)

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

Lemma (Derivations) (Equations of Differentials)

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

Differential Substitution Lemmas

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

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

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

Lemma (Differential assignment) (Effect on Differentials)

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

Lemma (Derivations) (Equations of Differentials)

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

Differential Substitution Lemmas ⤳ Proofs

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

$$DI\ \frac{\rightarrow [x' = f(x)\,\&\,Q](e)' = 0}{e = 0 \rightarrow [x' = f(x)\,\&\,Q]e = 0}$$

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)

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

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

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

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

Lemma (Differential assignment) (Effect on Differentials)

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

Lemma (Derivations) (Equations of Differentials)

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

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

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

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

Lemma (Differential assignment) (Effect on Differentials)

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

Axiomatics

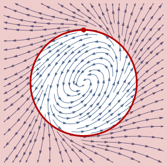
DE $[x' = f(x) \,\&\, Q]P \leftrightarrow [x' = f(x) \,\&\, Q][x' := f(x)]P$

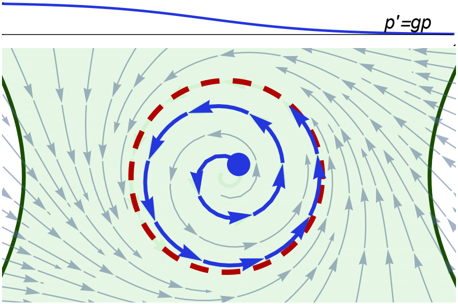
DI $\dfrac{\rightarrow [x' = f(x) \,\&\, Q](e)' = 0}{e = 0 \rightarrow [x' = f(x) \,\&\, Q]e = 0}$

ODE Axiomatization: Derived Darboux Rules

Darboux inequalities are DG

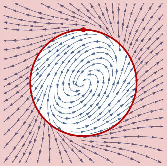
$$\frac{Q \to p^{\bullet} \geq gp}{p \succcurlyeq 0 \to [x' = f(x) \,\&\, Q]\, p \succcurlyeq 0} \quad (g \in \mathbb{R}[x])$$





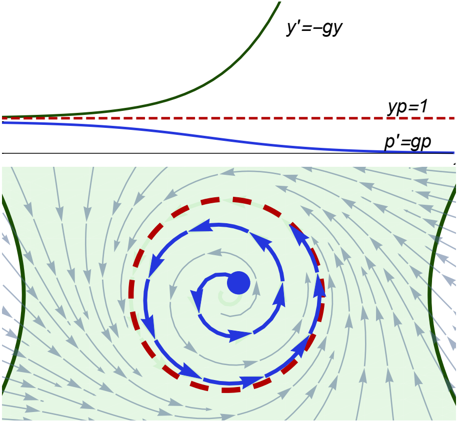
$$\frac{(1-u^2-v^2)^{\bullet} \geq -\frac{1}{2}(u^2+v^2)(1-u^2-v^2)}{\ldots \to \left[\begin{array}{l} u' = -v + \frac{u}{4}(1-u^2-v^2) \\ v' = \quad u + \frac{v}{4}(1-u^2-v^2) \end{array}\right] 1-u^2-v^2 > 0}$$

ODE Axiomatization: Derived Darboux Rules



Darboux inequalities are DG

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



$$\frac{(1-u^2-v^2)^{\bullet} \geq -\frac{1}{2}(u^2+v^2)(1-u^2-v^2)}{\ldots \rightarrow \left[\begin{aligned} u' &= -v + \tfrac{u}{4}(1-u^2-v^2) \\ v' &= \;\;\, u + \tfrac{v}{4}(1-u^2-v^2) \\ y' &= \tfrac{1}{2}(u^2+v^2)y \end{aligned}\right]\, 1-u^2-v^2 > 0}$$

$$(1-u^2-v^2)y > 0$$

Darboux Inequalities are Differential Ghosts: Details

$$
\text{dG}\;\dfrac{\text{M}[\cdot],\exists\text{R}\;\dfrac{\text{dI}\;\dfrac{\mathbb{R}\;\dfrac{*}{Q \to (-gy)z^2 + y(2z(\frac{g}{2}z)) = 0}}{yz^2 = 1 \to [x' = f(x), y' = -gy, z' = \frac{g}{2}z \,\&\, Q]\, yz^2 = 1}}{y > 0 \to \exists z\, [x' = f(x), y' = -gy, z' = \frac{g}{2}z \,\&\, Q]\, y > 0}}{y > 0 \to [x' = f(x), y' = -gy \,\&\, Q]\, y > 0}
$$

$$
\text{dG}\;\dfrac{\text{M}[\cdot],\exists\text{R}\;\dfrac{\text{dC}\;\dfrac{\text{dI}\;\dfrac{\text{cut}\;\dfrac{Q \to p^{\bullet} \geq gp \qquad \mathbb{R}\;\dfrac{*}{p^{\bullet} \geq gp, y > 0 \to p^{\bullet} y - gyp \geq 0}}{Q, y > 0 \to p^{\bullet} y - gyp \geq 0}}{p \succcurlyeq 0, y > 0 \to [x' = f(x), y' = -gy \,\&\, Q \land y > 0]\, py \succcurlyeq 0 \quad \triangleright}}{p \succcurlyeq 0, y > 0 \to [x' = f(x), y' = -gy \,\&\, Q](y > 0 \land py \succcurlyeq 0)}}{p \succcurlyeq 0 \to \exists y\, [x' = f(x), y' = -gy \,\&\, Q]\, p \succcurlyeq 0}}{p \succcurlyeq 0 \to [x' = f(x) \,\&\, Q]\, p \succcurlyeq 0}
$$

P.S. $z' = \frac{g}{2}z$ superfluous for open inequalities $p > 0$ and $p \neq 0$.

Differential Radical Invariants

Theorem (Differential radical invariant characterization)

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

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

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

Corollary (Algebraic Invariants Decidable)

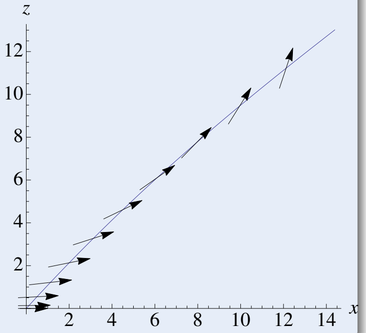
Algebraic invariants of algebraic differential equations are decidable.

with Khalil Ghorbal TACAS'14

Example: Longitudinal Dynamics of an Airplane

Study (6th Order Longitudinal Flight Equations)

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



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

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

with Khalil Ghorbal TACAS'14

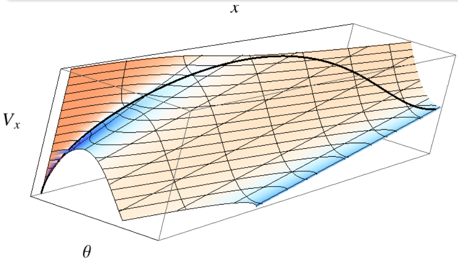
Example: Longitudinal Dynamics of an Airplane

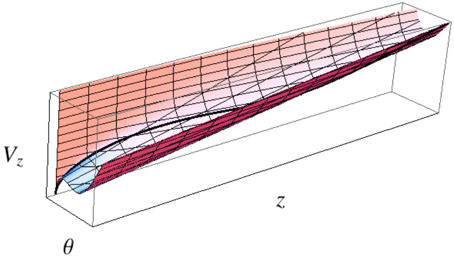
Result (DRI Automatically Generates Invariant Functions)

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

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

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





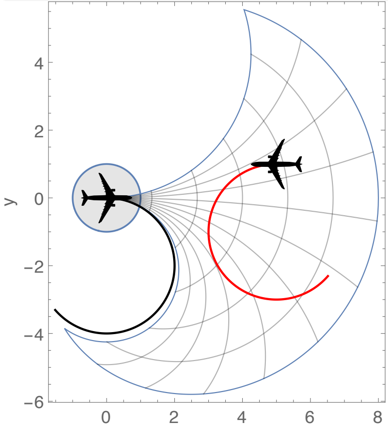
with Khalil Ghorbal TACAS'14

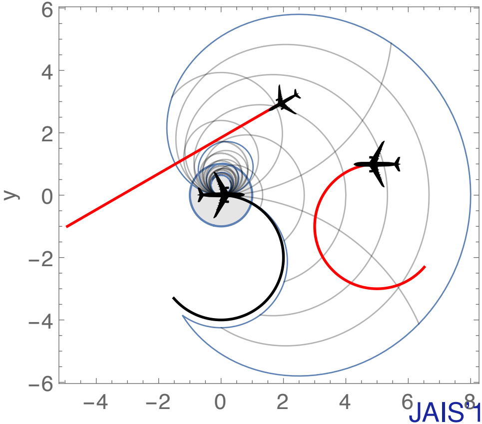
Example: Dubins Dynamics of 2 Airplanes

Result (DRI Automatically Generates Invariants)

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

$$\omega_1 \neq 0 \vee \omega_2 \neq 0 \rightarrow -\omega_1\omega_2(x^2 + y^2) + 2v_2\omega_1 \sin\vartheta\, x + 2(v_1\omega_2 - v_2\omega_1\cos\vartheta) y + 2v_1v_2\cos\vartheta > 2v_1v_2 + 2p(v_2|\omega_1| + v_1|\omega_2|) + p^2|\omega_1\omega_2|$$





JAIS'14

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

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

André Platzer.
Logics of dynamical systems.
In LICS [19], pages 13–24.
doi: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.

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 [19], 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.

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.

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

André Platzer.
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.

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

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

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

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

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

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