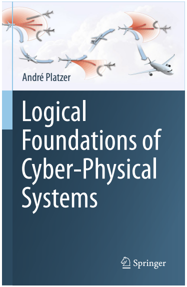
Programming Cyber-Physical Systems With Logic

André Platzer

Carnegie Mellon University

Symposium on Principles of Programming Languages 2019 TutorialFest

`http://keymaeraX.org/`



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.

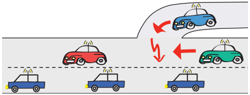
CPSs Promise Transformative Impact!

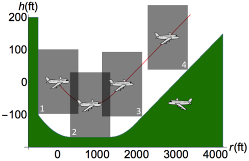
Prospects: Safe & Efficient

Driver assistance
Autonomous cars

Pilot decision support
Autopilots / UAVs

Train protection
Robots near humans





Prerequisite: CPSs need to be safe

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

Can you trust a computer to control physics?

Can you trust a computer to control physics?

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

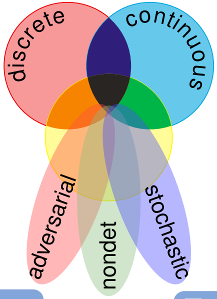
Rationale

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

CPSs deserve proofs as safety evidence!

CPS Dynamics

CPS are characterized by multiple facets of dynamical systems.



CPS Compositions

CPS combines multiple simple dynamical effects.

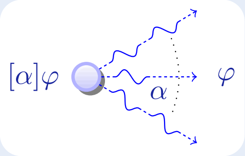
Descriptive simplification

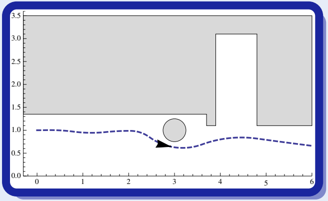
Tame Parts

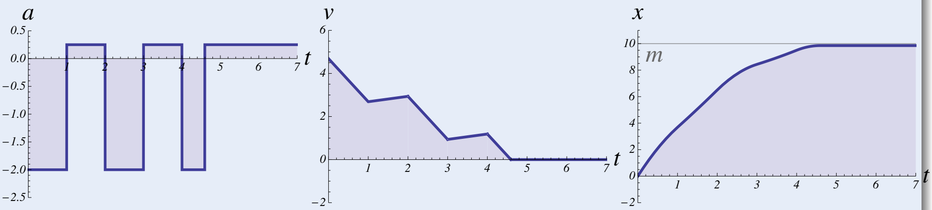
Exploiting compositionality tames CPS complexity.

Analytic simplification

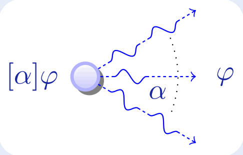
Concept (Differential Dynamic Logic) (JAR'08,LICS'12)

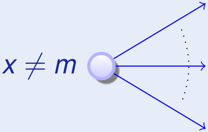


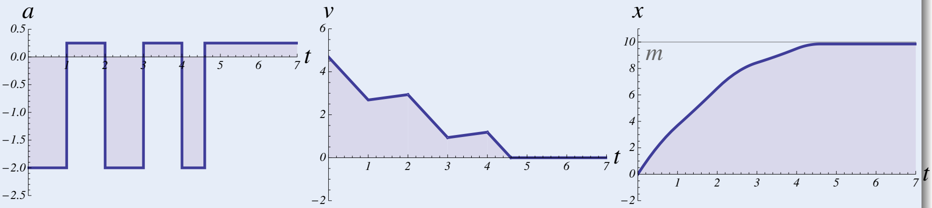




Concept (Differential Dynamic Logic) (JAR'08,LICS'12)

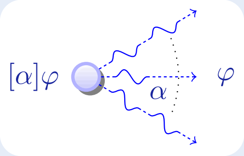


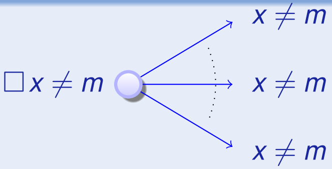


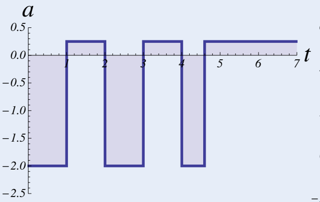


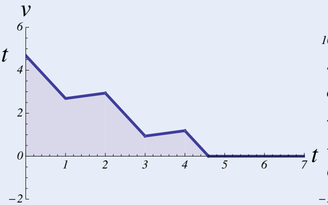
CPS Analysis

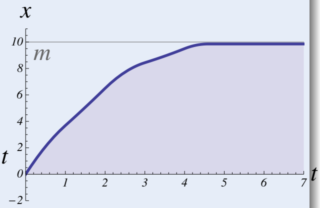
Concept (Differential Dynamic Logic) (JAR'08,LICS'12)





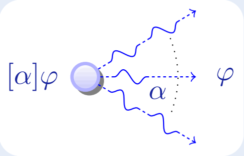


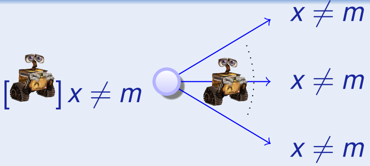


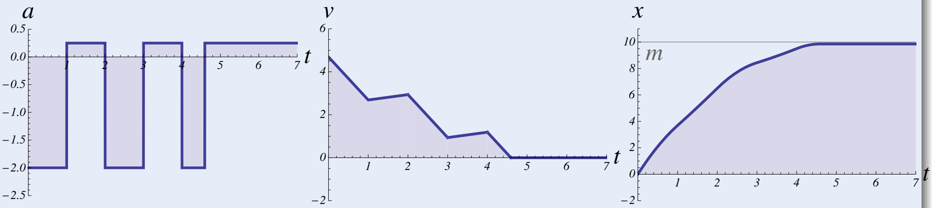


CPS Analysis

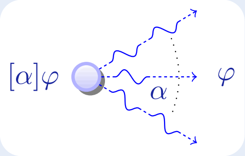
Concept (Differential Dynamic Logic) (JAR'08,LICS'12)

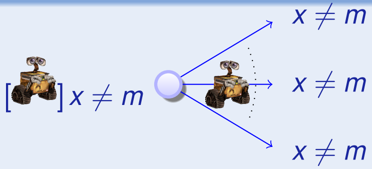




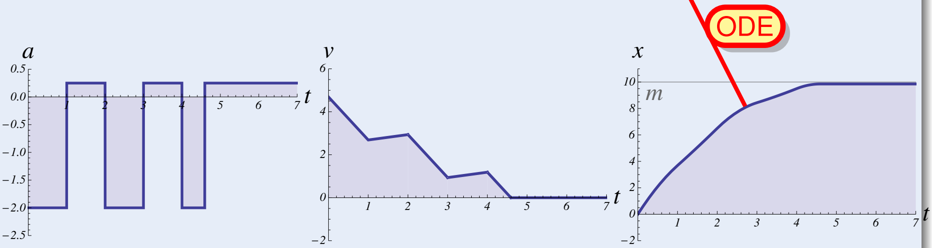


Concept (Differential Dynamic Logic) (JAR'08,LICS'12)

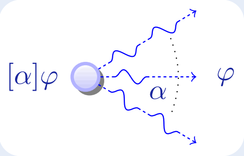


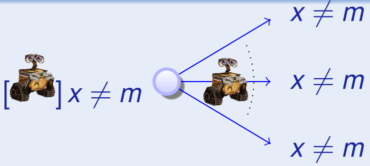


$$x' = v, v' = a$$

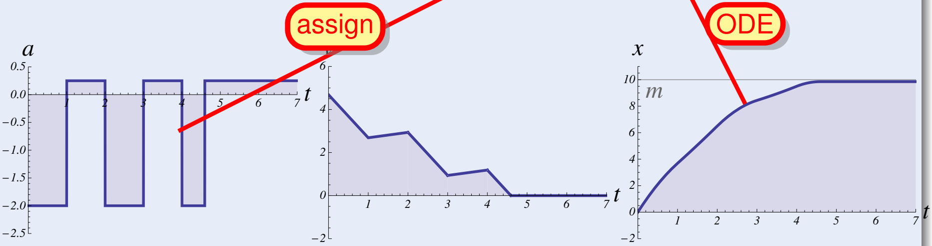


Concept (Differential Dynamic Logic) (JAR'08,LICS'12)

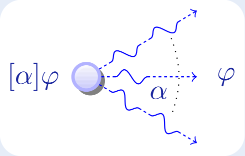


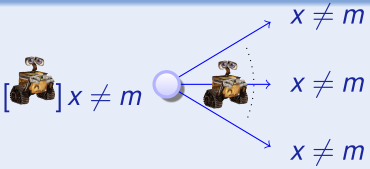


$a := -b$ $\quad x' = v, v' = a$

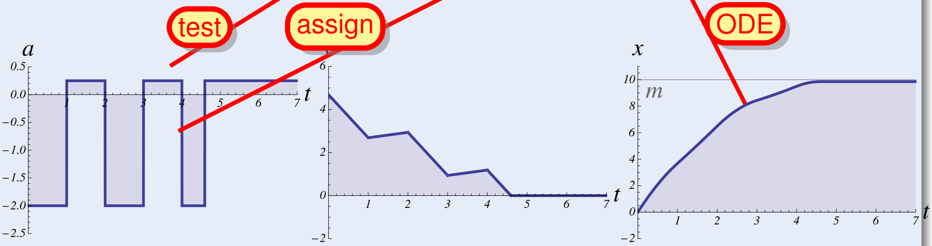


Concept (Differential Dynamic Logic) (JAR'08,LICS'12)

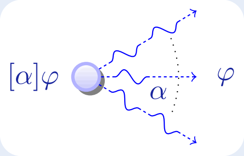




$(\text{if}(SB(x,m)) \quad a := -b) \quad x' = v, v' = a$



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



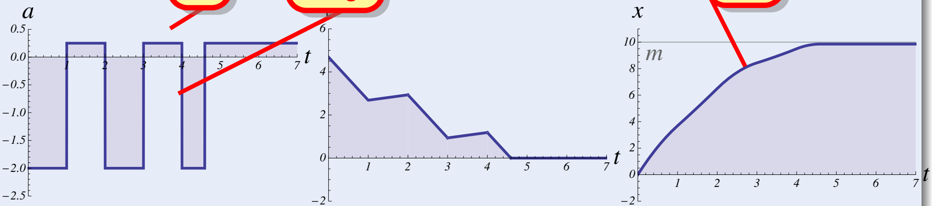
seq. compose

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

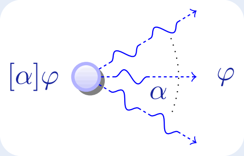
test

assign

ODE



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



seq. compose

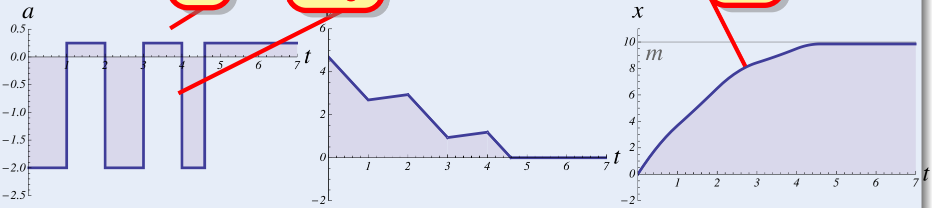
nondet. repeat

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

test

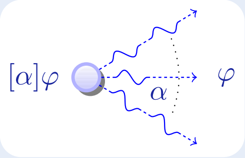
assign

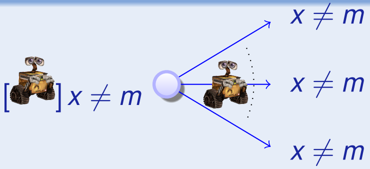
ODE



CPS Analysis

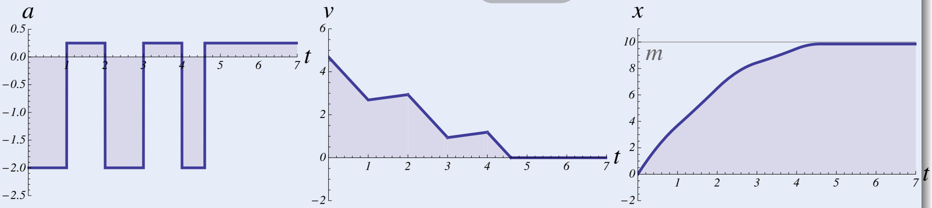
Concept (Differential Dynamic Logic) (JAR'08,LICS'12)



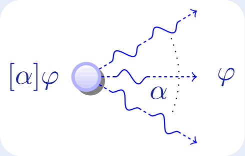


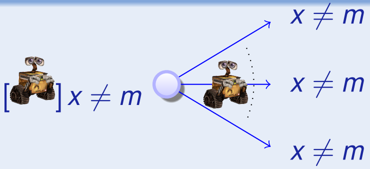
$$[((\text{if}(SB(x,m))\quad a := -b)\ ;\ x' = v, v' = a)^*]\underbrace{x \neq m}_{\text{post}}$$

all runs



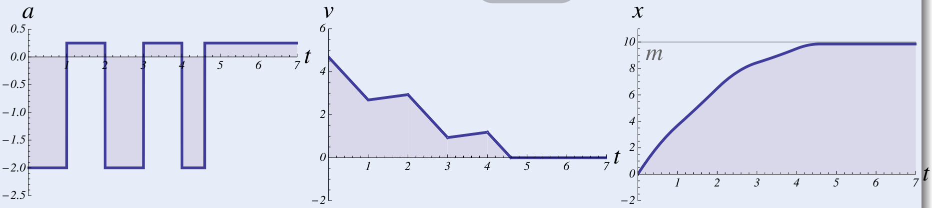
Concept (Differential Dynamic Logic) (JAR'08,LICS'12)



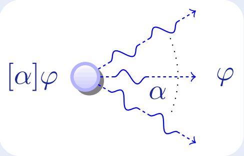


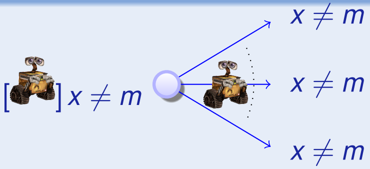
$$\underbrace{x \neq m \land b > 0}_{\text{init}} \rightarrow \Big[\big((\text{if}(\text{SB}(x,m))\quad a := -b)\ ;\ x' = v, v' = a\big)^*\Big]\underbrace{x \neq m}_{\text{post}}$$

all runs



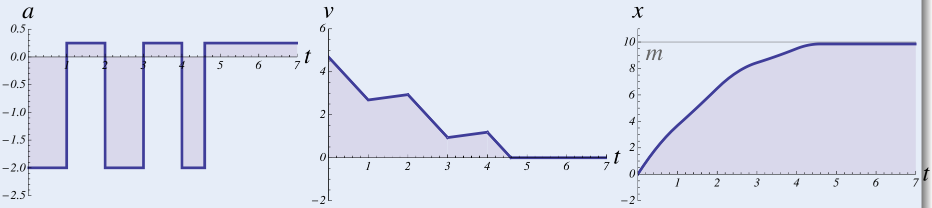
Concept (Differential Dynamic Logic) (JAR'08,LICS'12)



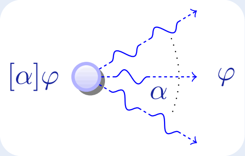


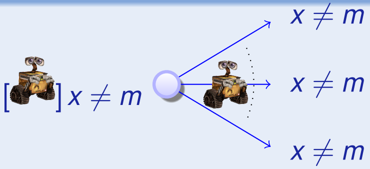
nondet. choice

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



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

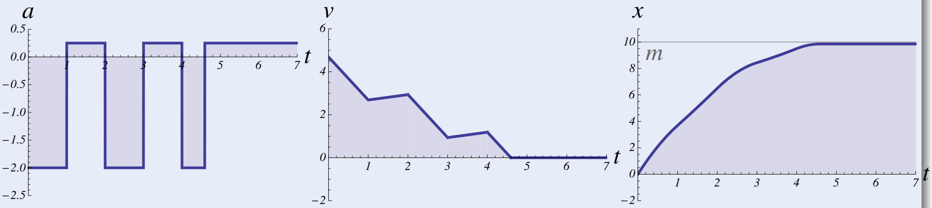




test

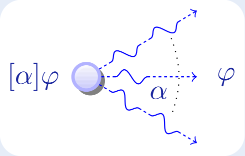
nondet. choice

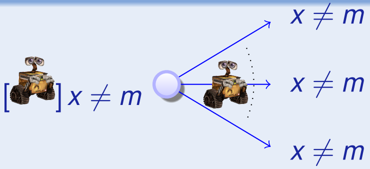
$$\underbrace{x \neq m \wedge b > 0}_{\text{init}} \rightarrow \left[\left((?\neg SB(x,m) \cup a := -b) \ ; \ x' = v, v' = a\right)^*\right] \underbrace{x \neq m}_{\text{post}}$$



CPS Analysis

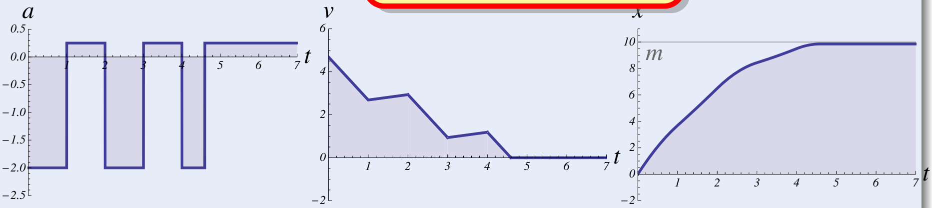
Concept (Differential Dynamic Logic) (JAR'08,LICS'12)





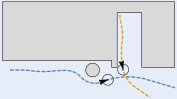
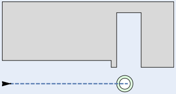
$$\underbrace{x \neq m \land b > 0}_{\text{init}} \rightarrow \Big[\big((?\neg \mathrm{SB}(x,m) \cup a := -b)\ ;\ x' = v, v' = a\big)^*\Big]\underbrace{x \neq m}_{\text{post}}$$

hybrid program dynamics

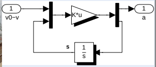


Application Highlights

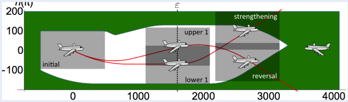
Obstacle Avoidance + Ground Navigation

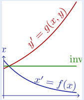
Train Control Brakes

Airborne Collision Avoidance (ACAS X)

Ship Cooling

NSF DARPA BOSCH SIEMENS JOHNS HOPKINS APPLIED PHYSICS LABORATORY

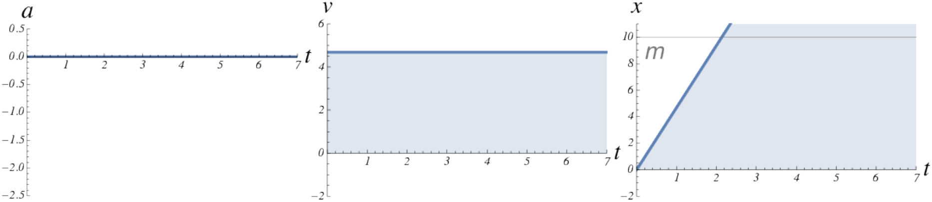
Outline (Modeling CPS)

Example (Speedy the point)

$$\{x' = v, v' = a\}$$

Purely continuous dynamics

What about the cyber?

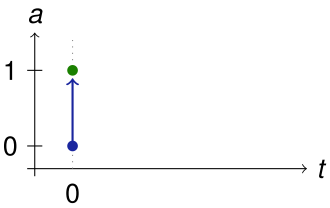


Example (Speedy the point)

$$a := a + 1$$

Purely discrete dynamics

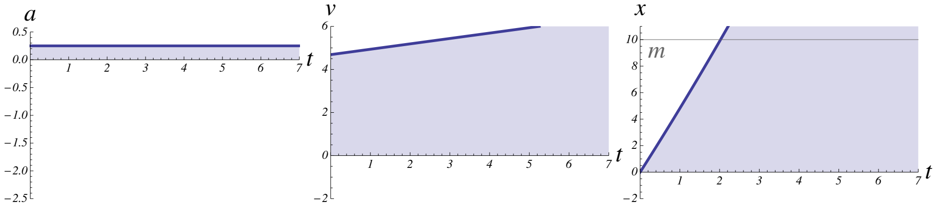
How do both meet?



Example (Speedy the point)

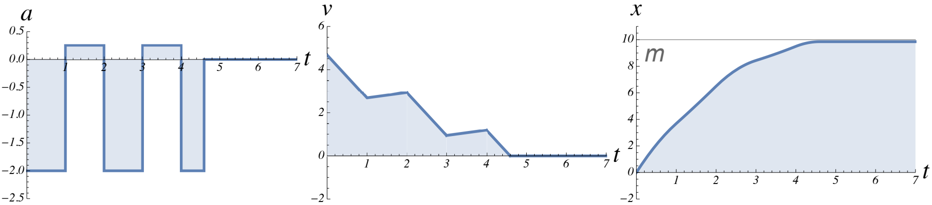
$$a := a + 1;\ \{x' = v, v' = a\}$$

Hybrid dynamics, i.e., composition of continuous and discrete dynamics
Here: sequential composition first;second



Example (Speedy the point)

$$\begin{aligned}
&a := -2; \quad \{x' = v, v' = a\};\\
&a := 0.25; \{x' = v, v' = a\};\\
&a := -2; \quad \{x' = v, v' = a\};\\
&a := 0.25; \{x' = v, v' = a\};\\
&a := -2; \quad \{x' = v, v' = a\};\\
&a := 0.25; \{x' = v, v' = a\}
\end{aligned}$$

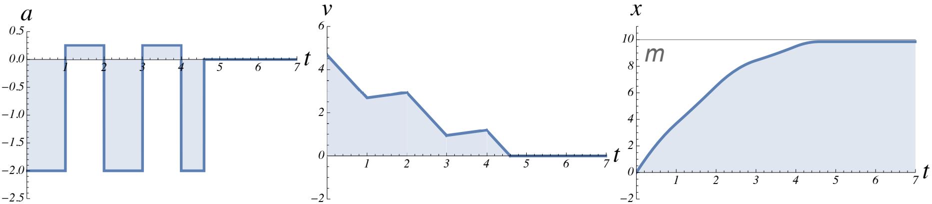


Playing with Acceleration and Braking

Example (Speedy the point)

$$a := -2;\ \{x' = v, v' = a\};$$
$$a := 0.25; \{x' = v, v' = a\};$$
$$a := -2;\ \{x' = v, v' = a\};$$
$$a := 0.25; \{x' = v, v' = a\};$$
$$a := -2;\ \{x' = v, v' = a\};$$
$$a := 0.25; \{x' = v, v' = a\}$$

How long to follow an ODE?

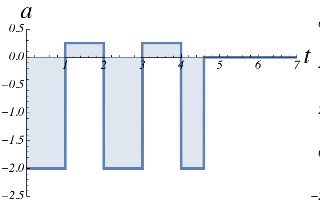


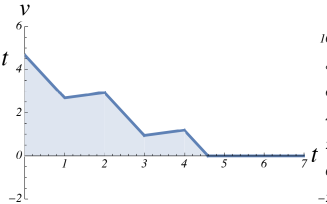
Playing with Acceleration and Braking

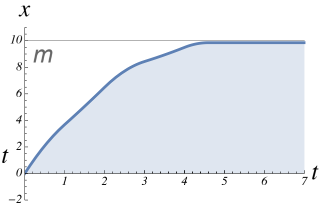
Example (Speedy the point)

$$
\begin{aligned}
&a := -2; \ \{x' = v, v' = a\};\\
&a := 0.25; \{x' = v, v' = a\};\\
&a := -2; \ \{x' = v, v' = a\};\\
&a := 0.25; \{x' = v, v' = a\};\\
&a := -2; \ \{x' = v, v' = a\};\\
&a := 0.25; \{x' = v, v' = a\}
\end{aligned}
$$

How to check conditions before actions?







Example (Speedy the point)

$$\text{if}(v < 4)\, a := a + 1 \text{ else } a := -b;$$
$$\{x' = v, v' = a\}$$

Velocity-dependent control

Example (Speedy the point)

$$\text{if}(x - m > s)\, a := a + 1 \,\text{else}\, a := -b;$$
$$\{x' = v, v' = a\}$$

Distance-dependent control for obstacle m

Example (Speedy the point)

$$\text{if}(x - m > s \land v < 4)\, a := a + 1 \,\text{else}\, a := -b;$$
$$\{x' = v, v' = a\}$$

Velocity and distance-dependent control

Iterative Design

Start as simple as possible, then add challenges once basics are correct.

Example (Speedy the point)

$$\text{if}(x - m > s \land v < 4 \land \text{efficiency})\, a := a + 1 \,\text{else}\, a := -b;$$
$$\{x' = v, v' = a\}$$

Also only accelerate if it's efficient to do so

Playing with Acceleration and Braking

Example (Speedy the point)

$$\text{if}(x - m > s \land v < 4 \land \text{efficiency})\, a := a + 1 \,\text{else}\, a := -b;$$
$$\{x' = v, v' = a\}$$

Exact models are unnecessarily complex. Not all features are safety-critical.

Playing with Acceleration and Braking

Example (Speedy the point)

$$(a := a + 1 \cup a := -b);$$
$$\{x' = v, v' = a\}$$

Nondeterministic choice $\cup$ allows either side to be run, arbitrarily

Power of Abstraction

Only include relevant aspects, elide irrelevant detail.
The model and its analysis become simpler. And apply to more systems.

Playing with Acceleration and Braking

Example (Speedy the point)

$$(a := a+1 \cup a := -b);$$
$$\{x' = v, v' = a\}$$

Nondeterministic choice $\cup$ allows either side to be run, arbitrarily

Oops, now it got too simple! Not every choice is always acceptable.

Playing with Acceleration and Braking

Example (Speedy the point)

$$(?v < 4; a := a + 1 \cup a := -b);$$
$$\{x' = v, v' = a\}$$

Test $?Q$ checks if formula Q is true in current state

Playing with Acceleration and Braking

Example (Speedy the point)

$$(?v < 4; a := a+1 \cup a := -b);$$
$$\{x' = v, v' = a\}$$

Test $?Q$ checks if formula Q is true in current state, otherwise run fails.

Discarding failed runs and backtracking

System runs that fail tests are discarded and not considered further.

$?v < 4;\ v := v+1$ only runs if
$v := v+1;\ ?v < 4$ only runs if

Broader significance of nondeterminism

Nondeterminism is a tool for abstraction to focus on critical aspects.
Nondeterminism is essential to describe imperfectly known environment.

Playing with Acceleration and Braking

Example (Speedy the point)

$$(?v < 4; a := a+1 \cup a := -b);$$
$$\{x' = v, v' = a\}$$

Test $?Q$ checks if formula Q is true in current state, otherwise run fails.

Discarding failed runs and backtracking

System runs that fail tests are discarded and not considered further.

$?v < 4;\ v := v+1$	only runs if $v < 4$ initially true
$v := v+1;\ ?v < 4$	only runs if $v < 3$ initially true

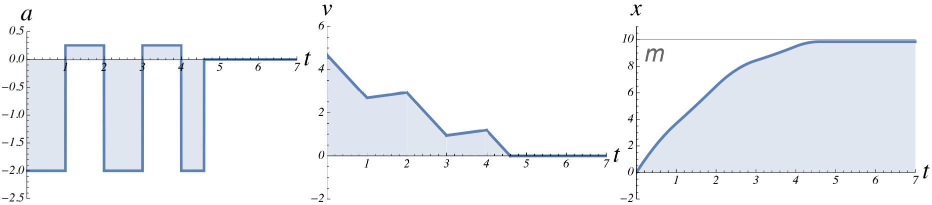
Broader significance of nondeterminism

Nondeterminism is a tool for abstraction to focus on critical aspects.
Nondeterminism is essential to describe imperfectly known environment.

Example (Speedy the point)

$$(?v < 4; a := a + 1 \cup a := -b);$$
$$\{x' = v, v' = a\};$$
$$(?v < 4; a := a + 1 \cup a := -b);$$
$$\{x' = v, v' = a\};$$
$$(?v < 4; a := a + 1 \cup a := -b);$$
$$\{x' = v, v' = a\}$$

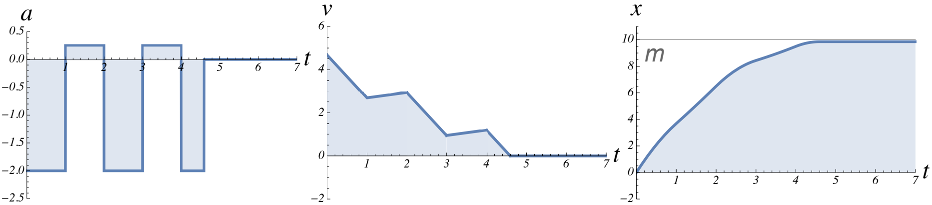
Repeated control needs longer programs, e.g., by copy&paste



Example (Speedy the point)

$$\big((?v < 4; a := a + 1 \cup a := -b);\ \{x' = v, v' = a\}\big)^*$$

Nondeterministic repetition * repeats *any* arbitrary number of times



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

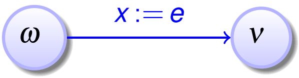
Hybrid Programs: Syntax

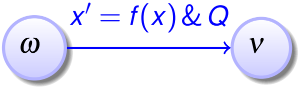
Definition (Syntax of hybrid program α)

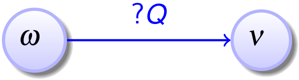
$$\alpha, \beta \ ::= \ x := e \mid ?Q \mid x' = f(x) \,\&\, Q \mid \alpha \cup \beta \mid \alpha ; \beta \mid \alpha^*$$

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

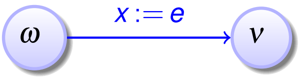
Like regular expressions. Everything nondeterministic

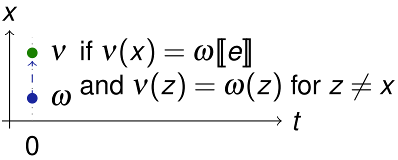

ω
$x := e$
ν

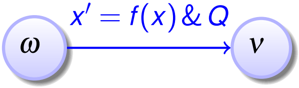

ω
$x' = f(x) \,\&\, Q$
ν

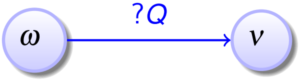

ω
$?Q$
ν

Hybrid Programs: Semantics

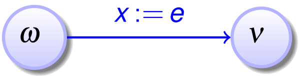


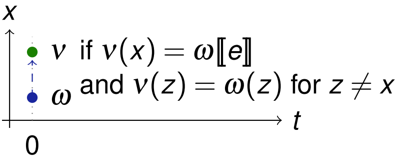


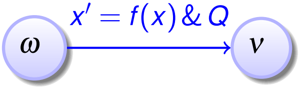


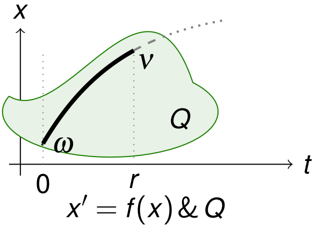


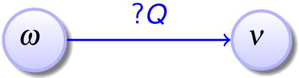
Hybrid Programs: Semantics



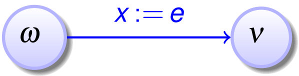


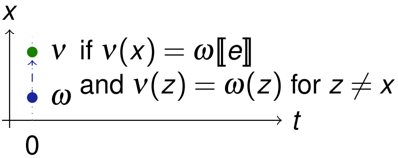


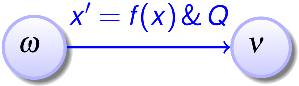


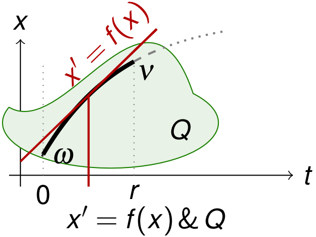


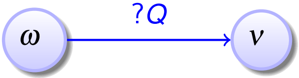
Hybrid Programs: Semantics



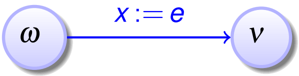


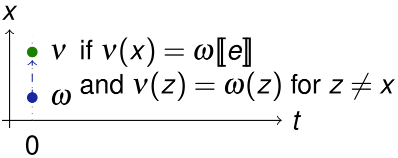


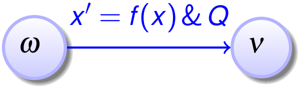


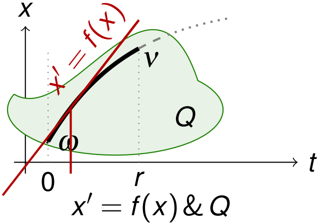


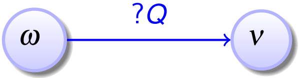
Hybrid Programs: Semantics



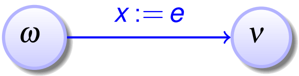


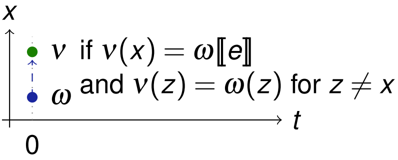


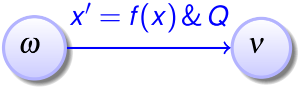


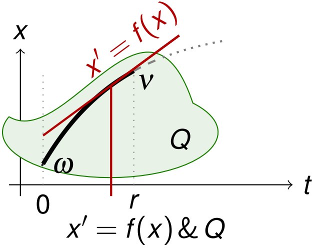


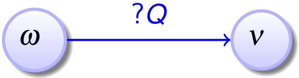
Hybrid Programs: Semantics

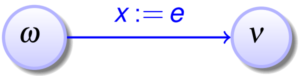


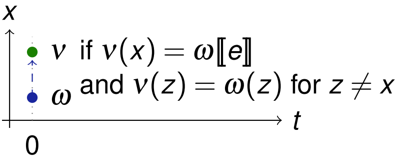


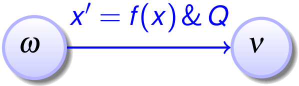


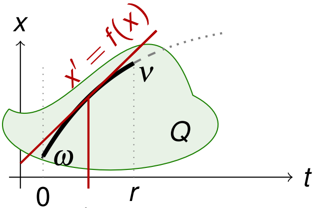




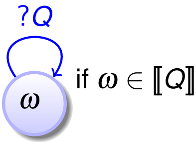

ω
$x := e$
ν

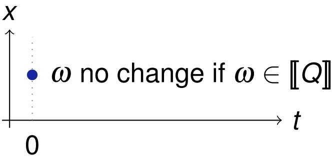

x
ν if $\nu(x) = \omega[\![e]\!]$
ω and $\nu(z) = \omega(z)$ for $z \neq x$
t
0


ω
$x' = f(x) \,\&\, Q$
ν

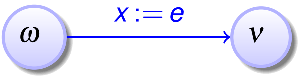

x
$x' = f(x)$
ν
Q
ω
t
0
r

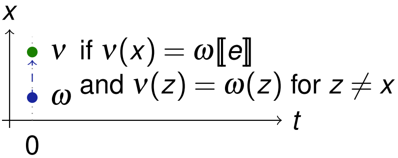
$x' = f(x) \,\&\, Q$

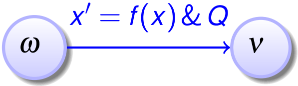

$?Q$
ω
if $\omega \in [\![Q]\!]$

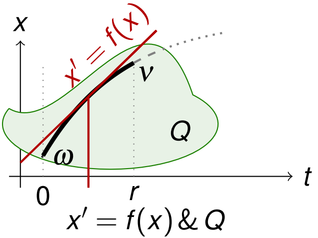

x
ω no change if $\omega \in [\![Q]\!]$
t
0

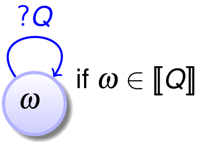
Hybrid Programs: Semantics

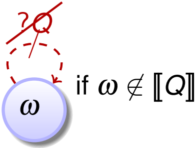


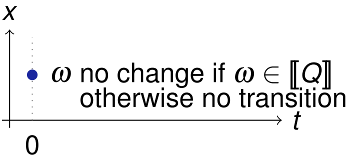




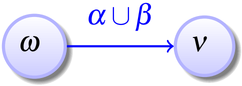


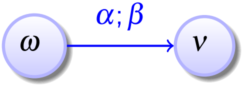


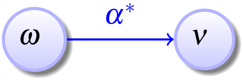


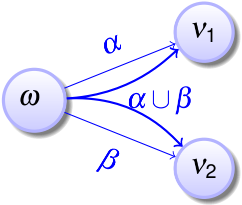


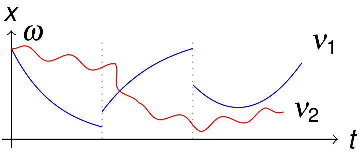
Hybrid Programs: Semantics

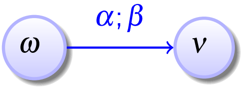


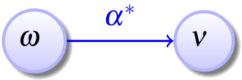


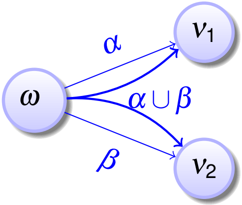



α
ω
v_1
α ∪ β
β
v_2

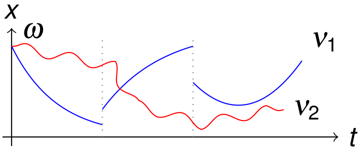

x
ω
v_1
v_2
t


ω
α; β
ν

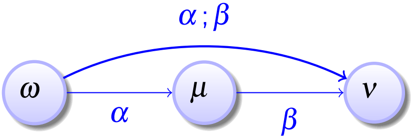

ω
α*
ν



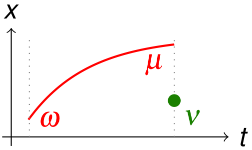
α
ν_1
ω
$\alpha \cup \beta$
β
ν_2



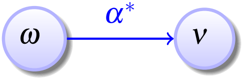
x
ω
ν_1
ν_2
t



$\alpha ; \beta$
ω
μ
ν
α
β

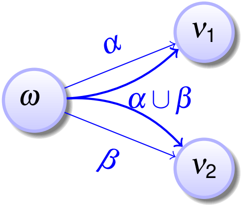


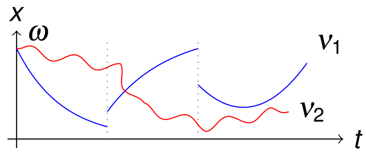
x
μ
ω
ν
t

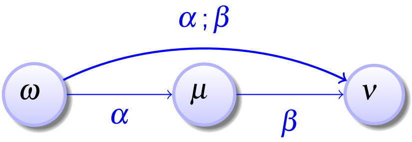


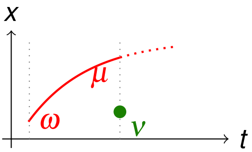
α^*
ω
ν

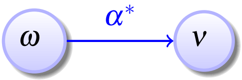
Hybrid Programs: Semantics



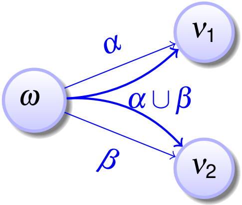


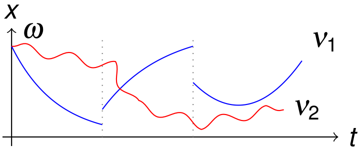


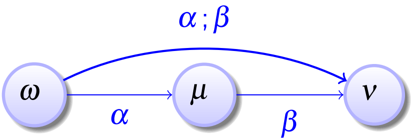


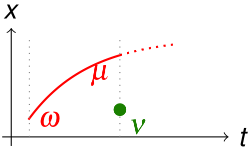


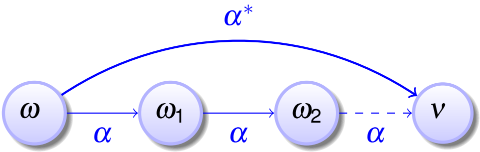
Hybrid Programs: Semantics

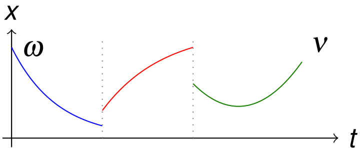




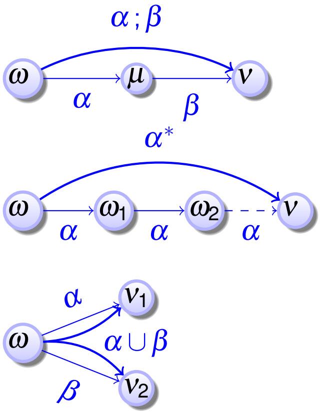




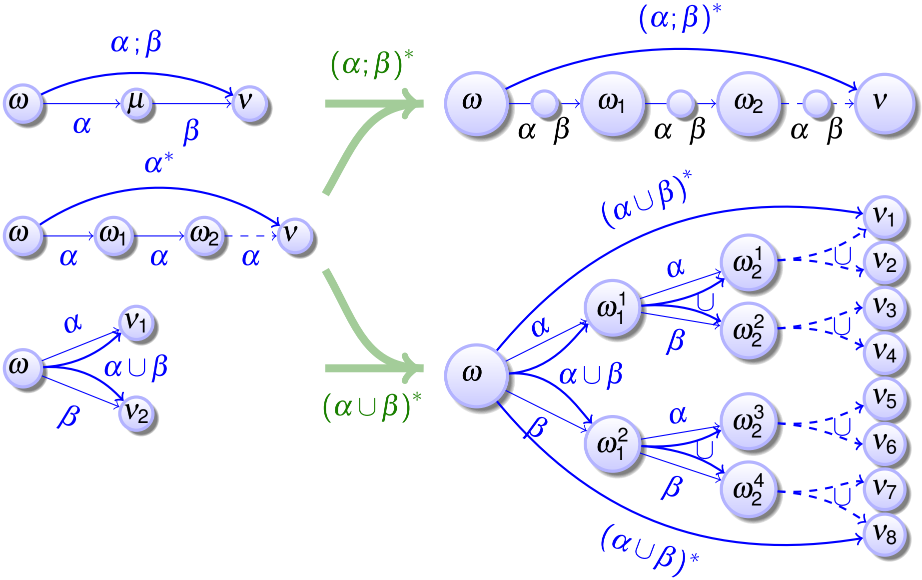




Plug-in for Semantics of Composed Hybrid Programs



Plug-in for Semantics of Composed Hybrid Programs



Hybrid Programs: Syntax & Semantics

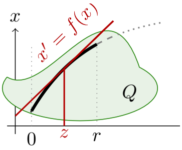
Definition (Syntax of hybrid program α)

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

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

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

compositional



Hybrid Programs: Syntax & Semantics

Definition (Syntax of hybrid program α)

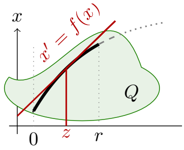
$$\alpha, \beta \ ::= \ x := e \mid ?Q \mid x' = f(x) \,\&\, Q \mid \alpha \cup \beta \mid \alpha; \beta \mid \alpha^*$$

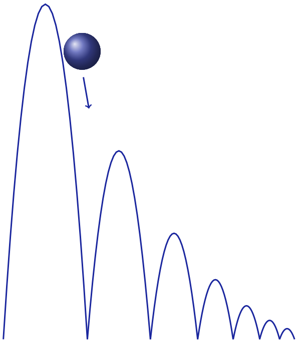
Definition (Semantics of hybrid programs) $(\llbracket\cdot\rrbracket : \mathrm{HP} \to \wp(\mathcal{S} \times \mathcal{S}))$

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

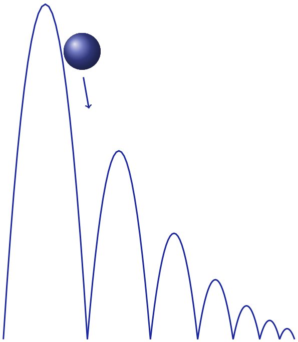
compositional

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





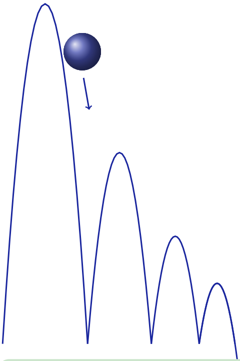
Example (Quantum the Bouncing Ball)



Example (Quantum the Bouncing Ball)

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

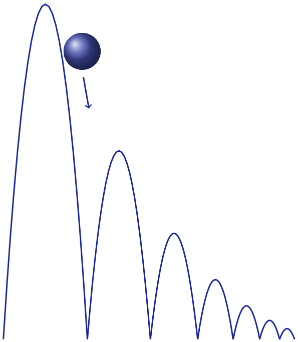
Quantum the Acrophobic Bouncing Ball



Example (Quantum the Bouncing Ball)

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

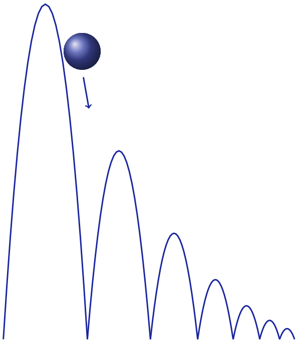
Quantum the Acrophobic Bouncing Ball



Example (Quantum the Bouncing Ball)

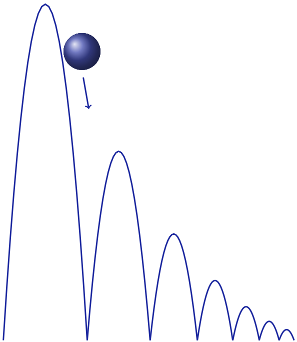
$$\{x' = v, v' = -g \,\&\, x \geq 0\}$$

Quantum the Acrophobic Bouncing Ball



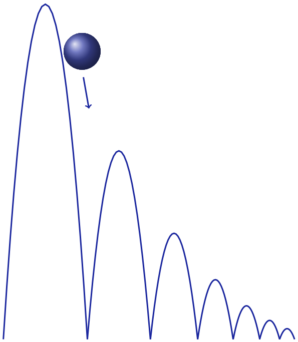
Example (Quantum the Bouncing Ball)

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



Example (Quantum the Bouncing Ball)

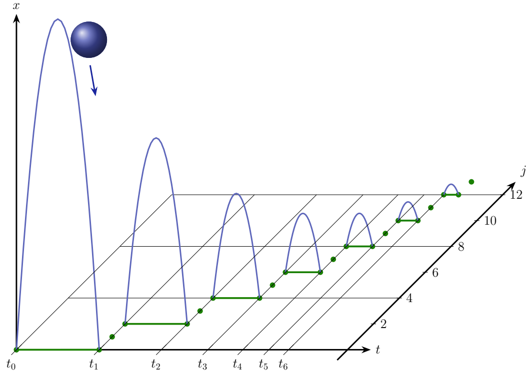
$$\big(\{x' = v, v' = -g \,\&\, x \geq 0\};$$
$$\text{if}(x = 0)\ \ v := -cv\big)^*$$



Example (Quantum the Bouncing Ball)

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

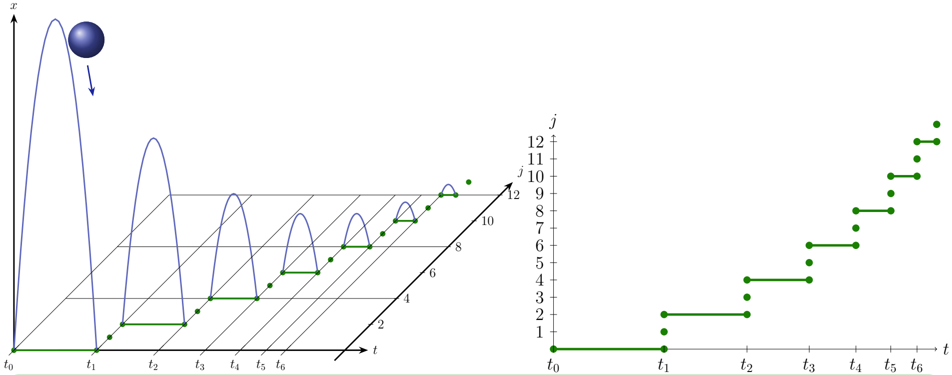
Quantum Discovered a Crack in the Fabric of Time



Example (Quantum the Bouncing Ball)

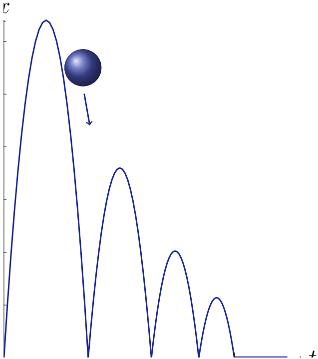
$$\big(\{x' = v, v' = -g \,\&\, x \geq 0\};$$
$$\text{if}(x = 0)\ \ v := -cv\big)^*$$

Quantum Discovered a Crack in the Fabric of Time



Example (Quantum the Bouncing Ball)

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

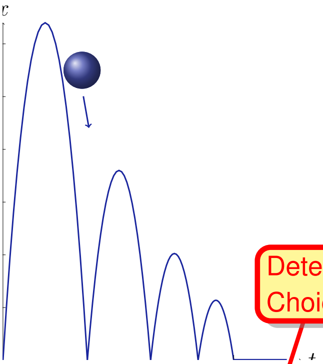


$\text{if}(Q)\,\alpha\,\text{else}\,\beta \equiv$

Example (Quantum the Bouncing Ball)

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

Quantum Learns to Deflate



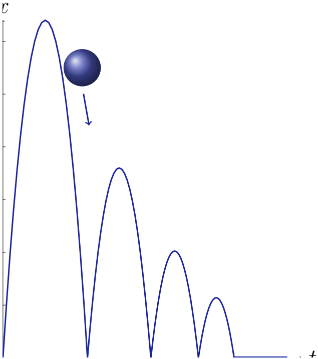
$$\text{if}(Q)\,\alpha\,\text{else}\,\beta \equiv (?Q;\alpha) \cup (?\neg Q;\beta)$$

Determ. Choice

Nondet. Choice

Example (Quantum the Bouncing Ball)

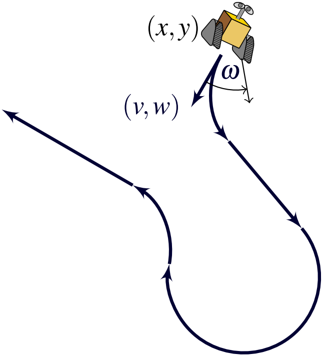
$$\big(\{x' = v, v' = -g \,\&\, x \geq 0\};$$
$$\text{if}(x = 0)\,(v := -cv \cup v := 0)\big)^*$$

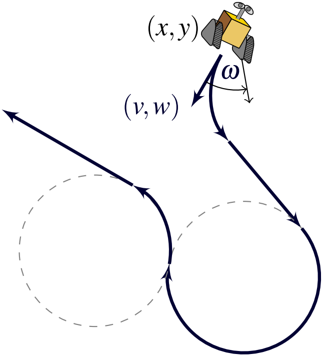


Nondet. Assign

Example (Quantum the Bouncing Ball)

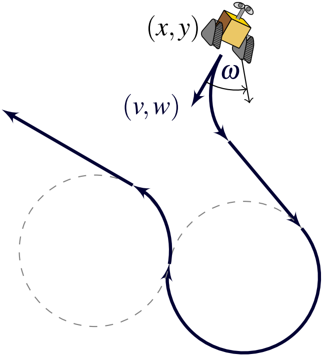
$$\big(\{x' = v, v' = -g \,\&\, x \geq 0\};\\ \text{if}(x = 0)\,(c := *; ?c \geq 0; v := -cv)\big)^*$$


(x, y)
ω
(v, w)



Example (Runaround Robot)

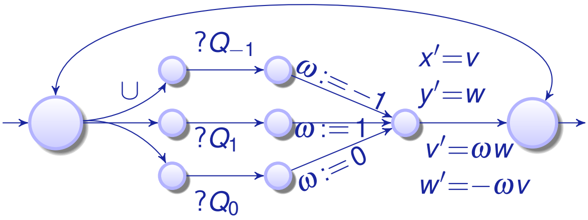
$$\Big((\omega := -1 \cup \omega := 1 \cup \omega := 0);$$
$$\{x' = v, y' = w, v' = \omega w, w' = -\omega v\}\Big)^*$$

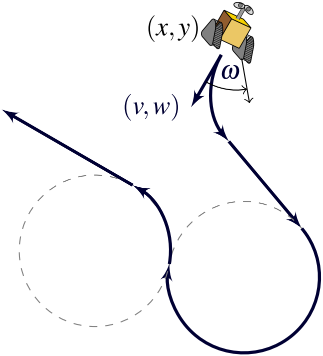


Example (Runaround Robot)

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

Runaround Robot with Dubins Paths

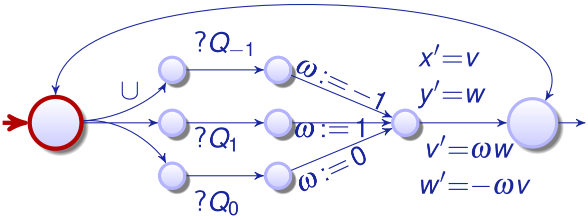


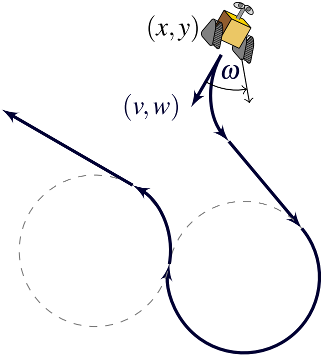


Example (Runaround Robot)

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

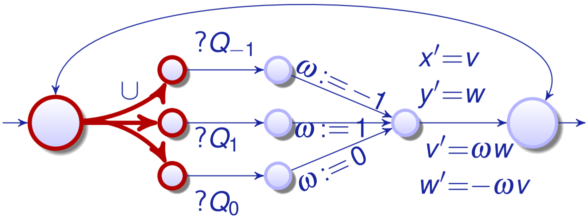
Runaround Robot with Dubins Paths

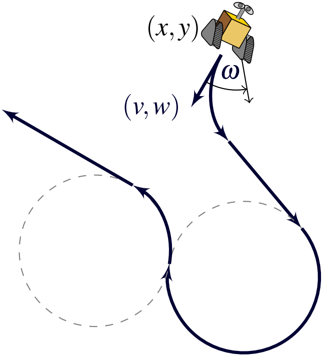




Example (Runaround Robot)

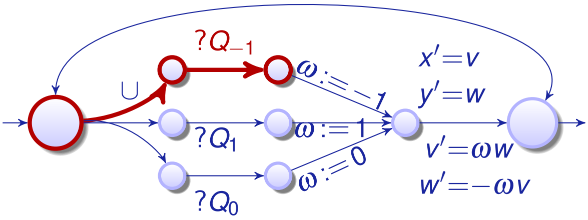
$$\Big((?Q_{-1}; \omega := -1 \cup ?Q_1; \omega := 1 \cup ?Q_0; \omega := 0);$$
$$\{x' = v, y' = w, v' = \omega w, w' = -\omega v\}\Big)^*$$

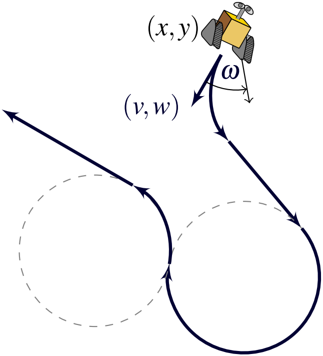




Example (Runaround Robot)

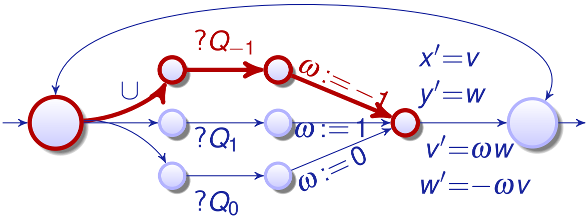
$$\big((?Q_{-1};\omega:=-1 \cup ?Q_1;\omega:=1 \cup ?Q_0;\omega:=0);$$
$$\{x'=v, y'=w, v'=\omega w, w'=-\omega v\}\big)^*$$

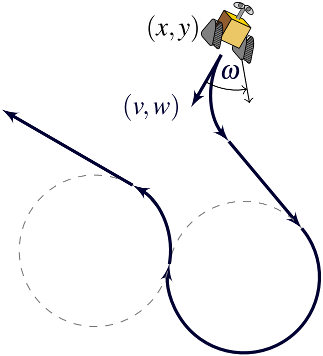




Example (Runaround Robot)

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

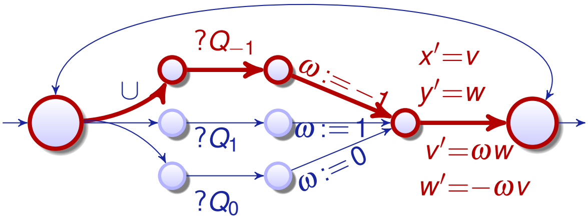


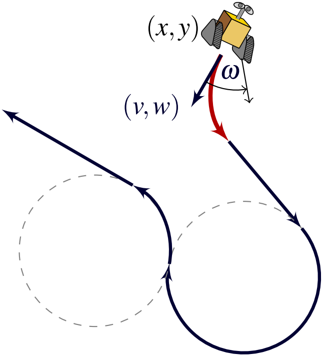


Example (Runaround Robot)

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

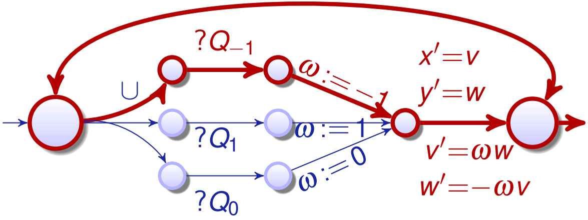
Runaround Robot with Dubins Paths

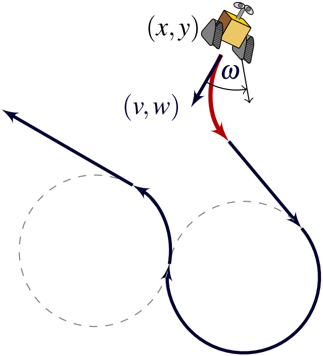




Example (Runaround Robot)

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

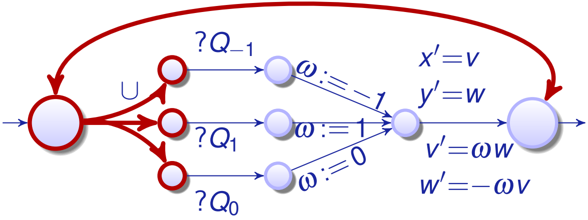


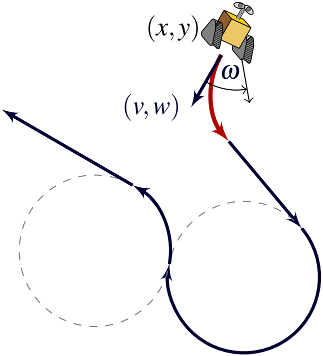


Example (Runaround Robot)

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

Runaround Robot with Dubins Paths

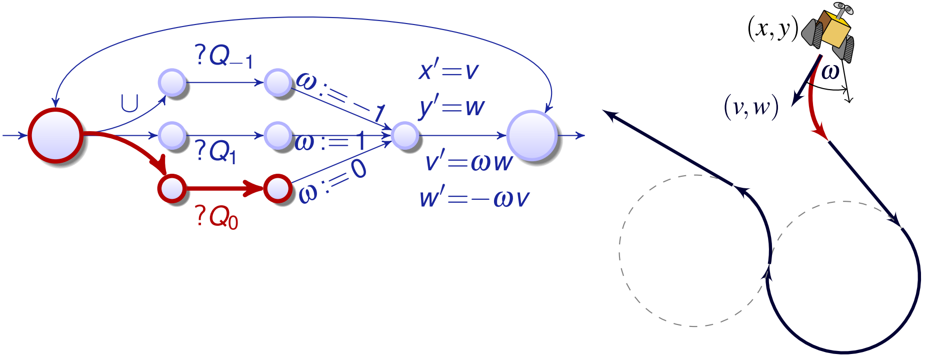




Example (Runaround Robot)

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

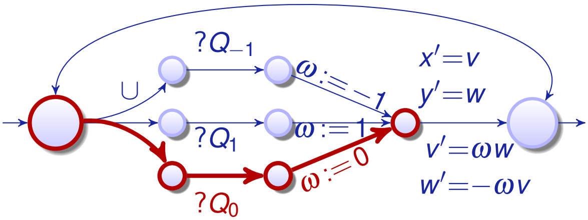
Runaround Robot with Dubins Paths

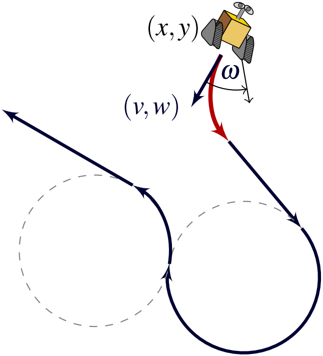


Example (Runaround Robot)

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

Runaround Robot with Dubins Paths

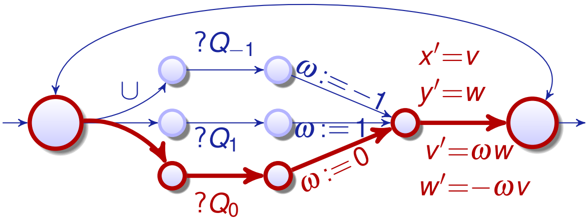


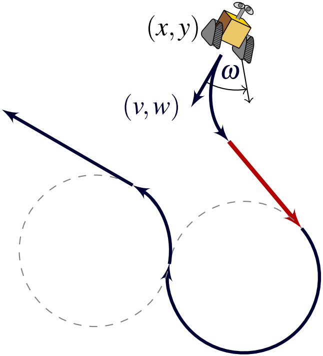


Example (Runaround Robot)

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

Runaround Robot with Dubins Paths

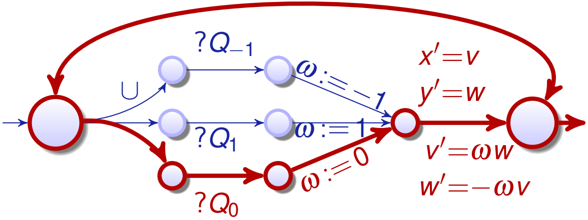


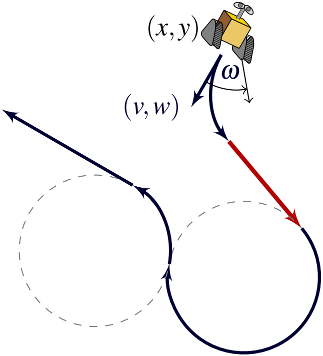


Example (Runaround Robot)

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

Runaround Robot with Dubins Paths

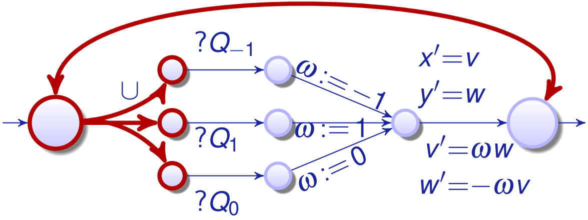


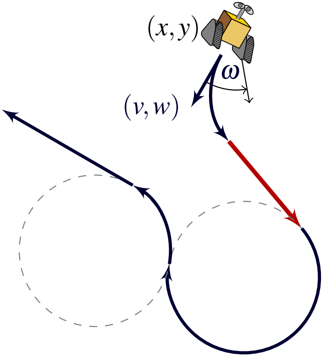


Example (Runaround Robot)

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

Runaround Robot with Dubins Paths

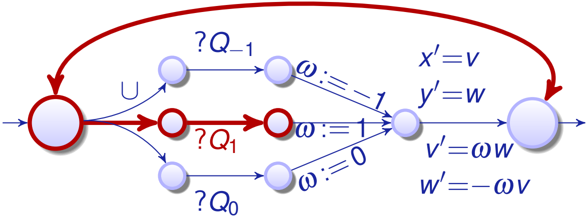


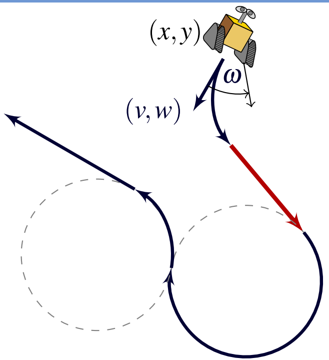


Example (Runaround Robot)

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

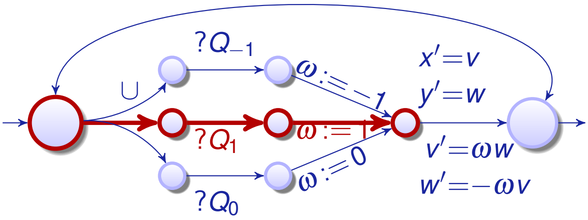
Runaround Robot with Dubins Paths

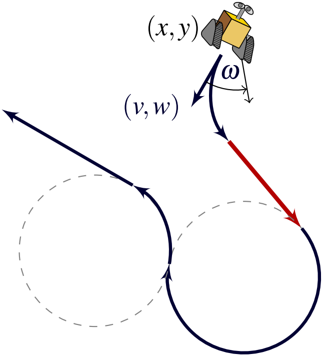




Example (Runaround Robot)

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

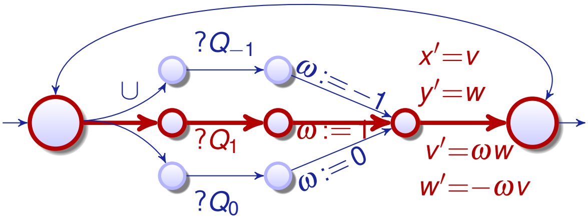


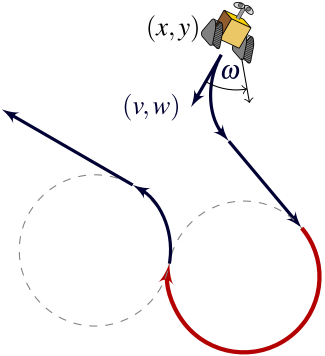


Example (Runaround Robot)

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

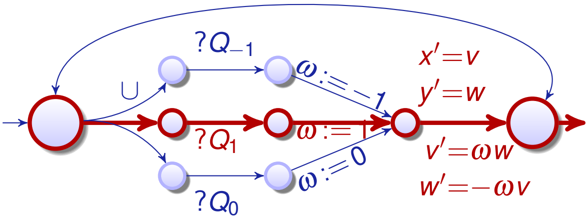
Runaround Robot with Dubins Paths

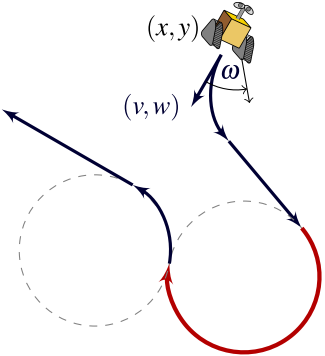




Example (Runaround Robot)

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





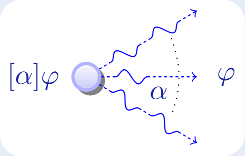
Example (Runaround Robot)

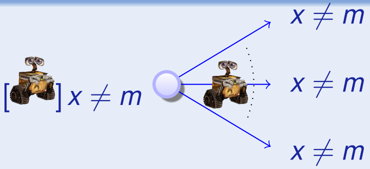
$$\big((?Q_{-1}; \omega := -1 \cup ?Q_1; \omega := 1 \cup ?Q_0; \omega := 0);$$
$$\{x' = v, y' = w, v' = \omega w, w' = -\omega v\}\big)^*$$

Outline (Specifying CPS)

CPS Analysis

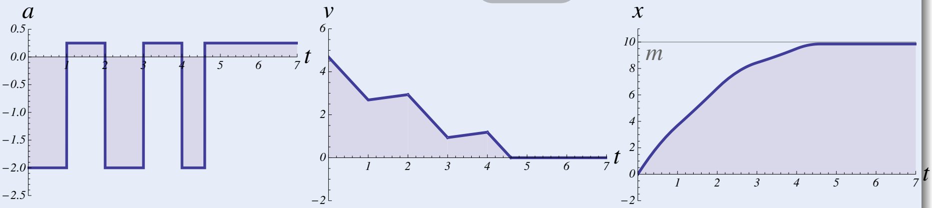
Concept (Differential Dynamic Logic) (JAR'08,LICS'12)



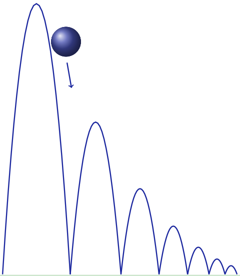


$$\underbrace{x \neq m \land b > 0}_{\text{init}} \rightarrow \Big[\big((\text{if}(\text{SB}(x,m)) \quad a := -b)\ ;\ x' = v, v' = a\big)^*\Big]\underbrace{x \neq m}_{\text{post}}$$

all runs

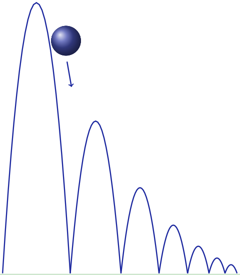


Contracts for Quantum the Acrophobic Bouncing Ball



Example (Quantum the Bouncing Ball)

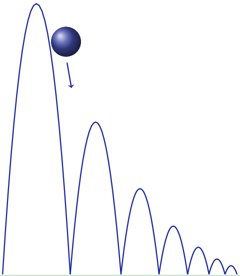
$$\big(\{x' = v, v' = -g \,\&\, x \geq 0\};$$
$$\text{if}(x = 0)\, v := -cv\big)^*$$



Example (Quantum the Bouncing Ball)

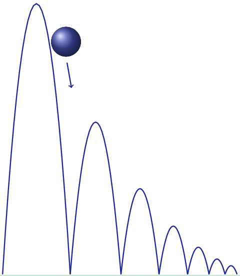
$\mathbf{ensures}(0 \leq x)$

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



Example (Quantum the Bouncing Ball)

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



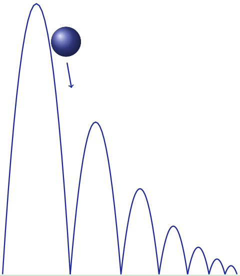
Example (Quantum the Bouncing Ball)

$\textbf{requires}(x = H)$

$\textbf{ensures}(0 \leq x)$

$\textbf{ensures}(x \leq H)$

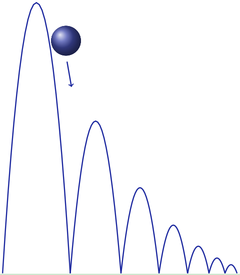
$$\big(\{x' = v, v' = -g \,\&\, x \geq 0\};$$
$$\text{if}(x = 0)\, v := -cv\big)^*$$



Example (Quantum the Bouncing Ball)

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

Contracts for Quantum the Acrophobic Bouncing Ball



Example (Quantum the Bouncing Ball)

$\textbf{requires}(x = H)$

$\textbf{requires}(0 \leq H)$

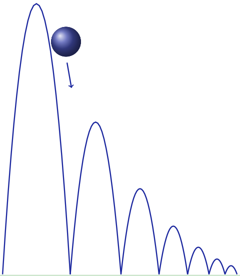
$\textbf{ensures}(0 \leq x)$

$\textbf{ensures}(x \leq H)$

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

$\text{if}(x = 0)\, v := -cv\big)^{*} \textbf{@invariant}(x \geq 0)$

Contracts for Quantum the Acrophobic Bouncing Ball



Example (Quantum the Bouncing Ball)

$$\textbf{requires}(x = H)$$
$$\textbf{requires}(0 \le H)$$
$$\textbf{ensures}(0 \le x)$$
$$\textbf{ensures}(x \le H)$$
$$\big(\{x' = v, v' = -g \,\&\, x \ge 0\};$$
$$\text{if}(x = 0)\, v := -cv\big)^* \textbf{@invariant}(x \ge 0)$$

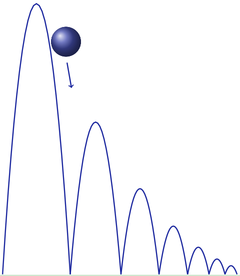
Contracts are Not Enough

CPS contracts are crucial for CPS safety.
We need to understand CPS programs and contracts and how we can convince ourselves that a CPS program respects its contract.

Contracts are at a disadvantage compared to full logic.

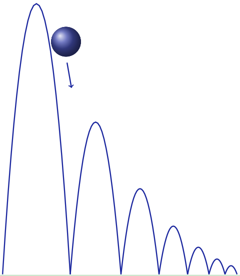
Logic is for Specification and Reasoning

1. Specification of a whole CPS program.
2. Analytic inspection of its parts.
3. Argumentative relations between contracts and program parts.
   "Yes, this CPS program meets its contract, and here's why ..."



Example (Quantum the Bouncing Ball)

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



Example (Quantum the Bouncing Ball)

requires$(x = H)$

requires$(0 \leq H)$

ensures$(0 \leq x)$

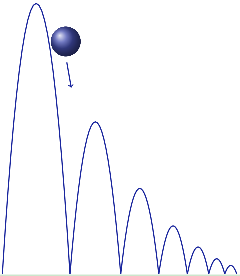
ensures$(x \leq H)$

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

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

Precondition:

$x = H \land 0 \leq H$ in FOL



Example (Quantum the Bouncing Ball)

requires$(x = H)$

requires$(0 \le H)$

ensures$(0 \le x)$

ensures$(x \le H)$

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

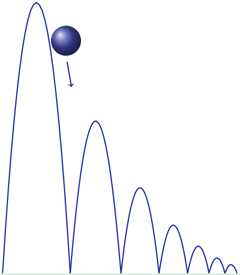
$\text{if}(x = 0)\, v := -cv)^*$

Precondition:

$x = H \land 0 \le H$ in FOL

Postcondition:

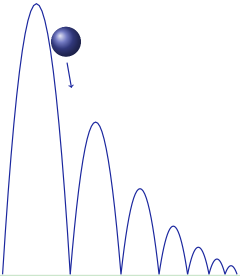
$0 \le x \land x \le H$ in FOL

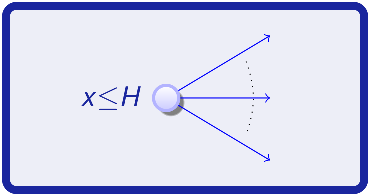


Example (Quantum the Bouncing Ball)

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

Precondition:
$x = H \land 0 \leq H$ in FOL
Postcondition:
$0 \leq x \land x \leq H$ in FOL
How to say post is true
after all HP runs?





Example (Quantum the Bouncing Ball)

requires$(x = H)$

requires$(0 \leq H)$

ensures$(0 \leq x)$

ensures$(x \leq H)$

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

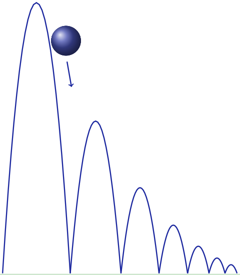
$\;\text{if}(x = 0)\, v := -cv\big)^*$

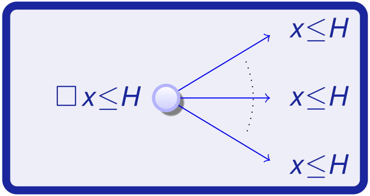
Precondition:

$x = H \land 0 \leq H$ in FOL

Postcondition:

$0 \leq x \land x \leq H$ in FOL

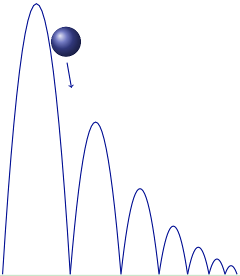


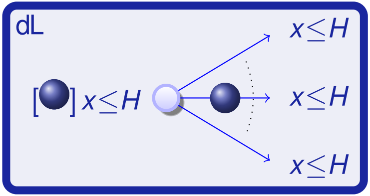


Example (Quantum the Bouncing Ball)

requires$(x = H)$
requires$(0 \le H)$
ensures$(0 \le x)$
ensures$(x \le H)$
$(\{x' = v, v' = -g \,\&\, x \ge 0\};$
$\text{if}(x = 0)\, v := -cv)^*$

Precondition:
$x = H \land 0 \le H$ in FOL
Postcondition:
$0 \le x \land x \le H$ in FOL

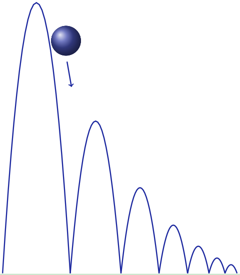


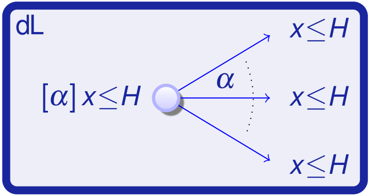


Example (Quantum the Bouncing Ball)

requires$(x = H)$
requires$(0 \le H)$
ensures$(0 \le x)$
ensures$(x \le H)$
$\big(\{x' = v, v' = -g \,\&\, x \ge 0\};$
$\text{if}(x = 0)\, v := -cv\big)^*$

Precondition:
$x = H \wedge 0 \le H$ in FOL
Postcondition:
$0 \le x \wedge x \le H$ in FOL





Example (Quantum the Bouncing Ball)

requires$(x = H)$	Precondition:
requires$(0 \leq H)$	$x = H \land 0 \leq H$ in FOL
ensures$(0 \leq x)$	Postcondition:
ensures$(x \leq H)$	$0 \leq x \land x \leq H$ in FOL

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

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

Example (Quantum the Bouncing Ball)

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

→ Precondition:
$x = H \land 0 \leq H$ in FOL

→ Postcondition:
$0 \leq x \land x \leq H$ in FOL

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

Example (Quantum the Bouncing Ball)

requires$(x = H)$

requires$(0 \leq H)$

ensures$(0 \leq x)$

ensures$(x \leq H)$

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

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

Precondition:

$x = H \wedge 0 \leq H$ in FOL

Postcondition:

$0 \leq x \wedge x \leq H$ in FOL

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

Example (Quantum the Bouncing Ball)

requires$(x = H)$

requires$(0 \leq H)$

ensures$(0 \leq x)$

ensures$(x \leq H)$

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

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

Precondition:

$x = H \land 0 \leq H$ in FOL

Postcondition:

$0 \leq x \land x \leq H$ in FOL

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

Example (Quantum the Bouncing Ball)

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

→ Precondition:
$x = H \land 0 \leq H$ in FOL

→ Postcondition:
$0 \leq x \land x \leq H$ in FOL

Contracts for Quantum the Acrophobic Bouncing Ball

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

Example (Quantum the Bouncing Ball)

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

Precondition:
$x = H \land 0 \leq H$ in FOL
Postcondition:
$0 \leq x \land x \leq H$ in FOL

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

Example (Quantum the Bouncing Ball)

requires$(x = H)$

requires$(0 \leq H)$

ensures$(0 \leq x)$

ensures$(x \leq H)$

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

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

Precondition:

$x = H \land 0 \leq H$ in FOL

Postcondition:

$0 \leq x \land x \leq H$ in FOL

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

Example (Quantum the Bouncing Ball)

requires$(x = H)$	→	Precondition:
requires$(0 \leq H)$		$x = H \land 0 \leq H$ in FOL
ensures$(0 \leq x)$	→	Postcondition:
ensures$(x \leq H)$		$0 \leq x \land x \leq H$ in FOL

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

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

Contracts for Quantum the Acrophobic Bouncing Ball

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

Example (Quantum the Bouncing Ball)

requires$(x = H)$

requires$(0 \leq H)$

ensures$(0 \leq x)$

ensures$(x \leq H)$

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

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

Precondition:

$x = H \land 0 \leq H$ in FOL

Postcondition:

$0 \leq x \land x \leq H$ in FOL

Differential Dynamic Logic: Syntax

Definition (Syntax of differential dynamic logic)

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

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

Differential Dynamic Logic: Syntax

Definition (Syntax of differential dynamic logic)

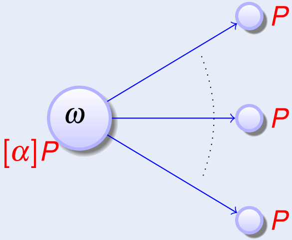
The *formulas* of *differential dynamic logic* are defined by the grammar:

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

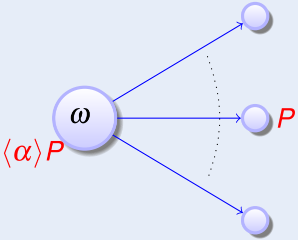
Not | And | Or | Imply | All reals | Some real | All runs | Some runs

Differential Dynamic Logic dL: Semantics

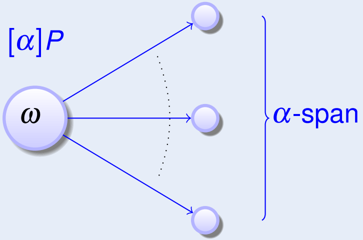
Definition (dL Formulas)



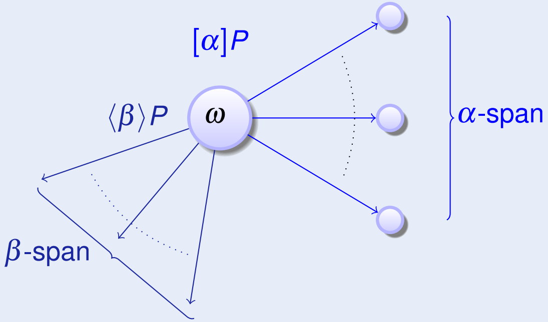
Definition (dL Formulas)



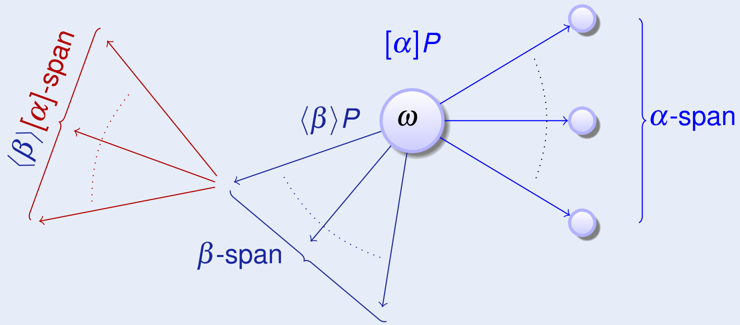
Definition (dL Formulas)



Definition (dL Formulas)



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:

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

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

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

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

$[\![P]\!]$	the set of states in which formula P is true
$\omega \in [\![P]\!]$	formula P is true in state ω, alias $\omega \models P$
$\models P$	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 $\quad [x:=x+1;x'=d]x\geq 0$ and $\quad \langle x'=d\rangle x\geq 0$

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

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

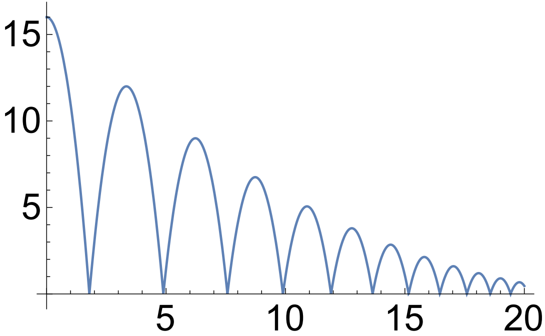
Differential Dynamic Logic: Syntax & Semantics

$[\![P]\!]$	the set of states in which formula P is true
$\omega \in [\![P]\!]$	formula P is true in state ω, alias $\omega \models P$
$\models P$	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 $\not\models \langle x'=d\rangle x\geq 0$

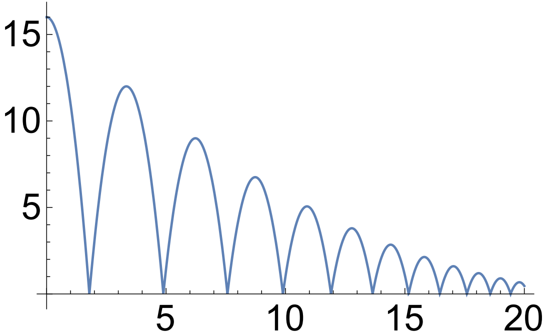
Definition (dL semantics) $([\![\cdot]\!] : \mathrm{Fml} \to \wp(\mathscr{S}))$

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



Example (Bouncing Ball)

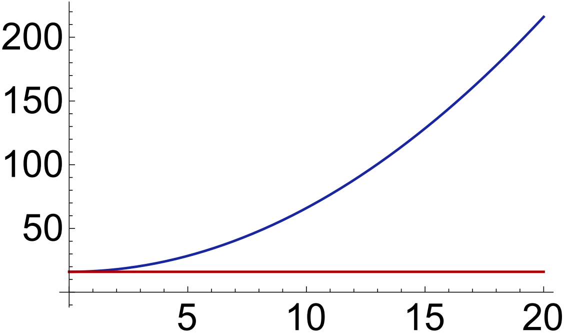
$$\big(\{x' = v, v' = -g \,\&\, x \geq 0\};$$
$$\text{if}(x = 0)\, v := -cv\big)^*$$



Example (Bouncing Ball)

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

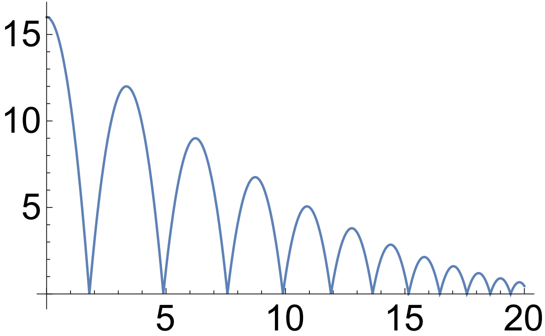
Quantum the Acrophobic Bouncing Ball



Not if $g < 0$ in anti-gravity

Example (Bouncing Ball)

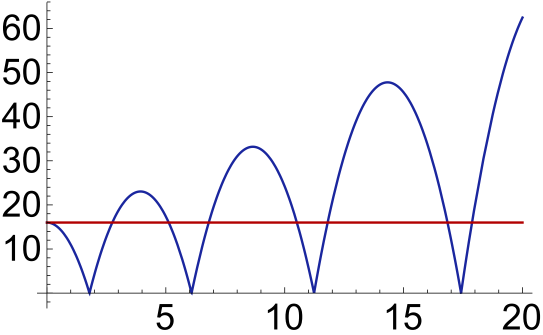
$$H=x\geq 0 \rightarrow [(\{x'=v, v'=-g \,\&\, x\geq 0\}; \text{if}(x=0)\, v:=-cv)^*]\, 0\leq x\leq H$$



Example (Bouncing Ball)

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

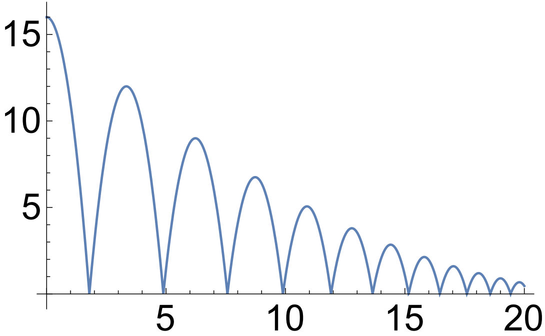
Quantum the Acrophobic Bouncing Ball



Not if $c > 1$ for anti-damping

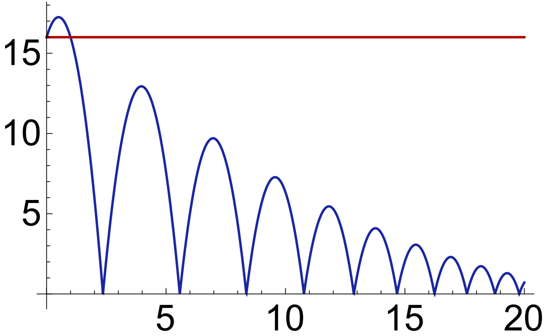
Example (Bouncing Ball)

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



Example (Bouncing Ball)

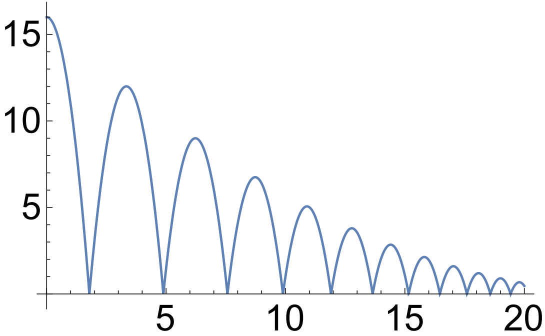
$$1 \geq c \geq 0 \land H = x \geq 0 \land g > 0 \to \left[\left(\{x' = v, v' = -g \,\&\, x \geq 0\};\right.\right.$$
$$\left.\left.\text{if}(x = 0)\, v := -cv\right)^*\right] 0 \leq x \leq H$$



Not if $v > 0$ initial climbing

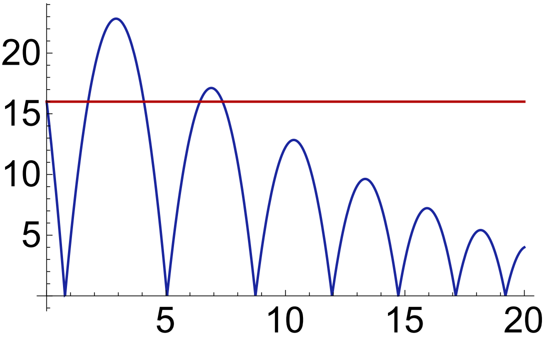
Example (Bouncing Ball)

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



Example (Bouncing Ball)

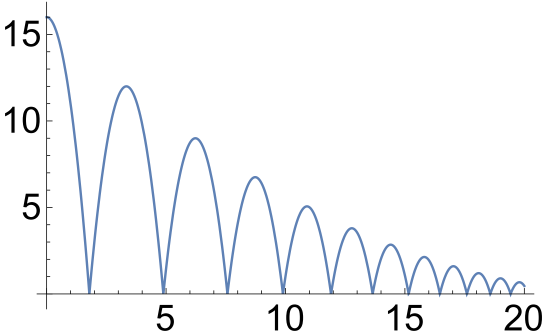
$$v\leq 0 \land 1\geq c\geq 0 \land H=x\geq 0 \land g>0 \rightarrow \left[\left(\{x'=v, v'=-g \,\&\, x\geq 0\};\right.\right.$$
$$\left.\left.\text{if}(x=0)\, v:=-cv\right)^*\right] 0\leq x\leq H$$



Not if $v \ll 0$ initial dribbling

Example (Bouncing Ball)

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



Example (Bouncing Ball)

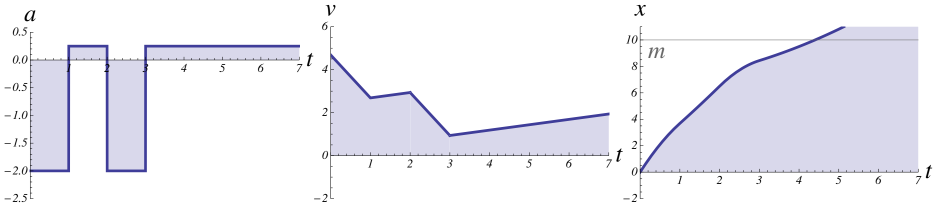
$$v{=}0 \land 1{\geq}c{\geq}0 \land H{=}x{\geq}0 \land g{>}0 \rightarrow \Big[\big(\{x' = v, v' = -g \,\&\, x \geq 0\};\\ \text{if}(x = 0)\, v := -cv\big)^*\Big]\, 0{\leq}x{\leq}H$$

Ex: Car Control Programs

Repeat control decisions

Example (Single car car_s)

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

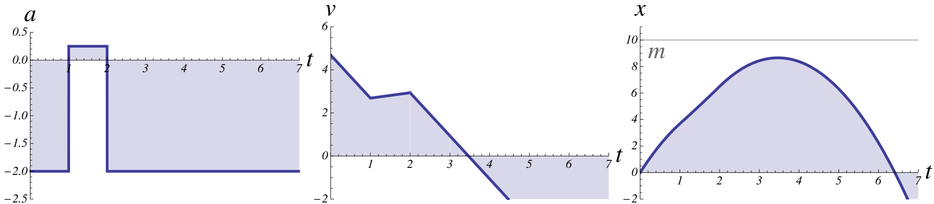


Ex: Car Control Programs

How does this model brake?

Example (Single car car_s)

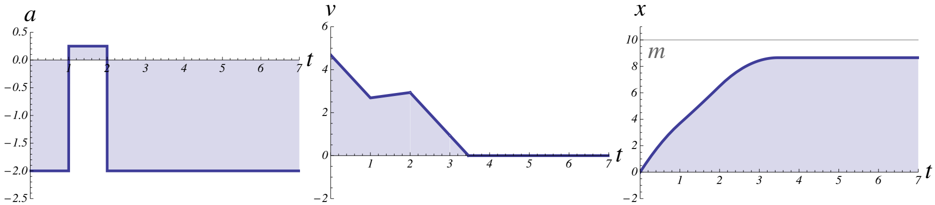
$$\big((\ a:=A\ \cup a:=-b);\ \{x'=v, v'=a\}\big)^*$$



Velocity bound $v \geq 0$ in evolution domain

Example (Single car car_s)

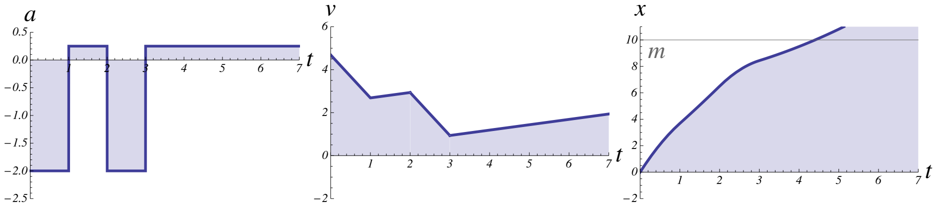
$$\big((a := A \cup a := -b);\ \{x' = v, v' = a \,\&\, v \geq 0\}\big)^*$$



Acceleration not always safe

Example (Single car car_s)

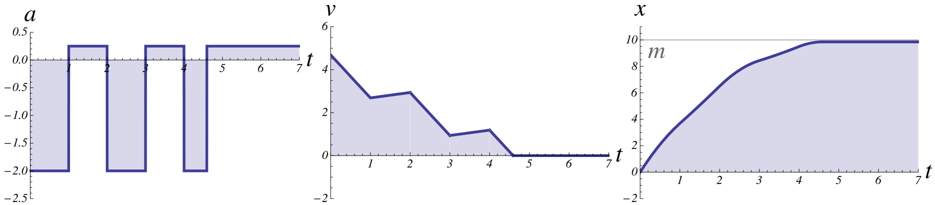
$$\big((\color{red}{a := A} \cup a := -b);\ \{x' = v, v' = a \,\&\, v \geq 0\}\big)^*$$



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

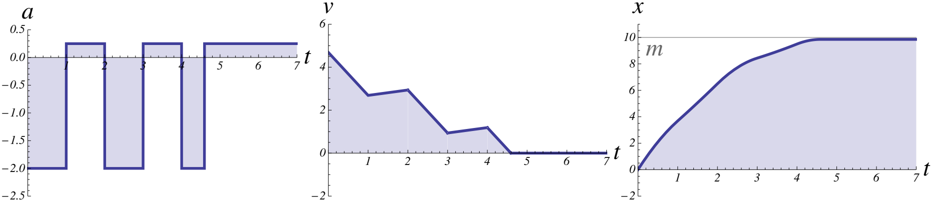
$Q \equiv$

Example (Single car car_ε time-triggered)

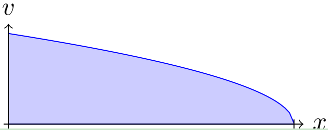
$$\Big(\big((?Q; a := A) \cup a := -b\big); t := 0; \{x' = v, v' = a, t' = 1 \,\&\, v \geq 0 \wedge t \leq \varepsilon\}\Big)^*$$

Example (Safely stays before traffic light m)

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



$Q \equiv$

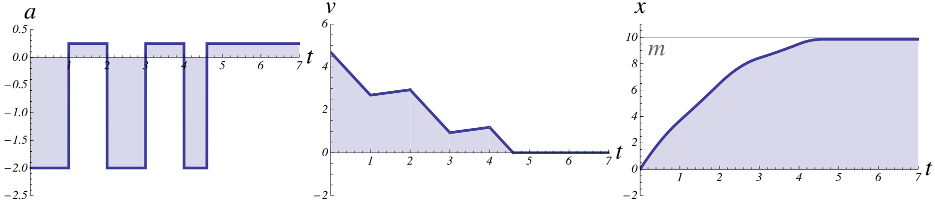


Example (Single car car_ε time-triggered)

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

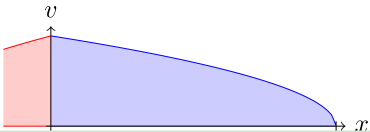
Example (Safely stays before traffic light m)

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



Ex: Car Control Properties

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

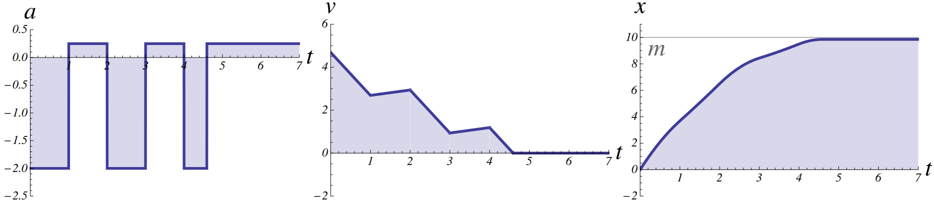


Example (Single car car_ε time-triggered)

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

Example (Safely stays before traffic light m)

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



Ex: Car Control Properties

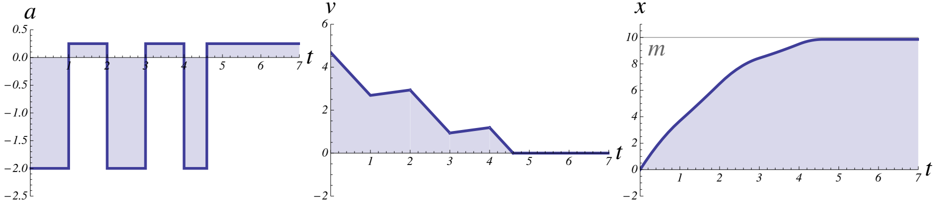
$Q \equiv 2b(m-x) \geq v^2 + \big(A+b\big)\big(A\varepsilon^2 + 2\varepsilon v\big)$

Example (Single car car_ε time-triggered)

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

Example (Live, can move everywhere)

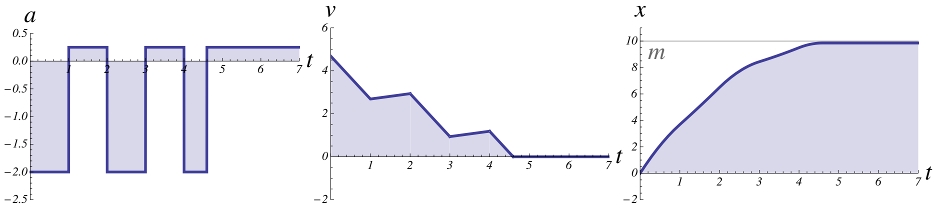
$$\varepsilon > 0 \land A > 0 \land b > 0 \rightarrow \forall p \exists m \langle car_\varepsilon \rangle\, x \geq p$$



Example (dL-based model-predictive control design)

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

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

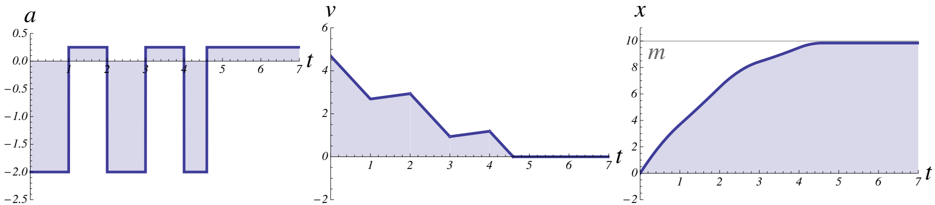


Example (dL-based model-predictive control design)

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

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

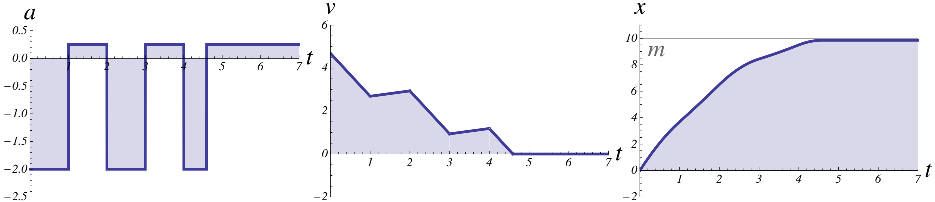
$$t := 0;\ \{x' = v, v' = a, t' = 1 \,\&\, v \geq 0 \land t \leq \varepsilon\})^*]\, x \leq m$$



Example (dL-based model-predictive control design)

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

$$\Big[\Big(\Big(\big(?\underline{\hspace{20em}};\ a:=A\big) \cup a:=-b\big);\ t:=0;\ \{x'=v, v'=a, t'=1 \,\&\, v\ge 0 \land t\le\varepsilon\}\Big)^*\Big]\, x\le m$$



Example (dL-based model-predictive control design)

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

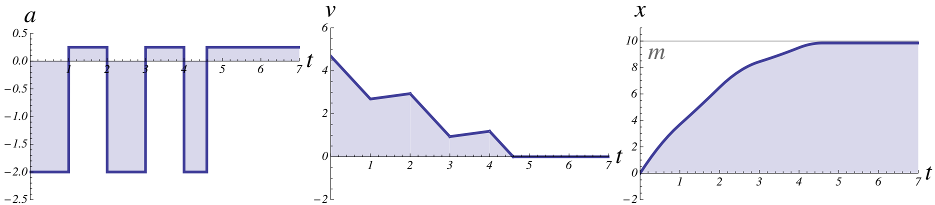
$\Big[\big(($

$(?$??? $\qquad;$

$a := A)$

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

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



Example (dL-based model-predictive control design)

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

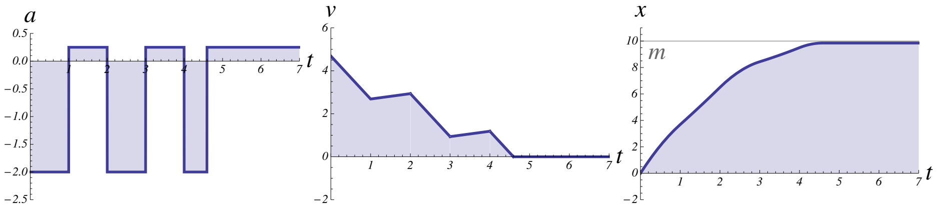
$$\Big[\Big(\Big($$

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

$$a := A)$$

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

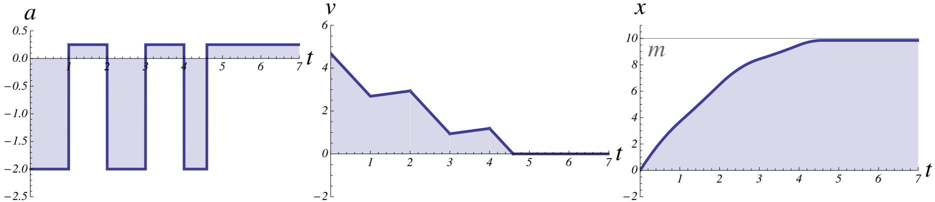
$$t := 0;\ \{x' = v, v' = a, t' = 1 \,\&\, v \ge 0 \land t \le \varepsilon\}\Big)^*\Big]\, x \le m$$



Example (dL-based model-predictive control design)

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

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



Example (dL-based model-predictive control design)

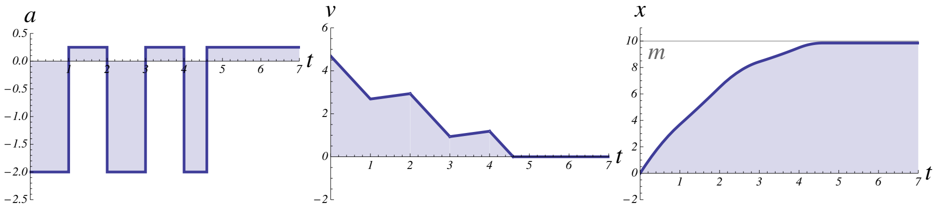
$$\underline{\color{red}{v^2 \le 2b(m-x)}} \land v \ge 0 \land A \ge 0 \land b > 0 \rightarrow$$

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

$$a:=A)$$

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

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



Example (dL-based model-predictive control design)

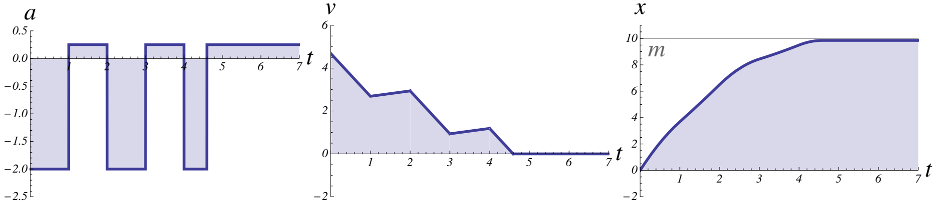
$$v^2 \le 2b(m-x) \land v \ge 0 \land A \ge 0 \land b > 0 \rightarrow$$

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

$$a:=A)$$

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

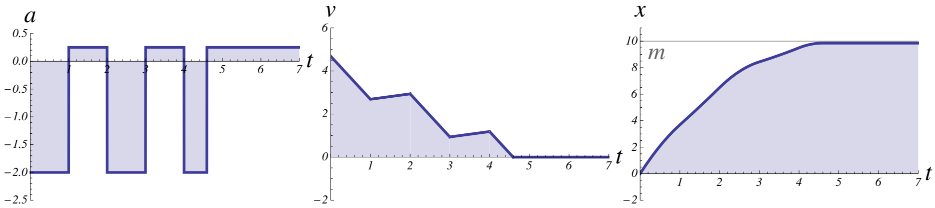
$$t:=0;\ \{x'=v, v'=a, t'=1 \,\&\, v \ge 0 \land t \le \varepsilon\})^*]\, x \le m$$



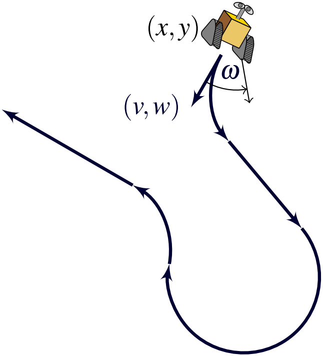
Example (dL-based model-predictive control design)

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

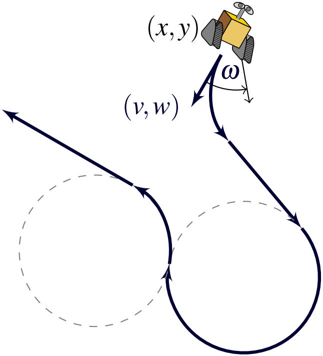
$$[((\; (?\underline{2b(m-x) \ge v^2 + (A+b)(A\varepsilon^2 + 2\varepsilon v)};\; a := A) \cup a := -b);\; t := 0;\; \{x' = v, v' = a, t' = 1 \,\&\, v \ge 0 \land t \le \varepsilon\})^*]\, x \le m$$



Runaround Robot with Dubins Paths



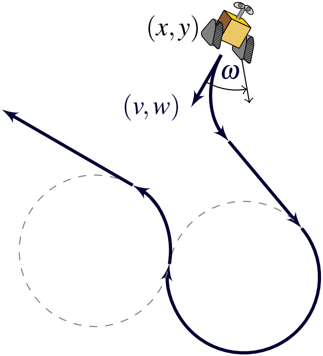
Runaround Robot with Dubins Paths



Example (Runaround Robot)

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

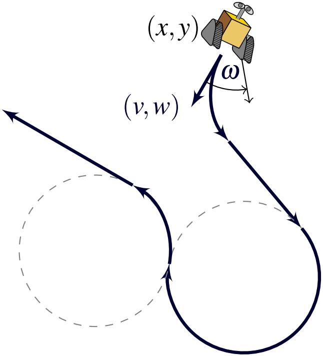
Runaround Robot with Dubins Paths



Example (Runaround Robot)

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

Runaround Robot with Dubins Paths



Example (Runaround Robot)

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

Outline (Proving CPS)

Differential Dynamic Logic: Axiomatization

equations of truth

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

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

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

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

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

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

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

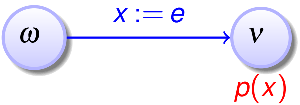
I $[\alpha^*]P \leftrightarrow P \wedge [\alpha^*](P \rightarrow [\alpha]P)$

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

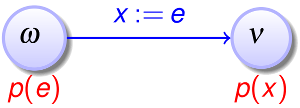
LICS'12,JAR'17

Dynamic Axioms for Dynamical Systems

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

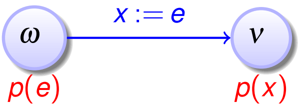


$[:=]\ [x := e]p(x) \leftrightarrow p(e)$

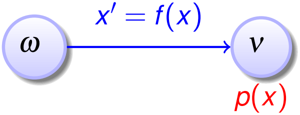


Dynamic Axioms for Dynamical Systems

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

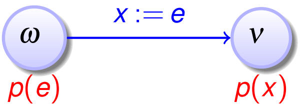


['] $[x' = f(x)]p(x) \leftrightarrow$

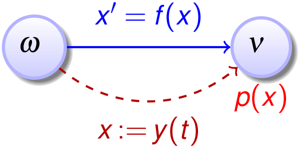


Dynamic Axioms for Dynamical Systems

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

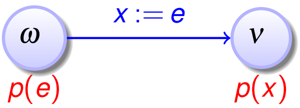


['] $[x' = f(x)]p(x) \leftrightarrow \qquad [x := y(t)]p(x)$

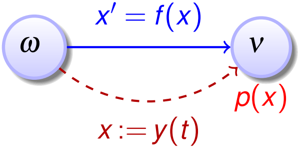


Dynamic Axioms for Dynamical Systems

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

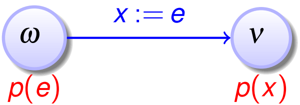


$[']$ $[x' = f(x)]p(x) \leftrightarrow \forall t \geq 0\, [x := y(t)]p(x)$

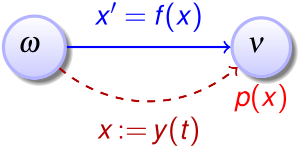


Dynamic Axioms for Dynamical Systems

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



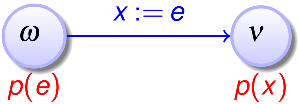
$[']$ $[x' = f(x)]p(x) \leftrightarrow \forall t{\geq}0\, [x := y(t)]p(x)$



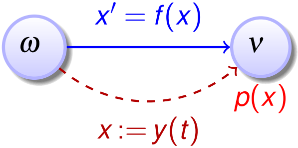
$[']$ $[x' = f(x)\,\&\, q(x)]p(x) \leftrightarrow \forall t{\geq}0\, \big([x := y(t)]p(x)\big)$

Dynamic Axioms for Dynamical Systems

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



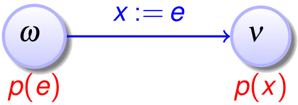
$['] \ [x' = f(x)]p(x) \leftrightarrow \forall t{\geq}0\, [x := y(t)]p(x)$



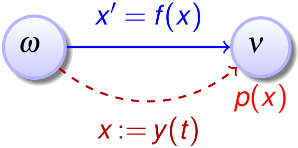
$['] \ [x' = f(x) \,\&\, q(x)]p(x) \leftrightarrow \forall t{\geq}0\, \big(\forall 0{\leq}s{\leq}t\, q(y(s)) \rightarrow [x := y(t)]p(x)\big)$

Dynamic Axioms for Dynamical Systems

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

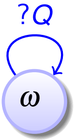


['] $[x' = f(x)]p(x) \leftrightarrow \forall t \geq 0\, [x := y(t)]p(x)$



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

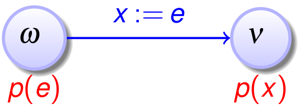
[?] $[?Q]P \leftrightarrow$



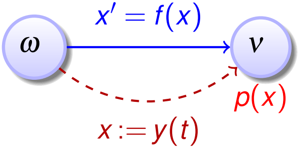
if $\omega \in [\![Q]\!]$

Dynamic Axioms for Dynamical Systems

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

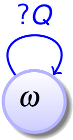


$[']\ [x' = f(x)]p(x) \leftrightarrow \forall t \geq 0\, [x := y(t)]p(x)$



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

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



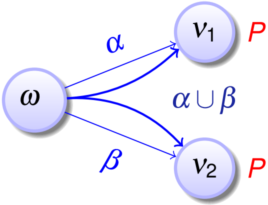
if $\omega \in [\![Q]\!]$

Dynamic Axioms for Dynamical Systems

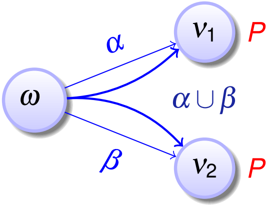
compositional semantics $\Rightarrow$ compositional proofs

Dynamic Axioms for Dynamical Systems

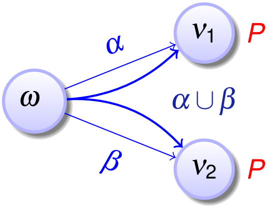
$[\cup]$ $[\alpha \cup \beta]P \leftrightarrow$



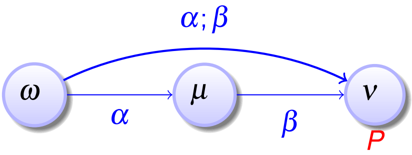
[∪] $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$



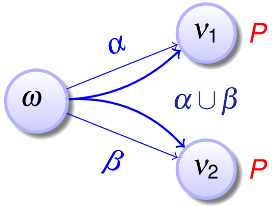
[∪] $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$



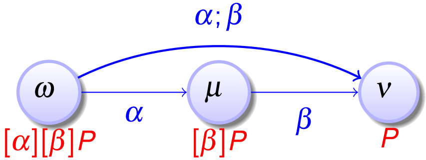
[;] $[\alpha;\beta]P \leftrightarrow$



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



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

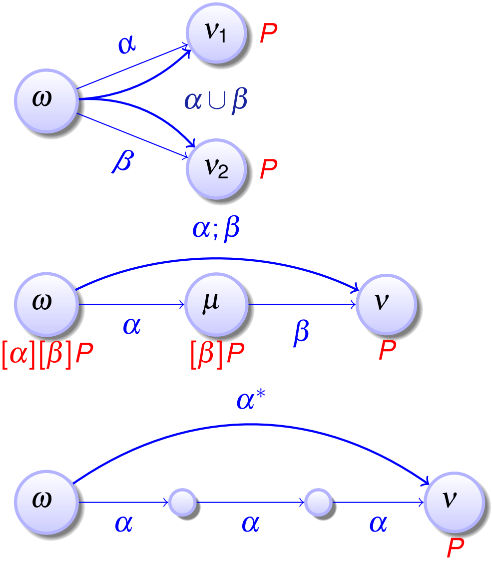


Dynamic Axioms for Dynamical Systems

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

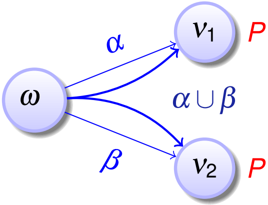
[;] $[\alpha;\beta]P \leftrightarrow [\alpha][\beta]P$

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

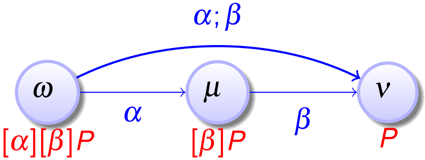


Dynamic Axioms for Dynamical Systems

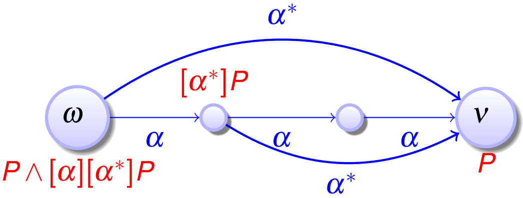
$[\cup]$ $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \land [\beta]P$



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

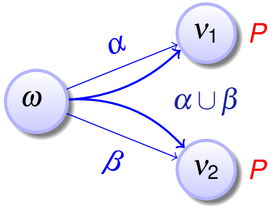


$[^*]$ $[\alpha^*]P \leftrightarrow P \land [\alpha][\alpha^*]P$

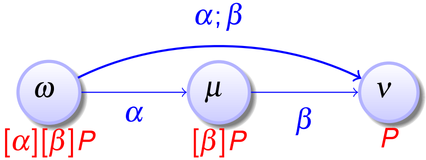


Dynamic Axioms for Dynamical Systems

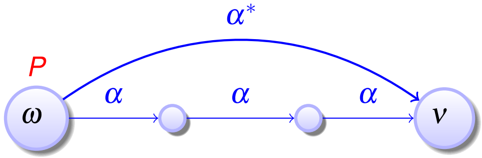
$[\cup]$ $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$



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

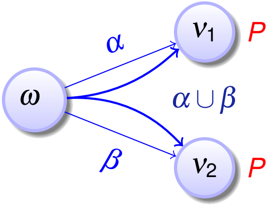


I $[\alpha^*]P \leftrightarrow P \wedge$

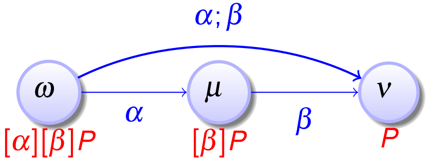


Dynamic Axioms for Dynamical Systems

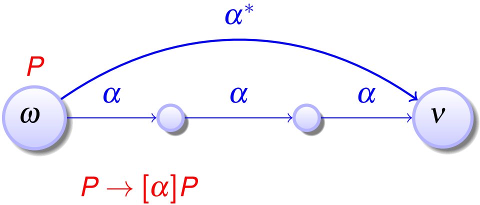
[∪] $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$



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

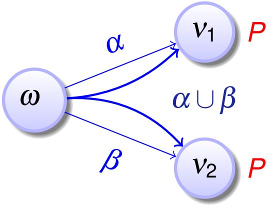


I $[\alpha^*]P \leftrightarrow P \wedge \qquad (P \to [\alpha]P)$

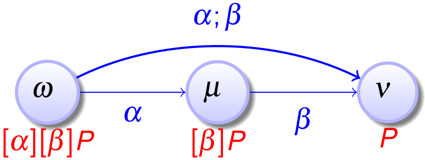


Dynamic Axioms for Dynamical Systems

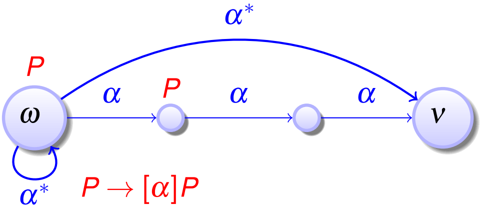
[∪] $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$



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

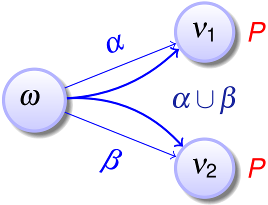


I $[\alpha^*]P \leftrightarrow P \wedge [\alpha^*](P \rightarrow [\alpha]P)$

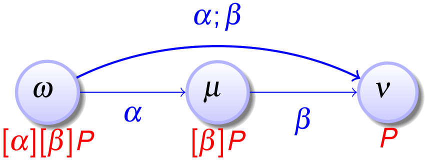


Dynamic Axioms for Dynamical Systems

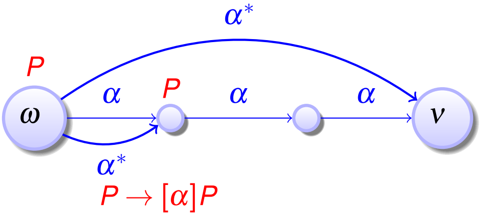
[∪] $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \land [\beta]P$



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

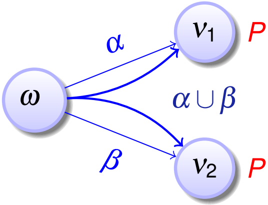


I $[\alpha^*]P \leftrightarrow P \land [\alpha^*](P \rightarrow [\alpha]P)$

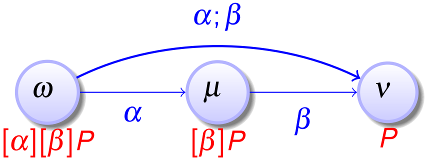


Dynamic Axioms for Dynamical Systems

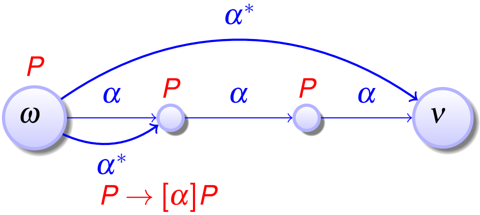
[∪] $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$



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

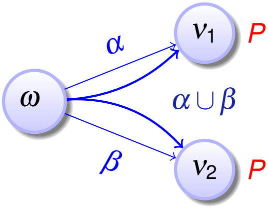


I $[\alpha^*]P \leftrightarrow P \wedge [\alpha^*](P \rightarrow [\alpha]P)$

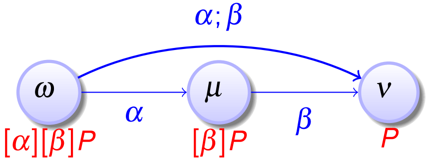


Dynamic Axioms for Dynamical Systems

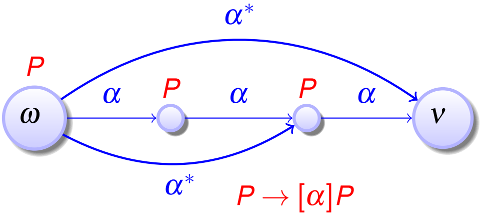
$[\cup]$ $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \land [\beta]P$



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

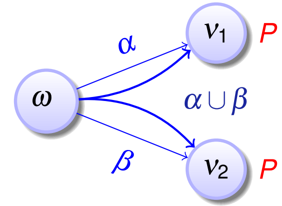


I $[\alpha^*]P \leftrightarrow P \land [\alpha^*](P \rightarrow [\alpha]P)$

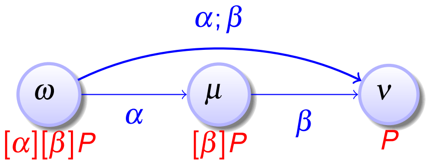


Dynamic Axioms for Dynamical Systems

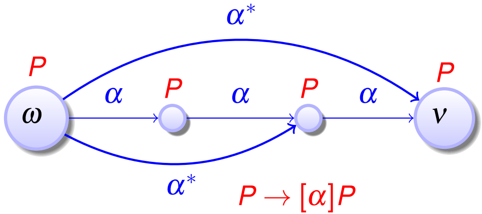
[∪] $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \land [\beta]P$



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

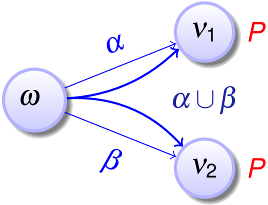


I $[\alpha^*]P \leftrightarrow P \land [\alpha^*](P \rightarrow [\alpha]P)$

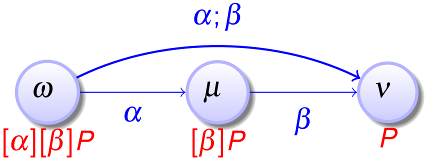


Dynamic Axioms for Dynamical Systems

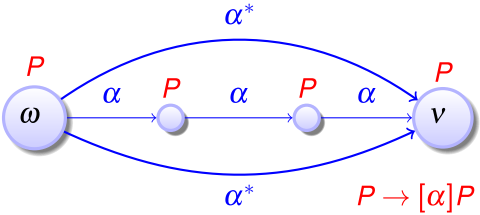
$[\cup]$ $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \land [\beta]P$



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



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

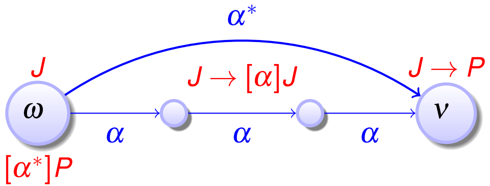


Proof Rule: Loop Invariants

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

Lemma (Loop invariant rule is derived)

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



Proof Rule: Loop Invariants

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

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

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

Lemma (Loop invariant rule is derived)

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

Proof (Derived rule).

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

□

Proof Rule: Loop Invariants

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

Lemma (Loop invariant rule is derived)

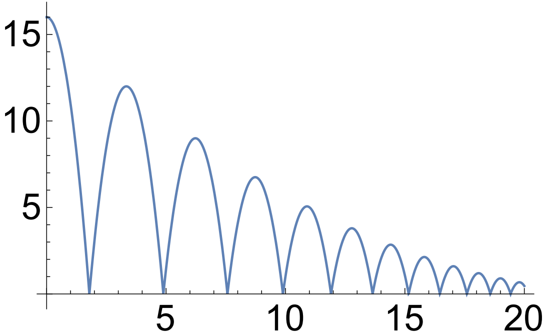
$$\textit{loop}\ \frac{\Gamma \vdash J, \Delta \quad J \vdash [\alpha]J \quad J \vdash P}{\Gamma \vdash [\alpha^*]P, \Delta}$$

Proof (Derived rule).

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

□

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



Example (Bouncing Ball)

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

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

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

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

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

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

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

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

$$[:=]\ \dfrac{j(x,v),\ x{=}0 \vdash j(x,-cv)}{j(x,v),\ x{=}0 \vdash [v:=-cv]j(x,v)}$$

$$[?],\!\to\!R\ \dfrac{j(x,v),\ x{=}0 \vdash [v:=-cv]j(x,v)}{j(x,v) \vdash [?x{=}0][v:=-cv]j(x,v)}$$

$$[;]\ \dfrac{j(x,v) \vdash [?x{=}0][v:=-cv]j(x,v)}{j(x,v) \vdash [?x{=}0;\ v:=-cv]j(x,v)}
\qquad
[?]\ \dfrac{j(x,v),\ x{\neq}0 \vdash j(x,v)}{j(x,v) \vdash [?x{\neq}0]j(x,v)}$$

$$\wedge R\ \dfrac{j(x,v) \vdash [?x{=}0;\ v:=-cv]j(x,v) \qquad j(x,v) \vdash [?x{\neq}0]j(x,v)}{j(x,v) \vdash [?x{=}0;\ v:=-cv]j(x,v) \wedge [?x{\neq}0]j(x,v)}$$

$$[\cup]\ \dfrac{j(x,v) \vdash [?x{=}0;\ v:=-cv]j(x,v) \wedge [?x{\neq}0]j(x,v)}{j(x,v) \vdash [?x{=}0;\ v:=-cv \cup ?x{\neq}0]j(x,v)}$$

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

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

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

$\mathrm{j}(x,v) \vdash 0 \leq x \land x \leq H$

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

$\mathrm{j}(x,v) \vdash 0 \leq x \land x \leq H$

2. $\mathrm{j}(x,v) \equiv 0 \leq x \land x \leq H$

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

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

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

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

2. $\mathrm{j}(x,v) \equiv 0 \le x \land x \le H$ — 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

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

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

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

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

$j(x,v) \vdash 0 \leq x \land x \leq H$

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

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 $v \gg 0$

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

$\mathrm{j}(x,v) \vdash 0 \le x \wedge x \le H$

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

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

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

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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. $j(x,v) \equiv x = 0 \lor x = H \land v = 0$

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

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. $j(x,v) \equiv x = 0 \vee x = H \wedge v = 0$ — no space for intermediate states
5. $j(x,v) \equiv 2gx = 2gH - v^2 \wedge x \ge 0$

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

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

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

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

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

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

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

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

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

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 $x > 0$
4. $j(x,v) \equiv x = 0 \lor x = H \land v = 0$ — no space for intermediate states
5. $j(x,v) \equiv 2gx{=}2gH{-}v^2 \land x{\geq}0$ — works: implicitly links v and x

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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 $x > 0$
4. $j(x,v) \equiv x = 0 \lor x = H \land v = 0$ — no space for intermediate states
5. $j(x,v) \equiv 2gx{=}2gH{-}v^2 \land x{\geq}0$ — works: implicitly links v and x

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

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

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

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

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

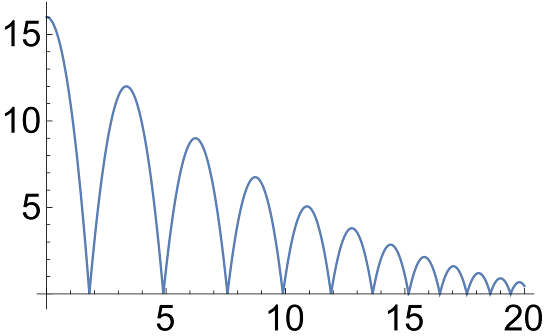
✓ $2gx{=}2gH{-}v^2 \land x{\geq}0, x{=}0 \vdash 2gx{=}2gH{-}({-}cv)^2 \land x{\geq}0$ if $c = 1\ldots$

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

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

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 $x > 0$
4. $j(x,v) \equiv x = 0 \lor x = H \land v = 0$ — no space for intermediate states
5. $j(x,v) \equiv 2gx{=}2gH{-}v^2 \land x{\geq}0$ — works: implicitly links v and x

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



Example (Bouncing Ball)

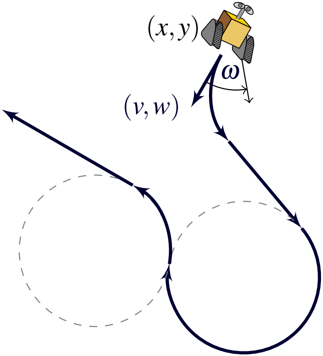
$$v=0 \land 1 \geq c \geq 0 \land H=x \geq 0 \land g>0 \rightarrow \Big[\big(\{x' = v, v' = -g \,\&\, x \geq 0\};$$
$$\text{if}(x = 0)\, v:=-cv\big)^*\Big]\, 0 \leq x \leq H$$

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

Runaround Robot with Dubins Paths



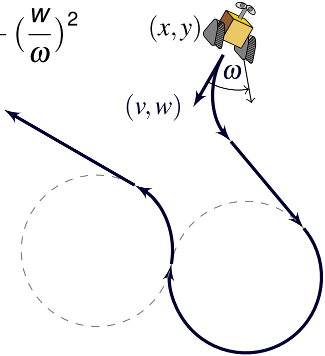
Example (Runaround Robot)

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

Runaround Robot with Dubins Paths

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

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

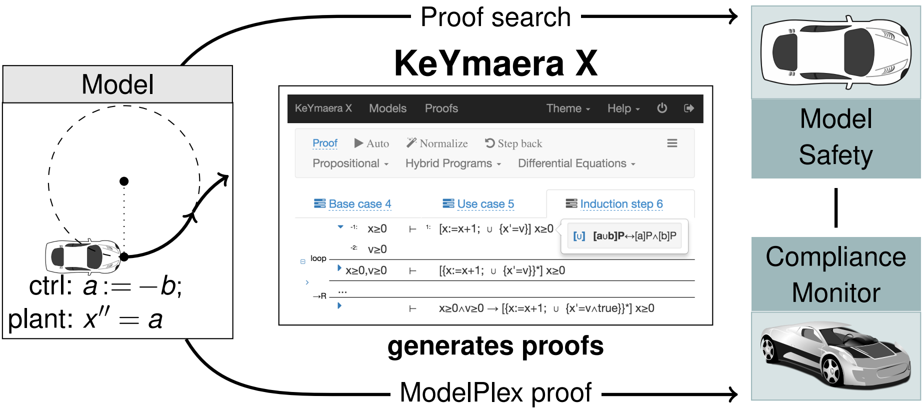


1. Obstacle not on tangential circle
2. Obstacle not on ray $(x,y) + \mathbb{R}(v,w)$

Example (Runaround Robot)

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

KeYmaera X aXiomatic Tactical Theorem Prover for CPS



Trustworthy

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

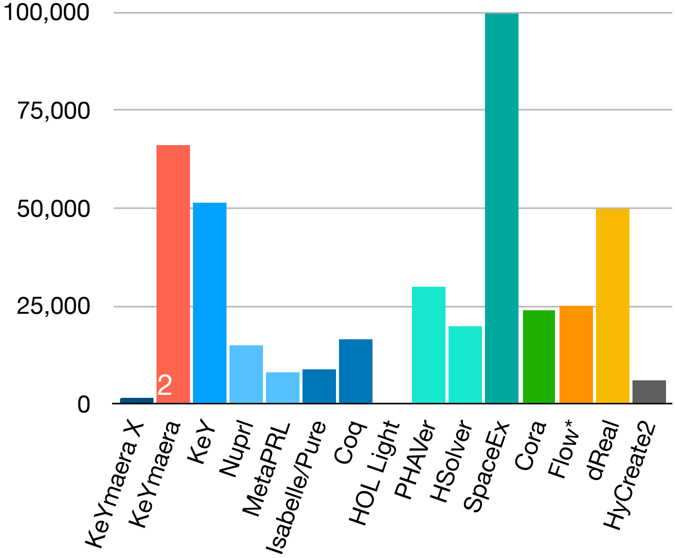
Flexible

- 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 $p(\cdot)$

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

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 operator $\otimes$
are not free in the substitution on its argument θ (U-admissible)

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

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 operator $\otimes$
are not free in the substitution on its argument θ (U-admissible)

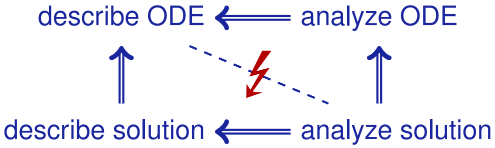
Uniform substitution σ replaces all occurrences of $p(\theta)$ for any θ by $\psi(\theta)$
function $f(\theta)$ for any θ by $\eta(\theta)$
quantifier $C(\phi)$ for any ϕ by $\psi(\theta)$
program const. a by α

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

Outline (Proving ODEs)

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

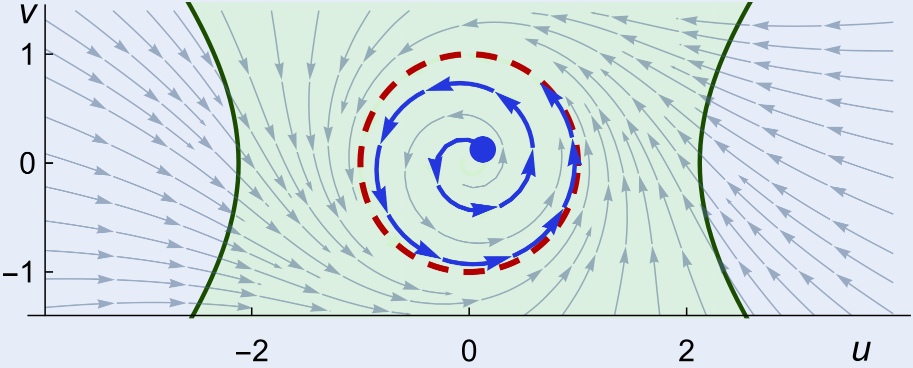
$$x'' = -x \qquad \text{has } x(t) = \sin(t) = t - \frac{t^3}{3!} + \frac{t^5}{5!} - \frac{t^7}{7!} + \frac{t^9}{9!} - \dots$$

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

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

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

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



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.*

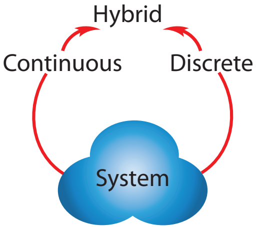
Differential Equation Axiomatization

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.*

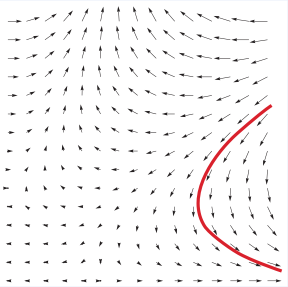
Theorem (Sound & Complete) (JAR'08, LICS'12, JAR'17)

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

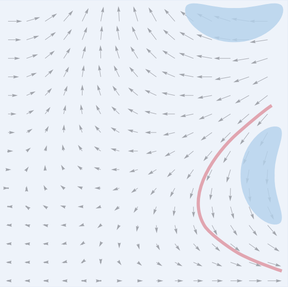


Differential Invariants for Differential Equations

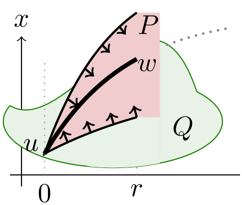
Differential Invariant

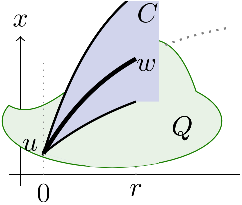


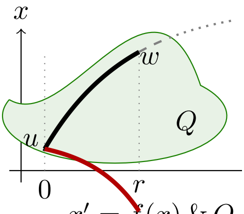
Differential Cut



Differential Ghost

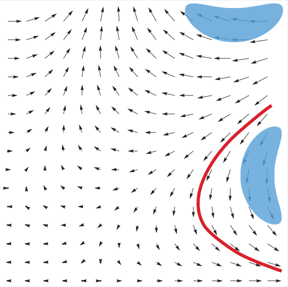




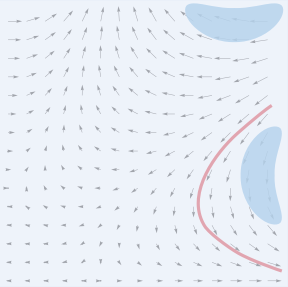


Differential Invariants for Differential Equations

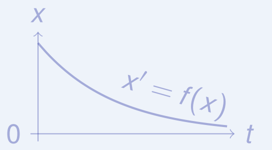
Differential Invariant

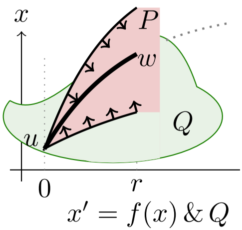


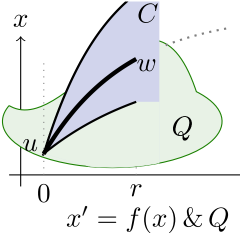
Differential Cut

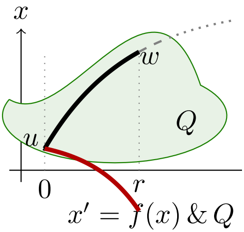


Differential Ghost



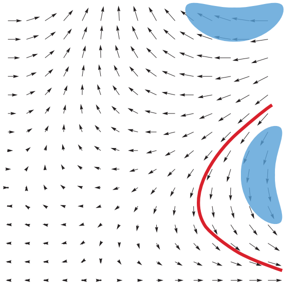




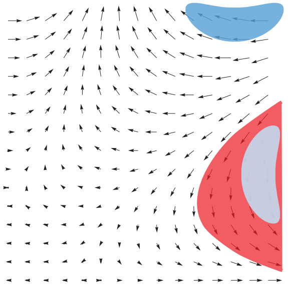


Differential Invariants for Differential Equations

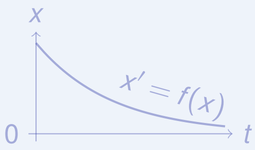
Differential Invariant

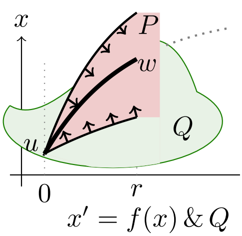


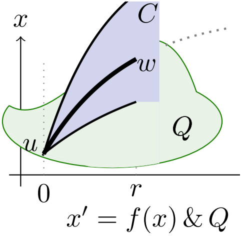
Differential Cut

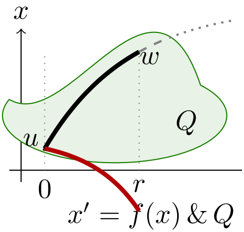


Differential Ghost



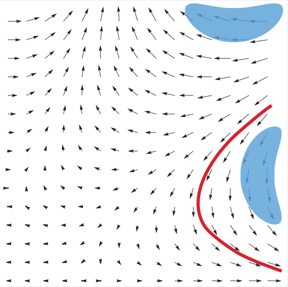




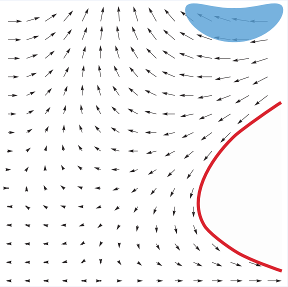


Differential Invariants for Differential Equations

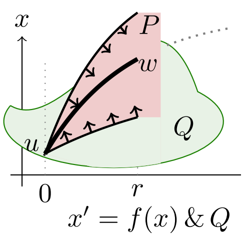
Differential Invariant

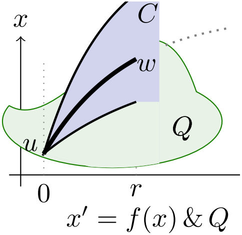


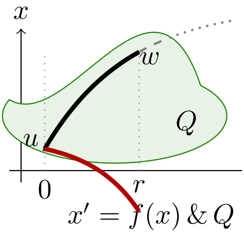
Differential Cut



Differential Ghost

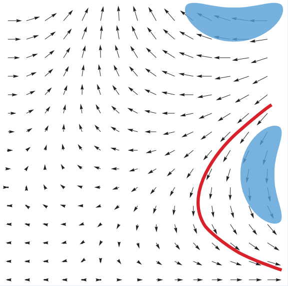




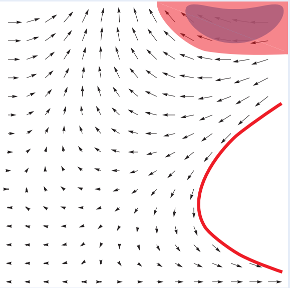


Differential Invariants for Differential Equations

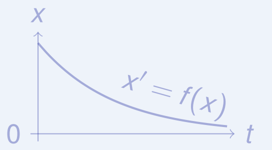
Differential Invariant

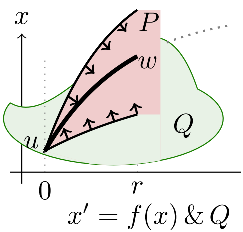


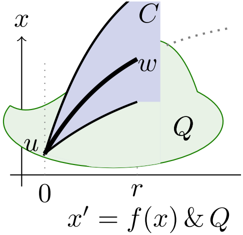
Differential Cut

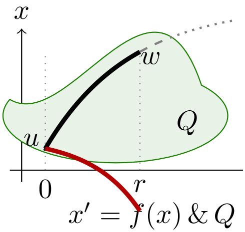


Differential Ghost



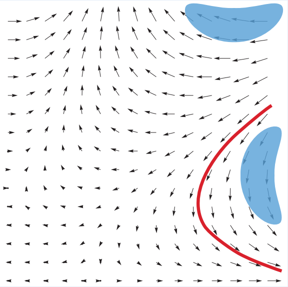




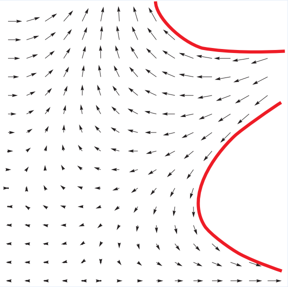


Differential Invariants for Differential Equations

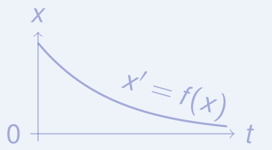
Differential Invariant

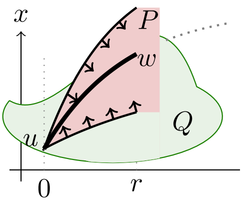


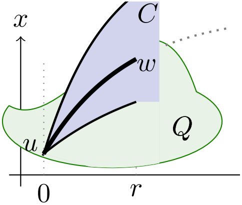
Differential Cut

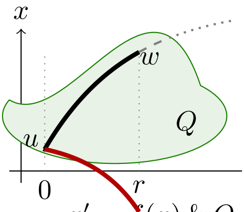


Differential Ghost



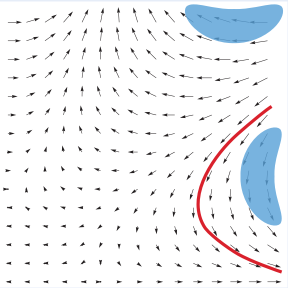


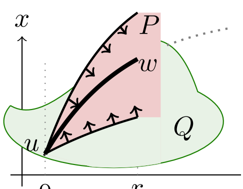




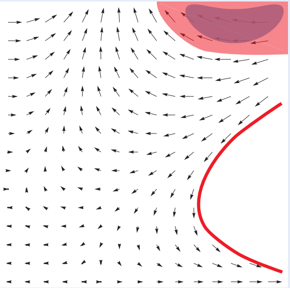
Differential Invariants for Differential Equations

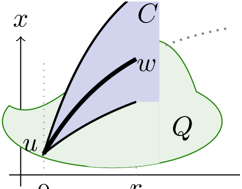
Differential Invariant



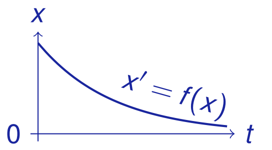


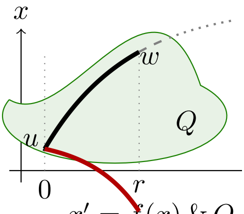
Differential Cut



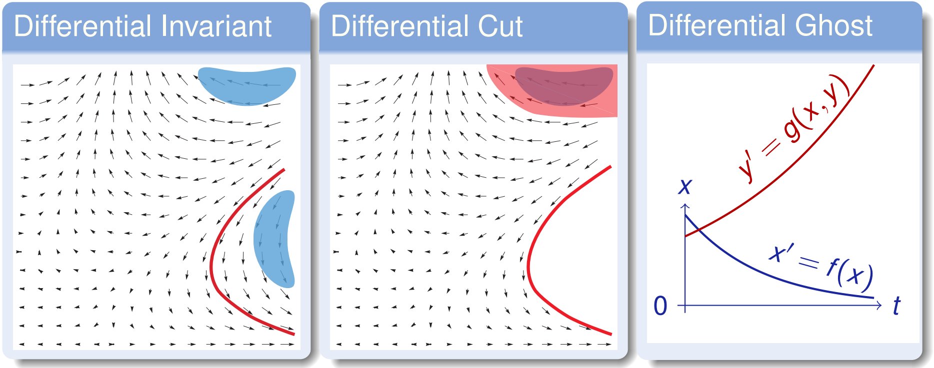


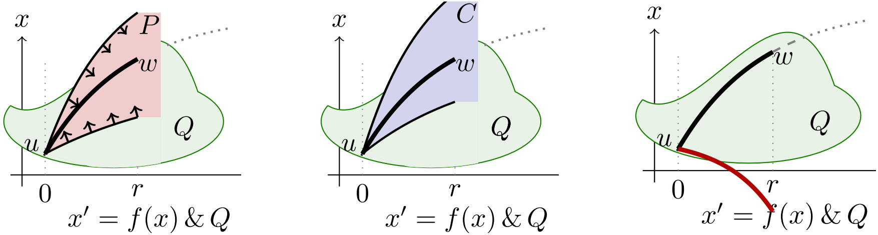
Differential Ghost





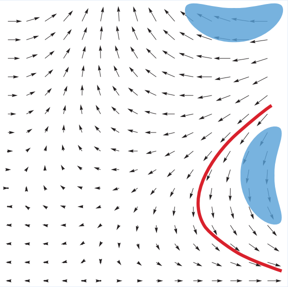
Differential Invariants for Differential Equations



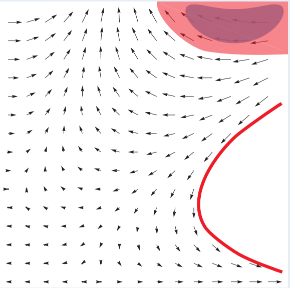


Differential Invariants for Differential Equations

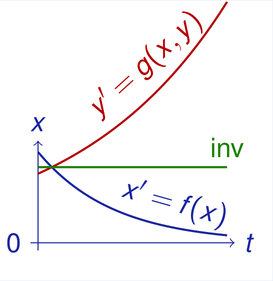
Differential Invariant

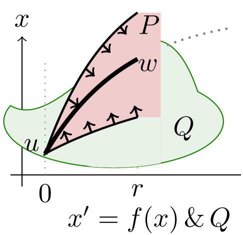


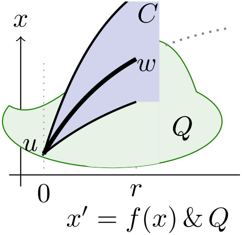
Differential Cut

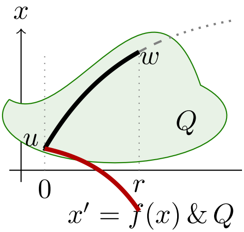


Differential Ghost





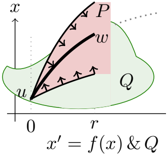




Differential Invariants for Differential Equations

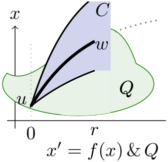
Differential Invariant

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



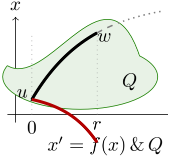
Differential Cut

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



Differential Ghost

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



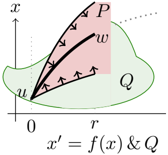
deductive power adds DI $\prec$ DC $\prec$ DG

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

Differential Invariants for Differential Equations

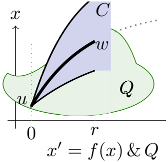
Differential Invariant

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



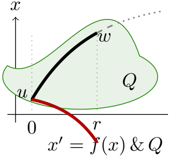
Differential Cut

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



Differential Ghost

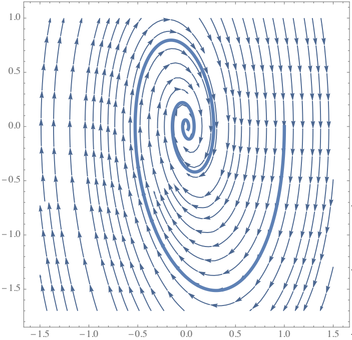
$$\frac{P \leftrightarrow \exists y\, G \quad G \vdash [x' = f(x), y' = g(x,y) \,\&\, Q]G}{P \vdash [x' = f(x) \,\&\, Q]P}$$

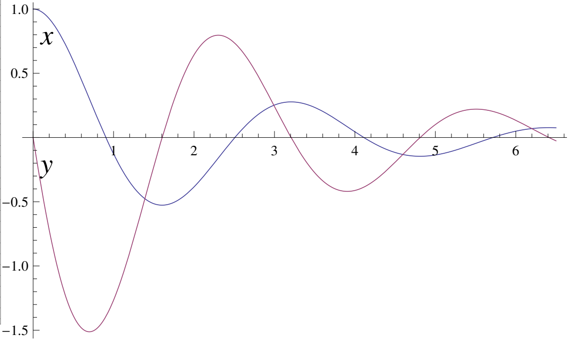


if new $y' = g(x,y)$ has long enough solution

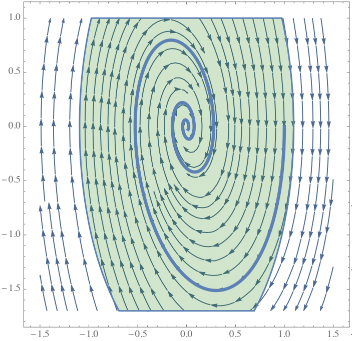
JLogComput'10,LMCS'12, LICS'12,JAR'17,LICS'18

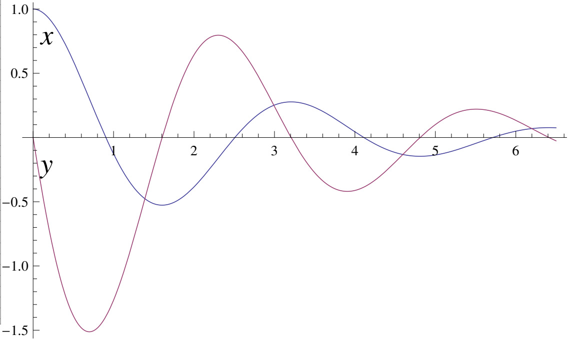
$$\frac{}{\omega^2 x^2 + y^2 \le c^2 \vdash [x' = y, y' = -\omega^2 x - 2d\omega y \,\&\, \omega \ge 0 \land d \ge 0]\, \omega^2 x^2 + y^2 \le c^2}$$





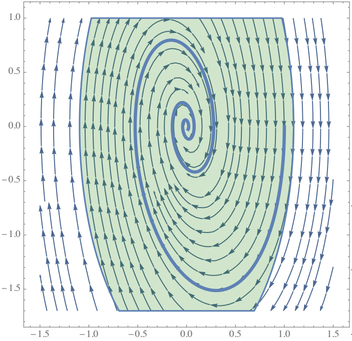
$$\frac{}{\omega^2x^2+y^2\le c^2 \vdash [x'=y, y'=-\omega^2x-2d\omega y \,\&\, \omega\ge 0 \land d\ge 0]\, \omega^2x^2+y^2\le c^2}$$

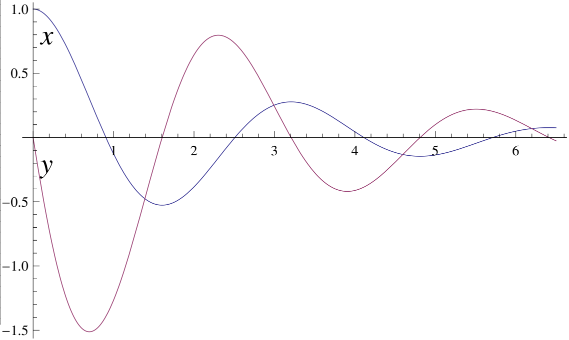




damped oscillator

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





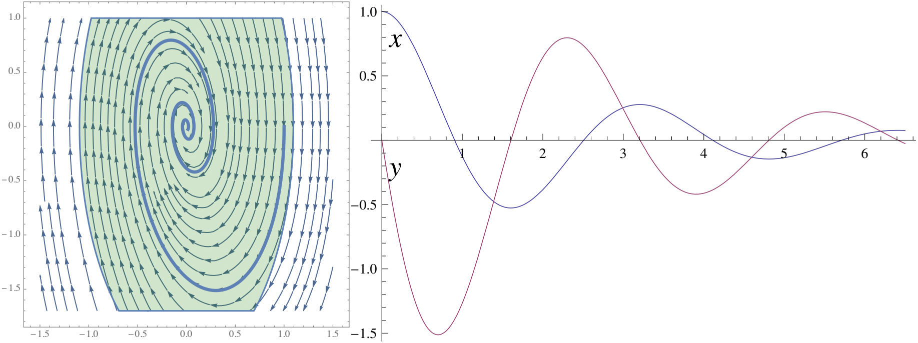
damped oscillator

Differential Invariants for Differential Equations

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

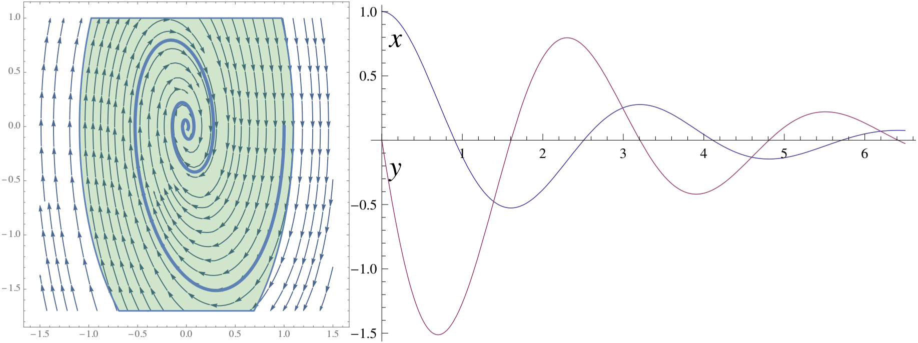
$$\omega\geq 0 \land d\geq 0 \vdash [x':=y][y':=-\omega^2 x - 2d\omega y]\,2\omega^2 x x' + 2y y' \leq 0$$

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



damped oscillator

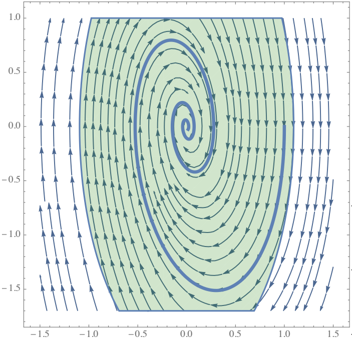
$$
\cfrac{\cfrac{\cfrac{*}{\omega\geq 0 \land d\geq 0 \vdash 2\omega^2 xy + 2y(-\omega^2 x - 2d\omega y) \leq 0}}{\omega\geq 0 \land d\geq 0 \vdash [x':=y][y':=-\omega^2 x - 2d\omega y]\, 2\omega^2 x x' + 2yy' \leq 0}}{\omega^2x^2+y^2\leq c^2 \vdash [x' = y, y' = -\omega^2 x - 2d\omega y \,\&\, \omega\geq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

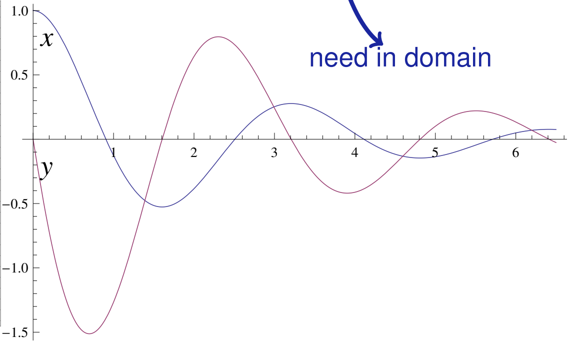


damped oscillator

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

need in domain

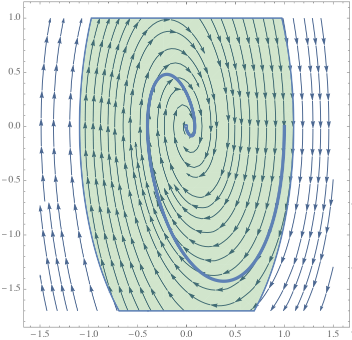


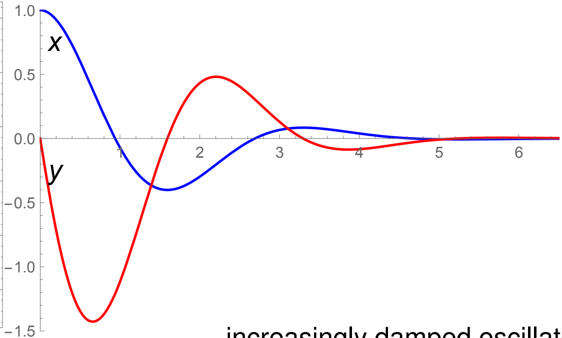


damped oscillator

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

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





increasingly damped oscillator

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

increasingly damped oscillator

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

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

ask

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

increasingly damped oscillator

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

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

increasingly damped oscillator

Differential Cuts for Differential Equations

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

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

increasingly damped oscillator

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

DC

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

increasingly damped oscillator

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

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

increasingly damped oscillator

$$\dfrac{\dfrac{\dfrac{\omega\geq0\land d\geq0 \vdash 2\omega^2xy+2y(-\omega^2x-2d\omega y)\leq0}{\omega\geq0\land d\geq0 \vdash [x':=y][y':=-\omega^2x-2d\omega y]\,2\omega^2xx'+2yy'\leq0}}{\omega^2x^2+y^2\leq c^2 \vdash [x'=y,y'=-\omega^2x-2d\omega y,d'=7\,\&\,\omega\geq0\land d\geq0]\,\omega^2x^2+y^2\leq c^2}}{\omega^2x^2+y^2\leq c^2 \vdash [x'=y,y'=-\omega^2x-2d\omega y,d'=7\,\&\,\omega\geq0]\,\omega^2x^2+y^2\leq c^2}$$

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

increasingly damped oscillator

Differential Cuts for Differential Equations

$$*$$

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

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

$$\omega^2x^2+y^2\leq c^2 \vdash [x'=y,y'=-\omega^2x-2d\omega y,d'=7\,\&\,\omega\geq0\land d\geq0]\,\omega^2x^2+y^2\leq c^2$$

$$\omega^2x^2+y^2\leq c^2 \vdash [x'=y,y'=-\omega^2x-2d\omega y,d'=7\,\&\,\omega\geq0]\,\omega^2x^2+y^2\leq c^2$$

$$*$$

$$\omega\geq0 \vdash 7\geq0$$

$$\omega\geq0 \vdash [d':=7]\,d'\geq0$$

$$d\geq0 \vdash [x'=y,y'=-\omega^2x-2d\omega y,d'=7\,\&\,\omega\geq0]\,d\geq0$$

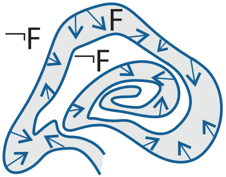
increasingly damped oscillator

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

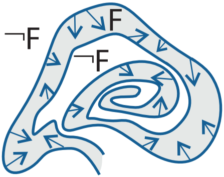
init

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

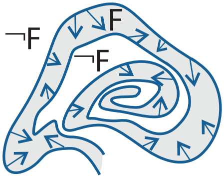
Could repeatedly diffcut in formulas to help the proof

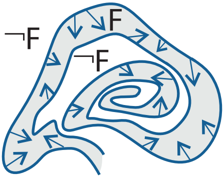


$$\frac{Q \vdash [x' := f(x)](F)'}{F \vdash [x' = f(x) \,\&\, Q]F}$$



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





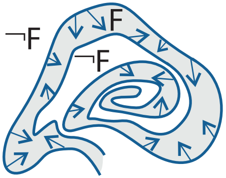
$$\frac{Q \vdash [x' := f(x)](F)'}{F \vdash [x' = f(x) \,\&\, Q]F}$$

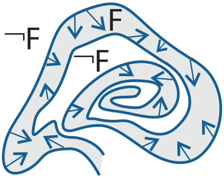
$$\frac{{\color{red}F} \land Q \vdash [x' := f(x)](F)'}{F \vdash [x' = f(x) \,\&\, Q]F}$$

Example (Inductive hypothesis)

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

Assuming Differential Invariance



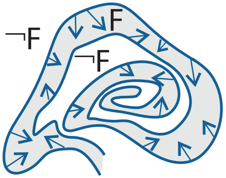


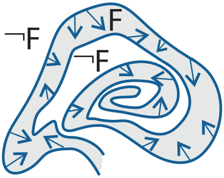
$$\frac{Q \vdash [x' := f(x)](F)'}{F \vdash [x' = f(x) \,\&\, Q]F}$$

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

Example (Inductive hypothesis)

$$\frac{\overline{v^2 - 2v + 1 = 0 \vdash [v' := w][w' := -v]2vv' - 2v' = 0}}{v^2 - 2v + 1 = 0 \vdash [v' = w, w' = -v]v^2 - 2v + 1 = 0}$$

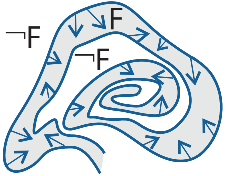




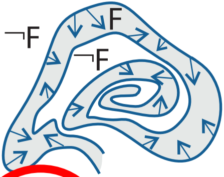
$$\frac{Q \vdash [x' := f(x)](F)'}{F \vdash [x' = f(x) \,\&\, Q]F} \qquad \frac{F \land Q \vdash [x' := f(x)](F)'}{F \vdash [x' = f(x) \,\&\, Q]F}$$

Example (Inductive hypothesis)

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



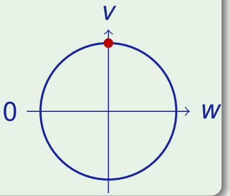
$$\frac{Q \vdash [x' := f(x)](F)'}{F \vdash [x' = f(x) \,\&\, Q]F}$$



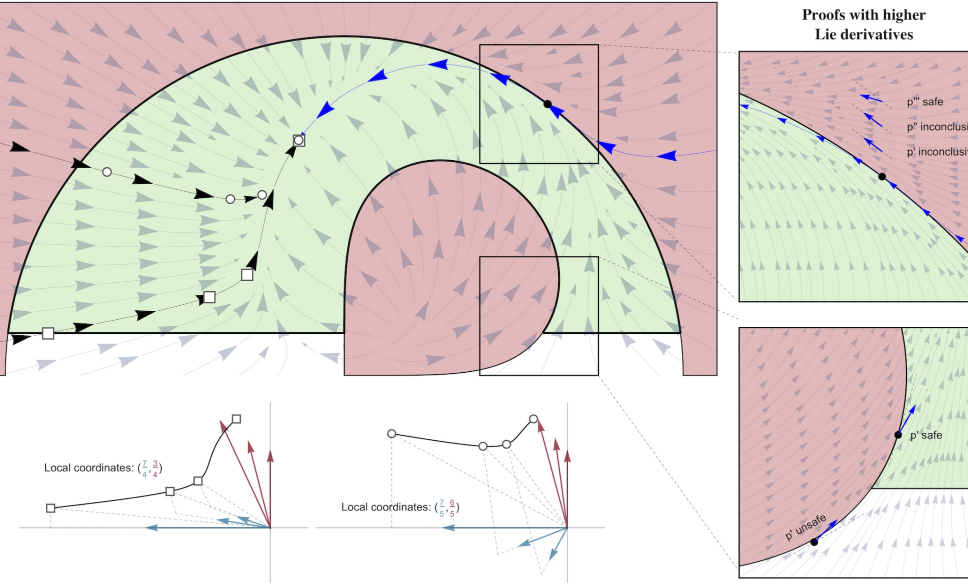
$$\frac{F \land Q \vdash [x' := f(x)](F)'}{F \vdash [x' = f(x) \,\&\, Q]F}$$

Example (Inductive hypothesis is unsound!)

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

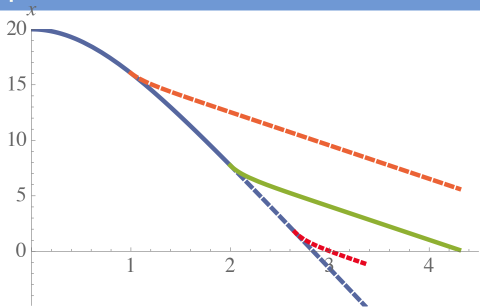


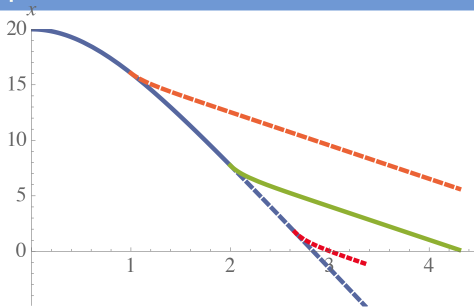
ODE Axiomatization



Proofs use continuously changing basis ↗ **to keep invariants at constant local coordinates**

Sound and complete ODE invariance proofs

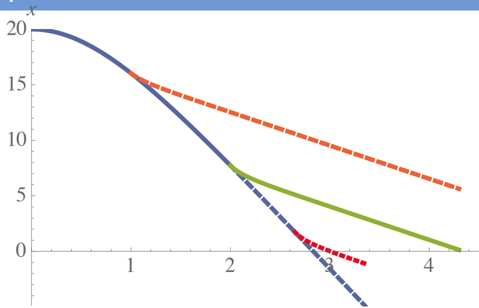

x
20
15
10
5
0
1
2
3
4



Example (Parachute)

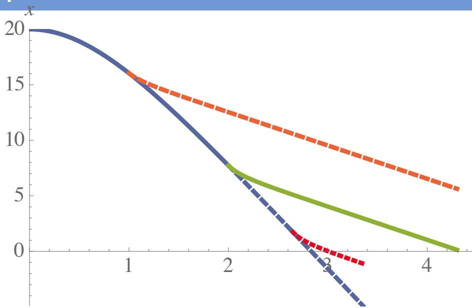
$$\big((?(Q\land r=a)\cup r:=p); t:=0;$$
$$\{x'=v, v'=-g+rv^2, t'=1 \,\&\, t\le T\land x\ge 0\land v<0\}\big)^*$$

Ex: Parachute Open or Keep Closed



Example (Parachute)

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



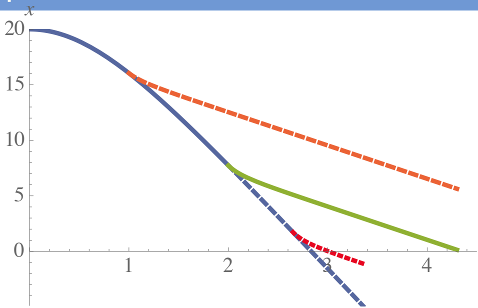
Example (Parachute)

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

Ex: Parachute Open or Keep Closed

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

Conservatively bounded next velocity above parachute's limit velocity.



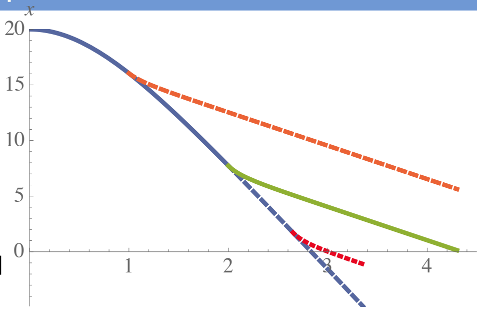
Example (Parachute)

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

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

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

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



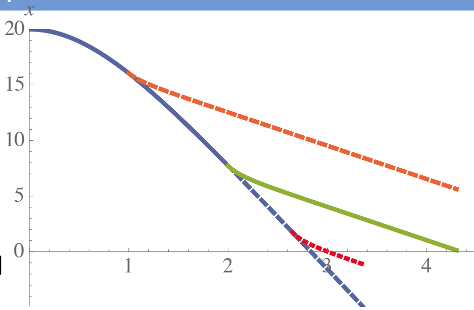
Example (Parachute)

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

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

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

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



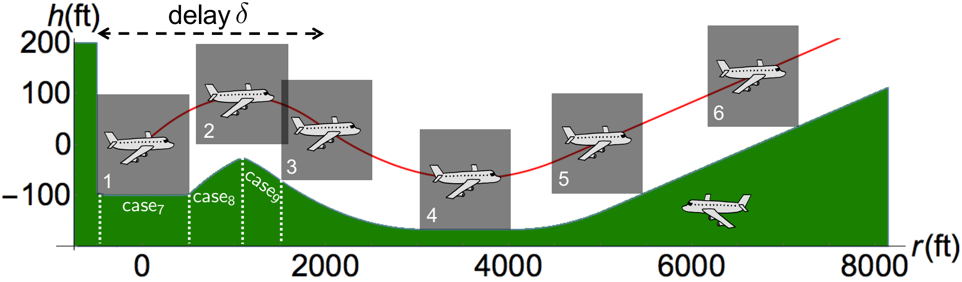
$v \geq \mathrm{old}(v) - gt$ if closed

Example (Parachute)

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

Outline (CPS Application Highlights)

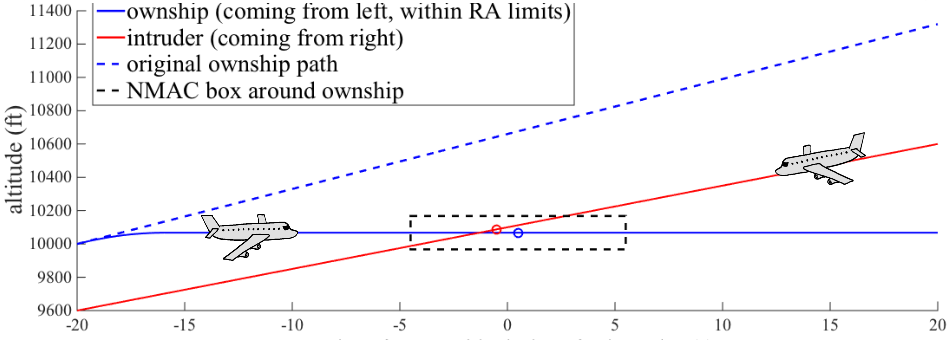
- Developed by the FAA to replace current TCAS in aircraft
- Approximately optimizes Markov Decision Process on a grid
- Advisory from lookup tables with numerous 5D interpolation regions



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

STTT'17

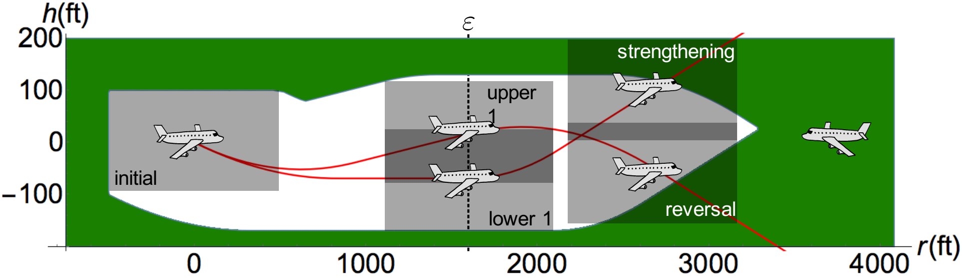
ACAS X table comparison shows safe advisory in 97.7% of the 648,591,384,375 states compared (15,160,434,734 counterexamples).



ACAS X issues DNC advisory, which induces collision unless corrected

STTT'17

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

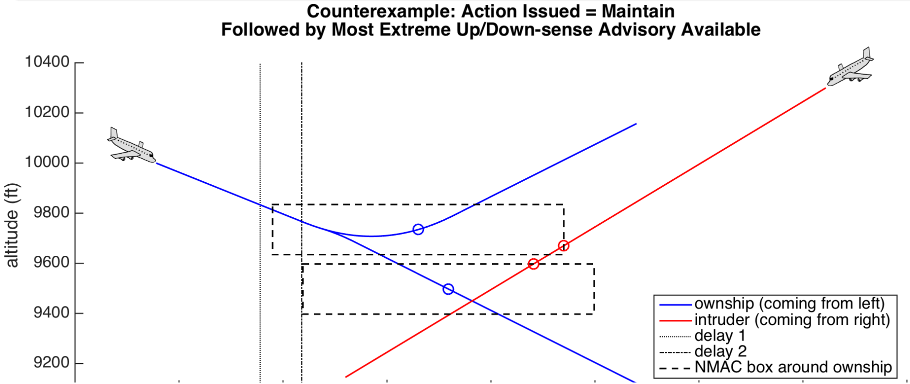


1. Identified safeable region for each advisory symbolically
2. Proved safety for hybrid systems flight model in KeYmaera X

STTT'17

Airborne Collision Avoidance System ACAS X: Compare

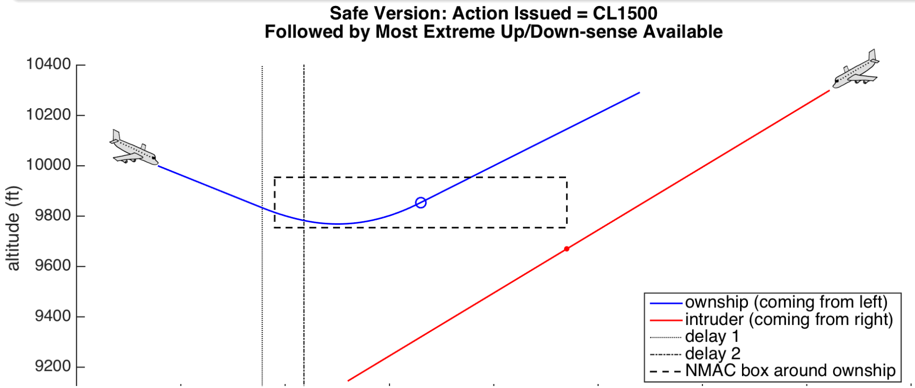
ACAS X table comparison shows safeable advisory in more of the 648,591,384,375 states compared (≈899 10^6 counterexamples).



ACAS X issues Maintain advisory instead of CL1500

STTT'17

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

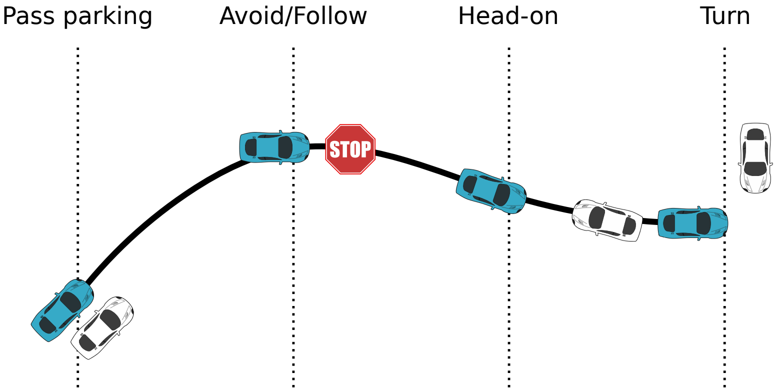


ACAS X issues Maintain advisory instead of CL1500

STTT'17

Ground Robot Obstacle Avoidance: Verify

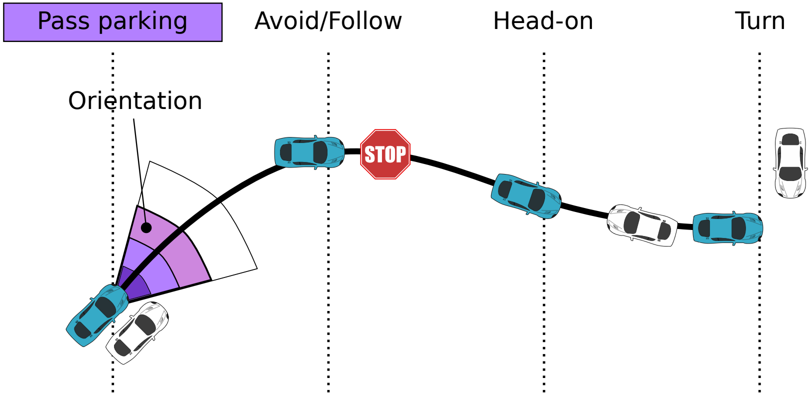
- Fundamental safety question for ground robot navigation — IJRR'17
- When will which control decision avoid obstacles?
- Depends on safety objective, physical capabilities of robot + obstacle



1. Identified safe region for each safety notion symbolically
2. Proved safety for hybrid systems ground robot model in KeYmaera X

Ground Robot Obstacle Avoidance: Verify

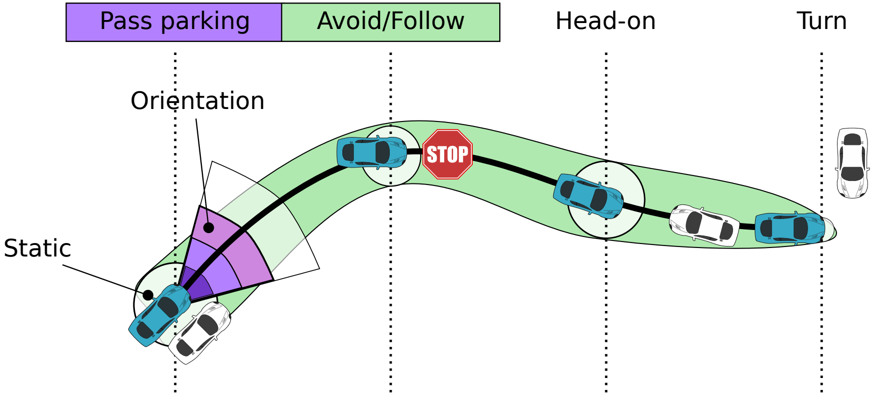
- Fundamental safety question for ground robot navigation — IJRR'17
- When will which control decision avoid obstacles?
- Depends on safety objective, physical capabilities of robot + obstacle



1. Identified safe region for each safety notion symbolically
2. Proved safety for hybrid systems ground robot model in KeYmaera X

Ground Robot Obstacle Avoidance: Verify

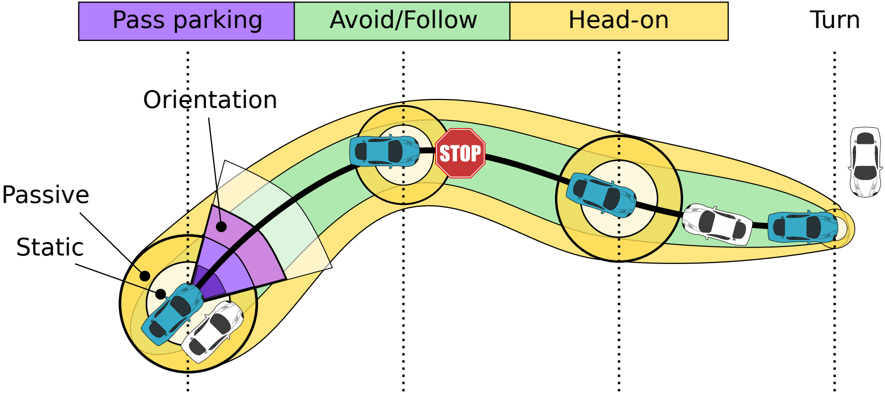
- Fundamental safety question for ground robot navigation IJRR'17
- When will which control decision avoid obstacles?
- Depends on safety objective, physical capabilities of robot + obstacle



1. Identified safe region for each safety notion symbolically
2. Proved safety for hybrid systems ground robot model in KeYmaera X

Ground Robot Obstacle Avoidance: Verify

- Fundamental safety question for ground robot navigation IJRR'17
- When will which control decision avoid obstacles?
- Depends on safety objective, physical capabilities of robot + obstacle

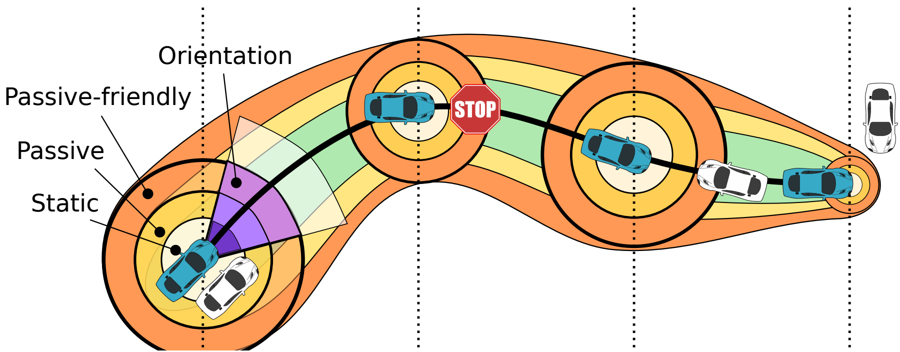


1. Identified safe region for each safety notion symbolically
2. Proved safety for hybrid systems ground robot model in KeYmaera X

Ground Robot Obstacle Avoidance: Verify

- Fundamental safety question for ground robot navigation — IJRR'17
- When will which control decision avoid obstacles?
- Depends on safety objective, physical capabilities of robot + obstacle

Pass parking	Avoid/Follow	Head-on	Turn



1. Identified safe region for each safety notion symbolically
2. Proved safety for hybrid systems ground robot model in KeYmaera X

Ground Robot Invariants and Safe Control Constraints

Safety	Invariant + Safe Control
static	$\lVert p-o\rVert_\infty > \frac{s^2}{2b} + \left(\frac{A}{b}+1\right)\left(\frac{A}{2}\varepsilon^2+\varepsilon s\right)$
passive	$s\neq 0 \rightarrow \lVert p-o\rVert_\infty > \frac{s^2}{2b} + V\frac{s}{b} + \left(\frac{A}{b}+1\right)\left(\frac{A}{2}\varepsilon^2+\varepsilon(s+V)\right)$
+ sensor	$\lVert \hat{p}-o\rVert_\infty > \frac{s^2}{2b} + V\frac{s}{b} + \left(\frac{A}{b}+1\right)\left(\frac{A}{2}\varepsilon^2+\varepsilon(s+V)\right) + \Delta_p$
+ disturb.	$\lVert p-o\rVert_\infty > \frac{s^2}{2b\Delta_a} + V\frac{s}{b\Delta_a} + \left(\frac{A}{b\Delta_a}+1\right)\left(\frac{A}{2}\varepsilon^2+\varepsilon(s+V)\right)$
+ failure	$\lVert \hat{p}-o\rVert_\infty > \frac{s^2}{2b} + V\frac{s}{b} + \left(\frac{A}{b}+1\right)\left(\frac{A}{2}\varepsilon^2+\varepsilon(v+V)\right) + \Delta_p + g\Delta$
friendly	$\lVert p-o\rVert_\infty > \frac{s^2}{2b} + \frac{V^2}{2b_o} + V\left(\frac{s}{b}+\tau\right) + \left(\frac{A}{b}+1\right)\left(\frac{A}{2}\varepsilon^2+\varepsilon(s+V)\right)$

⋮

IJRR'17

Ground Robot Invariants and Safe Control Constraints

Safety	Invariant + Safe Control
static	$\|p-o\|_\infty > \frac{s^2}{2b} + \left(\frac{A}{b}+1\right)\left(\frac{A}{2}\varepsilon^2+\varepsilon s\right)$
passive	$s \neq 0 \rightarrow \|p-o\|_\infty > \frac{s^2}{2b} + V\frac{s}{b} + \left(\frac{A}{b}+1\right)\left(\frac{A}{2}\varepsilon^2+\varepsilon(s+V)\right)$
+ sensor	[illegible] $V)\big) + \Delta_p$
+ disturb.	$\|p-o\|_\infty > \frac{[illegible]}{2b\Delta_a} + V\frac{[illegible]}{b\Delta_a} + \left(\frac{[illegible]}{b\Delta_a}+1\right)\left(\frac{[illegible]}{2}\varepsilon^{[illegible]}+\varepsilon(s+V)\right)$
+ failure	$\|\hat{p}-o\|_\infty > \frac{s^2}{2b} + V\frac{s}{b} + \left(\frac{A}{b}+1\right)\left(\frac{A}{2}\varepsilon^2+\varepsilon(v+V)\right) + \Delta_p + g\Delta$
friendly	$\|p-o\|_\infty > \frac{s^2}{2b} + \frac{V^2}{2b_o} + V\left(\frac{s}{b}+\tau\right) + \left(\frac{A}{b}+1\right)\left(\frac{A}{2}\varepsilon^2+\varepsilon(s+V)\right)$

⋮

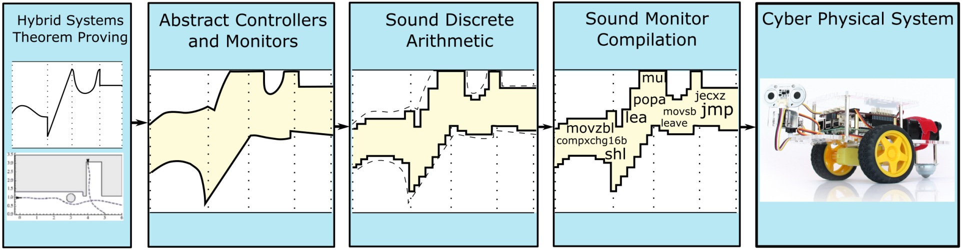
Question

How to find and justify constraints? Proof!

IJRR'17

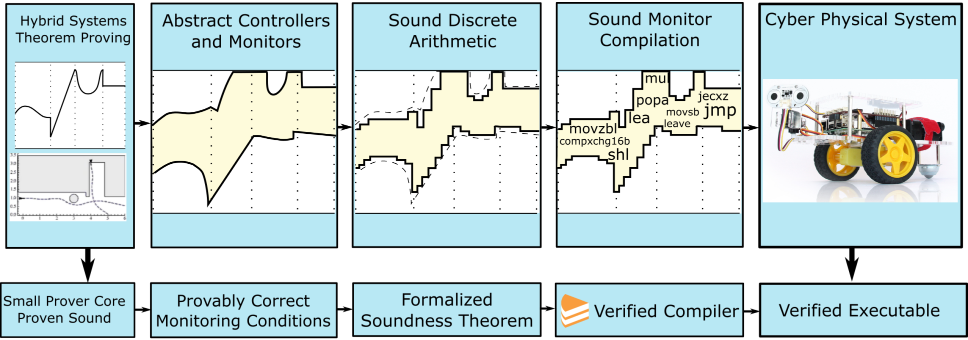
Outline (CPS Executables)

VeriPhy: Automatic, Verified EXEs from Controllers



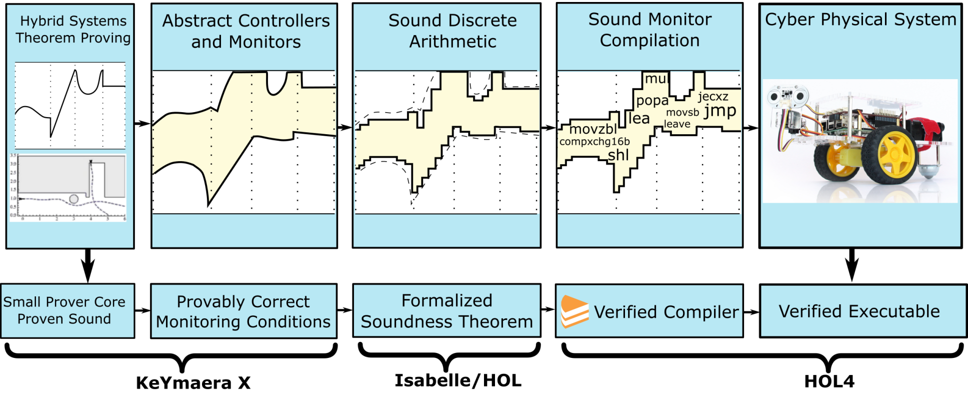
PLDI'18

VeriPhy: Automatic, Verified EXEs from Controllers



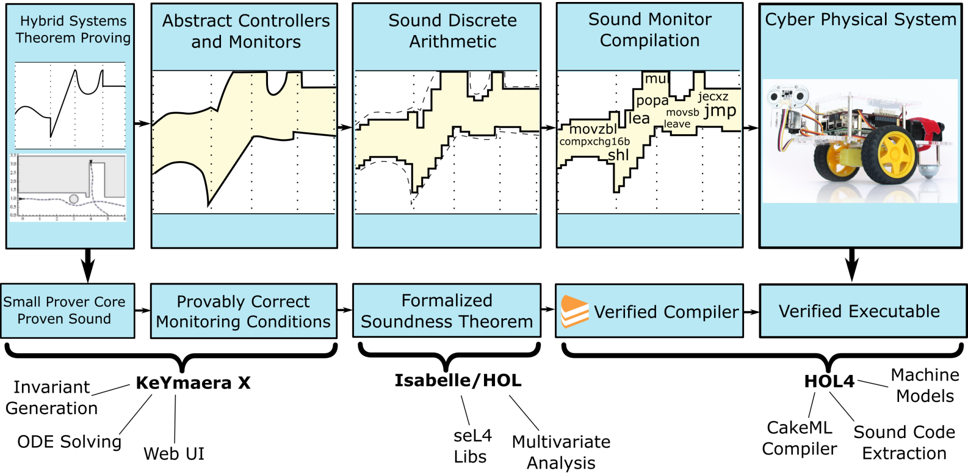
PLDI'18

VeriPhy: Automatic, Verified EXEs from Controllers



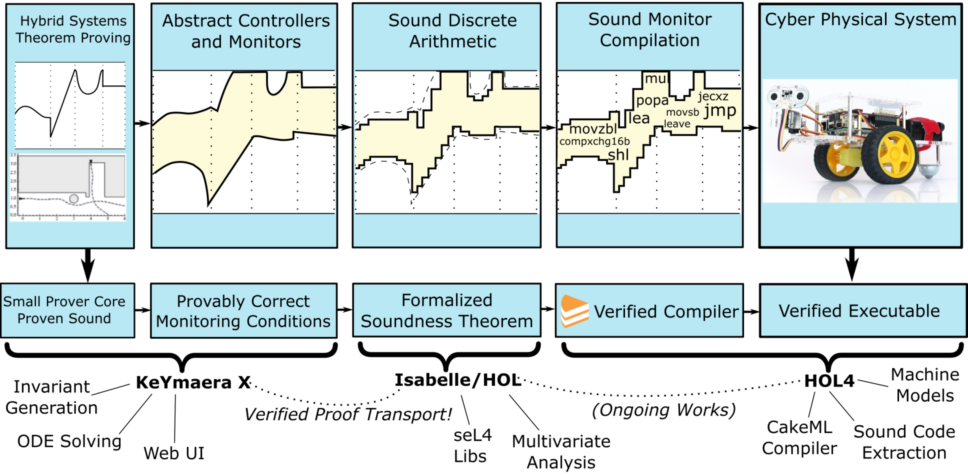
PLDI'18

VeriPhy: Automatic, Verified EXEs from Controllers



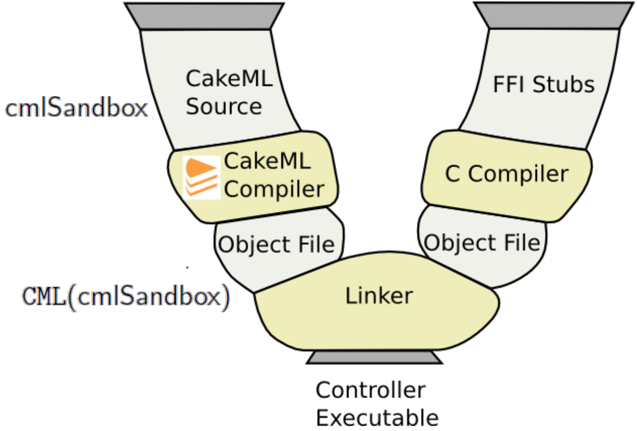
PLDI'18

VeriPhy: Automatic, Verified EXEs from Controllers



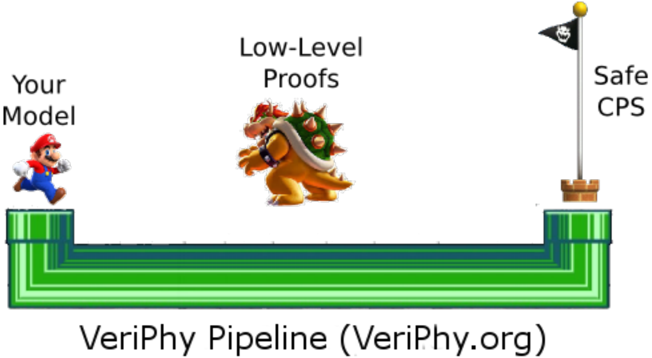
PLDI'18

CakeML Compiler Preserves Guarantees

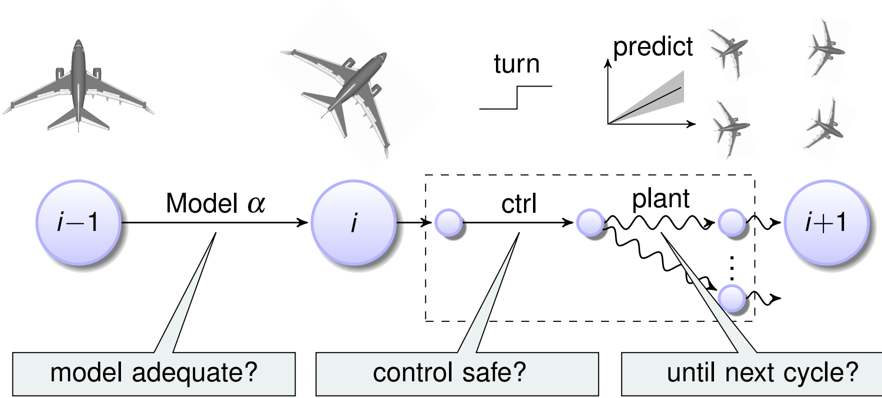


VeriPhy: Takeaway Metaphor

VeriPhy: Takeaway Metaphor



ModelPlex **ensures that verification results** about models **apply to CPS** implementations



FMSD'16

ModelPlex **ensures that verification results** about models **apply to CPS** implementations

Contributions

- Verification results about models transfer to CPS when validating model compliance
- Compliance with model is characterizable in logic
- Compliance formula transformed by proof to monitor
- Correct-by-construction provably correct model validation at runtime

model adequate? | control safe? | until next cycle?

FMSD'16

Provable Monitor ⇝ Provable Sandbox

Sandboxed controller uses external controller when decision is safe, else uses verified fallback. Detects non-compliant plants.

$$\phi \rightarrow [(\mathsf{ctrl};\mathsf{plant})^*]\psi$$

$$\begin{aligned}
&\vec{x} := *;\\
&?\phi;\\
&(\ \vec{x}^+ := \mathsf{extCtrl};\\
&\quad (\ \ ?\mathsf{ctrlMon}(\vec{x},\vec{x}^+)\\
&\quad\ \ \cup \mathsf{fallback}\ );\\
&\quad \vec{x} := \vec{x}^+;\\
&\quad \vec{x}^+ := *;\\
&\quad ?\mathsf{plantMon}(\vec{x},\vec{x}^+);\\
&\quad \vec{x} := \vec{x}^+)^*
\end{aligned}$$

Outline (Programming CPS with Logic)

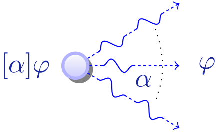
Logical Systems Lab at Carnegie Mellon University
Yong Kiam Tan, Brandon Bohrer, Nathan Fulton, Sarah Loos
Stefan Mitsch, Khalil Ghorbal, Jean-Baptiste Jeannin, Andrew Sogokon

Programming Cyber-Physical Systems With Logic

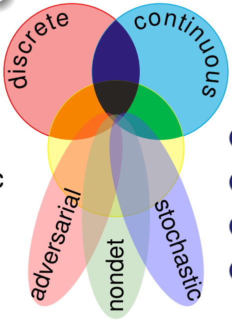
Programming language principles affect CPSs

differential dynamic logic

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



- Multi-dynamical systems
- Hybrid programs + dL logic
- Compositional proofs
- Logic impacts CPS

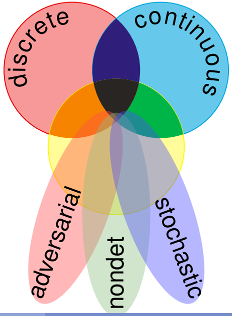


1. Analytic foundations
2. Practical proving
3. Significant applications
4. Bring sciences together

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 FMSD'09 TACAS'14
- Safe AI autonomy in CPS AAAI'18
- 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

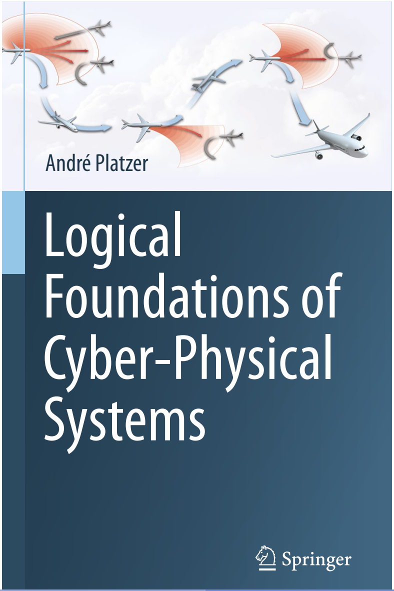
II Part: Differential Equations Analysis

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

9 Appendix
- Soundness and Completeness
- Differentials
- Differential Ghosts
- Differential Radical Invariants

Complete Proof Theory of Hybrid Systems

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

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

Corollary (Complete Proof-theoretical Bridge)

proving continuous = proving hybrid = proving discrete

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

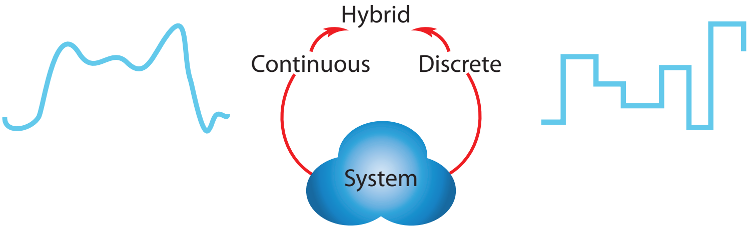
Complete Proof Theory of Hybrid Systems

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

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

Corollary (Complete Proof-theoretical Bridge)

proving continuous = proving hybrid = proving discrete



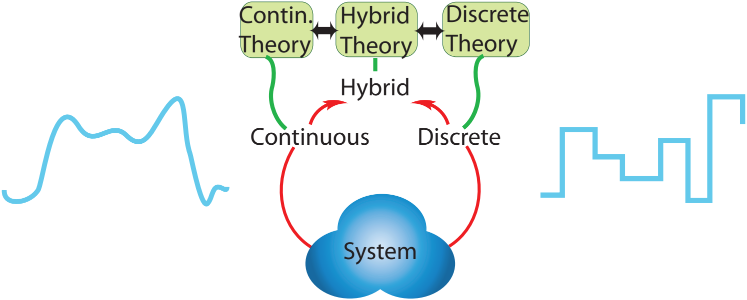
Complete Proof Theory of Hybrid Systems

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

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

Corollary (Complete Proof-theoretical Bridge)

proving continuous = proving hybrid = proving discrete



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

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

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

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

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

ODE

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

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

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

Differential Substitution Lemmas

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

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

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

Lemma (Differential assignment) (Effect on Differentials)

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

Lemma (Derivations) (Equations of Differentials)

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

Differential Substitution Lemmas $\rightsquigarrow$ Proofs

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

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

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

Lemma (Differential assignment) (Effect on Differentials)

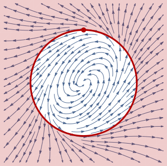
$DE\ [x' = f(x)\,\&\,Q]P \leftrightarrow [x' = f(x)\,\&\,Q][x' := f(x)]P$

Lemma (Derivations) (Equations of Differentials)

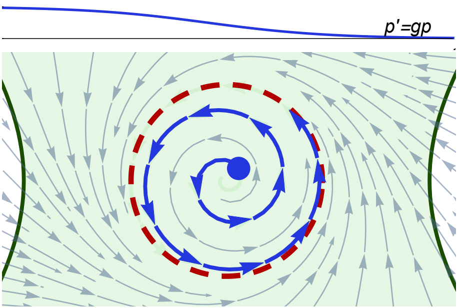
$+'$	$(e+k)' = (e)' + (k)'$
$\cdot'$	$(e \cdot k)' = (e)' \cdot k + e \cdot (k)'$
c'	$(c())' = 0$
x'	$(x)' = x'$

Darboux inequalities are DG

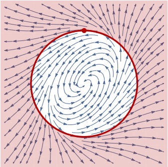
$$\frac{Q \vdash p' \geq gp}{p \succcurlyeq 0 \vdash [x' = f(x) \,\&\, Q]p \succcurlyeq 0} \quad (g \in \mathbb{R}[x])$$



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

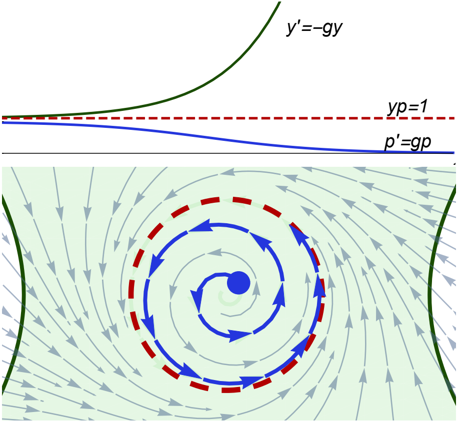


ODE Axiomatization: Derived Darboux Rules



Darboux inequalities are DG

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



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

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

$$*$$

$$\mathbb{R}\quad Q \vdash (-gy)z^2 + y(2z(\tfrac{g}{2}z)) = 0$$

$$\text{dI}\quad yz^2 = 1 \vdash [x' = f(x), y' = -gy, z' = \tfrac{g}{2}z \,\&\, Q]\, yz^2 = 1$$

$$\text{M}[\cdot],\exists\text{R}\quad y > 0 \vdash \exists z\, [x' = f(x), y' = -gy, z' = \tfrac{g}{2}z \,\&\, Q]\, y > 0$$

$$\text{DG}\quad y > 0 \vdash [x' = f(x), y' = -gy \,\&\, Q]\, y > 0$$

$$*$$

$$Q \vdash p' \geq gp \qquad \mathbb{R}\quad p' \geq gp, y > 0 \vdash p'y - gyp \geq 0$$

$$\text{cut}\quad Q, y > 0 \vdash p'y - gyp \geq 0$$

$$\text{dI}\quad p \succcurlyeq 0, y > 0 \vdash [x' = f(x), y' = -gy \,\&\, Q \land y > 0]\, py \succcurlyeq 0 \quad \triangleright$$

$$\text{dC}\quad p \succcurlyeq 0, y > 0 \vdash [x' = f(x), y' = -gy \,\&\, Q](y > 0 \land py \succcurlyeq 0)$$

$$\text{M}[\cdot],\exists\text{R}\quad p \succcurlyeq 0 \vdash \exists y\, [x' = f(x), y' = -gy \,\&\, Q]\, p \succcurlyeq 0$$

$$\text{DG}\quad p \succcurlyeq 0 \vdash [x' = f(x) \,\&\, Q]\, p \succcurlyeq 0$$

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)

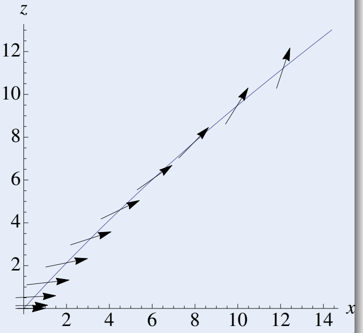
Algebraic invariants of algebraic differential equations are decidable.

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

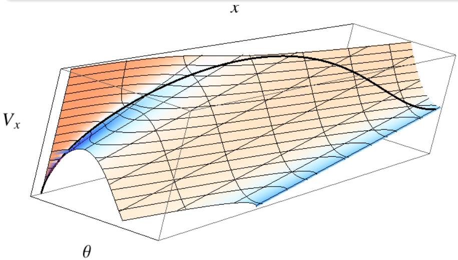
with Khalil Ghorbal TACAS'14

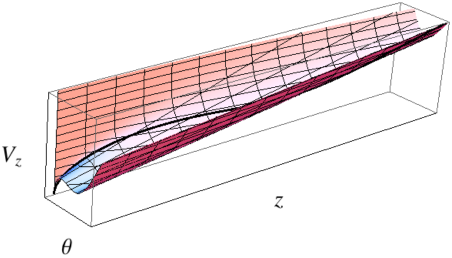
Result (DRI Automatically Generates Invariant Functions)

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

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

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





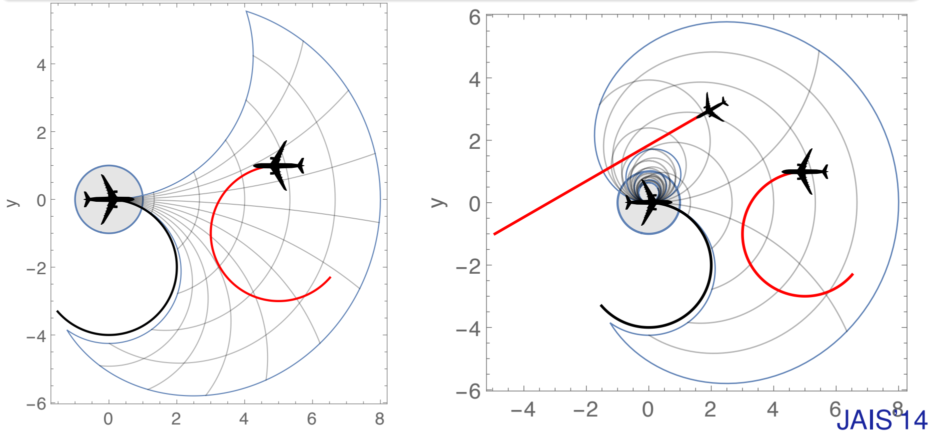
with Khalil Ghorbal TACAS'14

Example: Dubins Dynamics of 2 Airplanes

Result (DRI Automatically Generates Invariants)

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

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



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 [22], 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.

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

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

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

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

André Platzer.
The complete proof theory of hybrid systems.
In LICS [22], 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.

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.