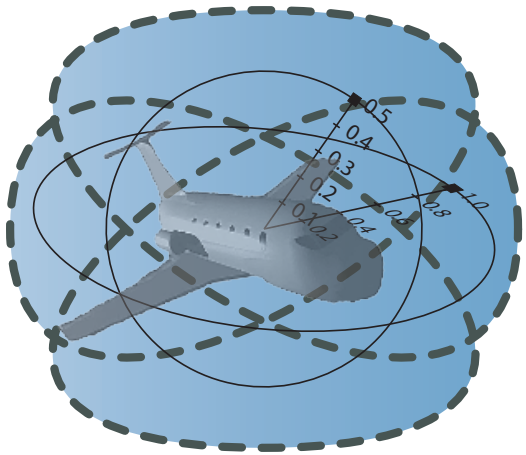
05: Dynamical Systems & Dynamic Axioms

15-424: Foundations of Cyber-Physical Systems

André Platzer

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



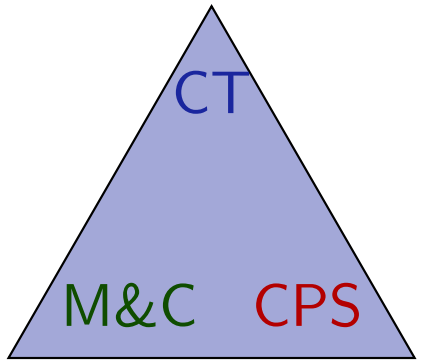
Outline

Outline

Learning Objectives

Dynamical Systems & Dynamic Axioms

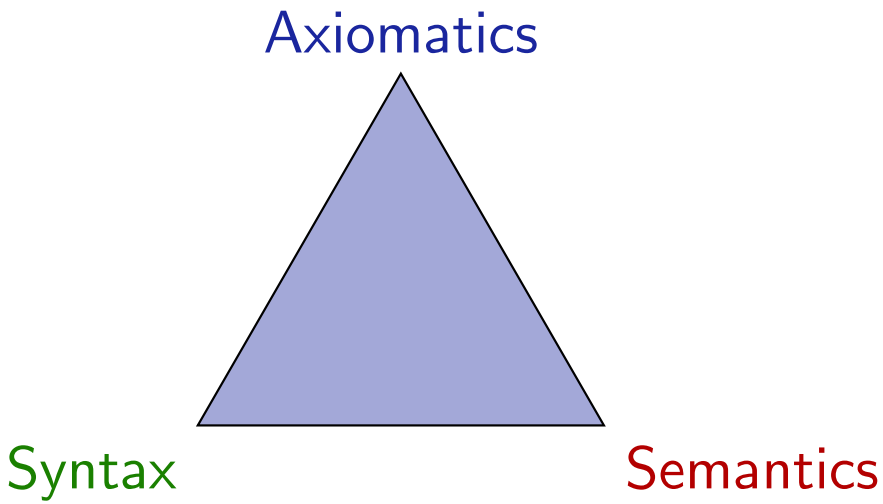
rigorous reasoning about CPS
dL as verification language



cyber+physics interaction
relate discrete+continuous

align semantics+reasoning
operational CPS effects

Logical Trinity



Syntax defines the notation
What problems are we allowed to write down?

Semantics what carries meaning.
What real or mathematical objects does the syntax stand for?

Axiomatics internalizes semantic relations into universal syntactic transformations.
How does the semantics of A relate to semantics of $A \wedge B$, syntactically? If A is true, is $A \wedge B$ true, too? Conversely?

Outline

Approach

Logical guiding principle: Compositionality

1. Every CPS is modeled by a hybrid program (or game . . .)
2. All hybrid programs are combinations of simpler hybrid programs (by a program operator such as $\cup$ and ; and *)
3. All CPS can be analyzed
   if only we identify one suitable analysis technique for each operator.

Outline

Differential Dynamic Logic dL: Semantics

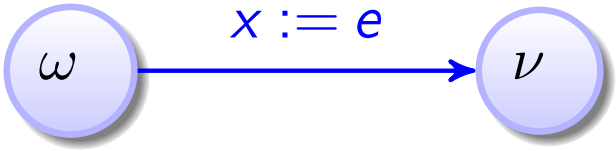
Definition (Hybrid program semantics) $([\![\cdot]\!] : \text{HP} \to \wp(\mathcal{S} \times \mathcal{S}))$

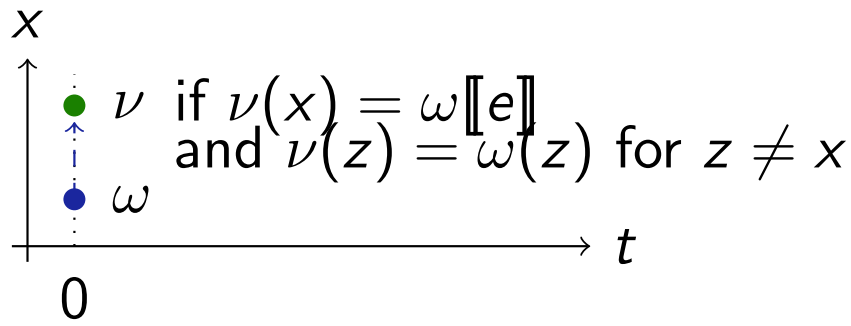
$$
\begin{aligned}
[\![x := e]\!] &= \{(\omega, \nu) \ : \ \nu = \omega \text{ except } \nu[\![x]\!] = \omega[\![e]\!]\} \\
[\![?Q]\!] &= \{(\omega, \omega) \ : \ \omega \in [\![Q]\!]\} \\
[\![x' = f(x)]\!] &= \{(\varphi(0), \varphi(r)) \ : \ \varphi \models x' = f(x) \text{ for some duration } r\} \\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

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

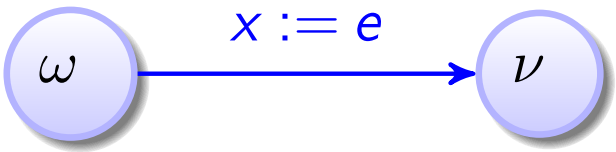
$$
\begin{aligned}
[\![\theta \geq \eta]\!] &= \{\omega \ : \ \omega[\![\theta]\!] \geq \omega[\![\eta]\!]\} \\
[\![\neg\phi]\!] &= ([\![\phi]\!])^{\complement} \\
[\![\phi \wedge \psi]\!] &= [\![\phi]\!] \cap [\![\psi]\!] \\
[\![\langle\alpha\rangle\phi]\!] &= [\![\alpha]\!] \circ [\![\phi]\!] = \{\omega \ : \ \nu \in [\![\phi]\!] \text{ for some } \nu : \ (\omega, \nu) \in [\![\alpha]\!]\} \\
[\![[\alpha]\phi]\!] &= [\![\neg\langle\alpha\rangle\neg\phi]\!] = \{\omega \ : \ \nu \in [\![\phi]\!] \text{ for all } \nu : \ (\omega, \nu) \in [\![\alpha]\!]\} \\
[\![\exists x \, \phi]\!] &= \{\omega \ : \ \omega^r_x \in [\![\phi]\!] \text{ for some } r \in \mathbb{R}\}
\end{aligned}
$$

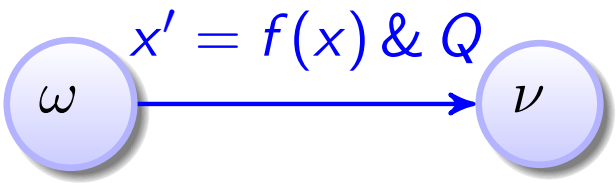
Differential Dynamic Logic dL: Transition Semantics

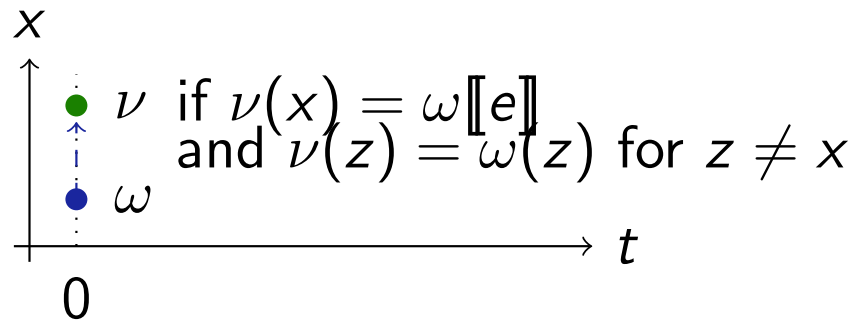


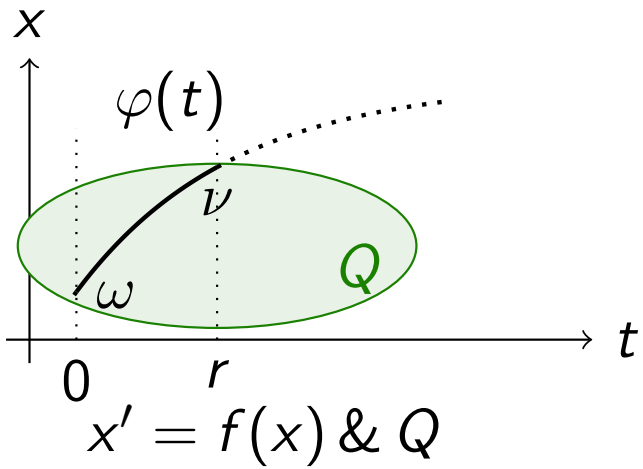


Differential Dynamic Logic dL: Transition Semantics

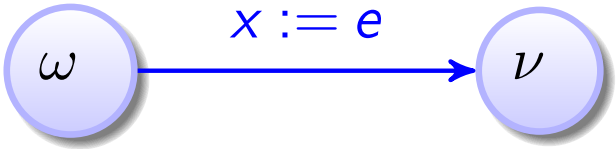


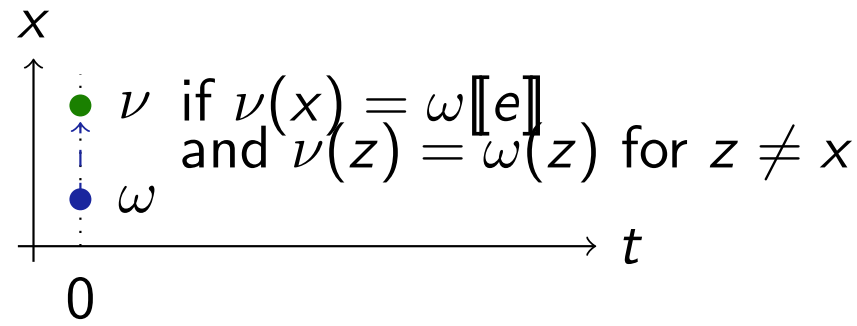


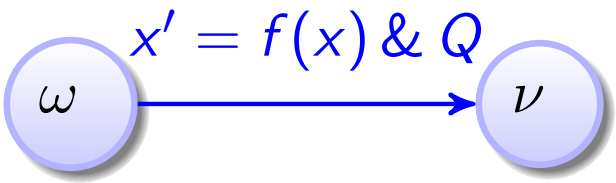


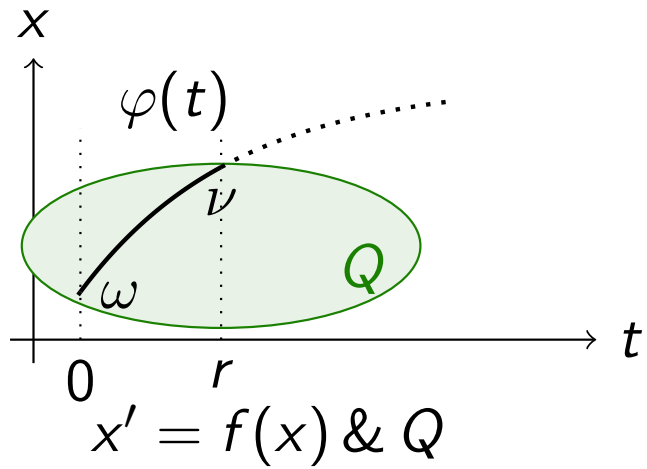


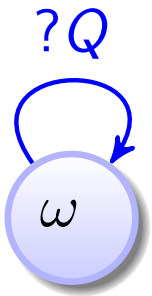
Differential Dynamic Logic dL: Transition Semantics



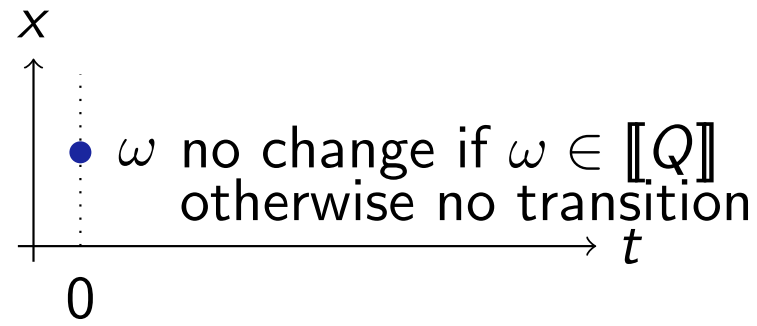




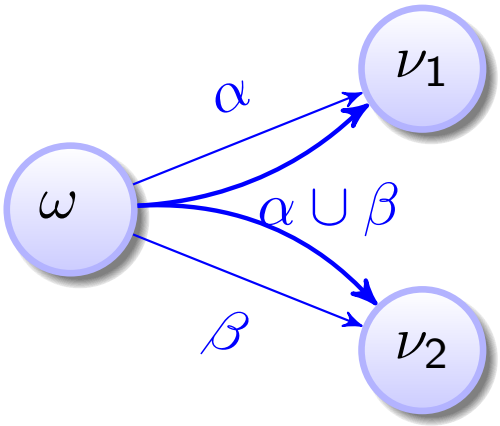


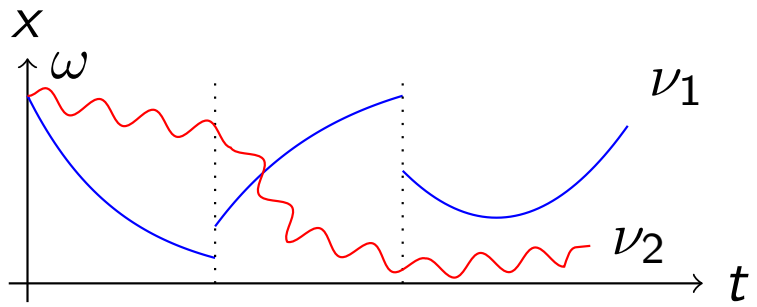


if $\omega \in [\![Q]\!]$

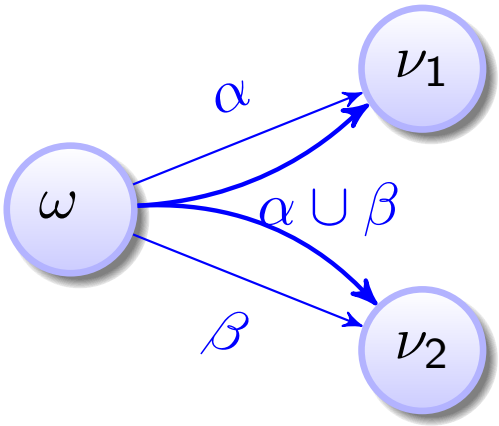


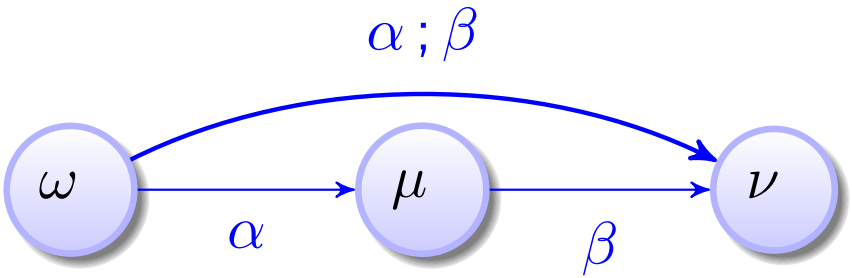
Differential Dynamic Logic dL: Transition Semantics

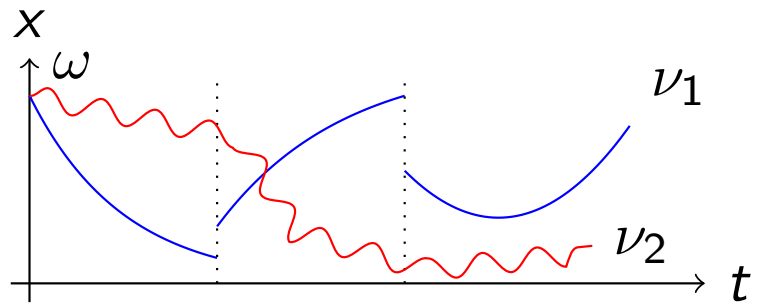


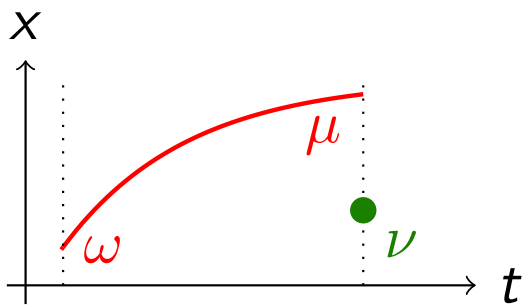


Differential Dynamic Logic dL: Transition Semantics

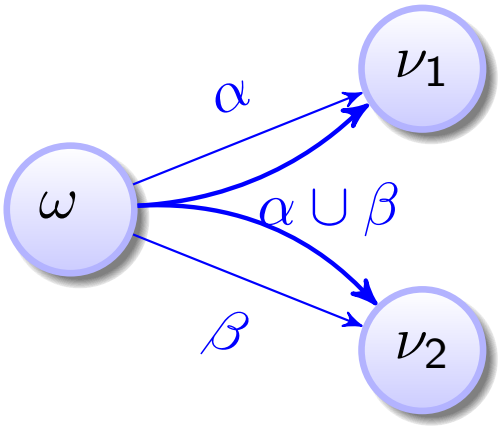


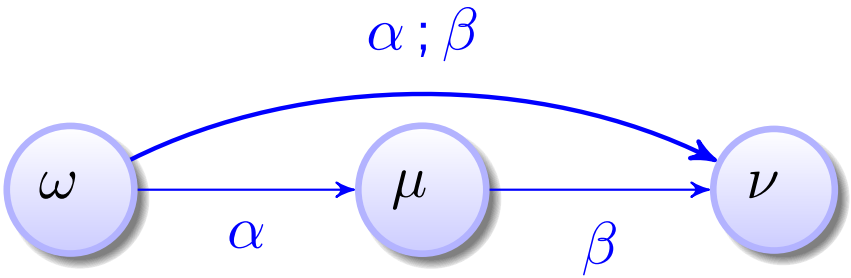


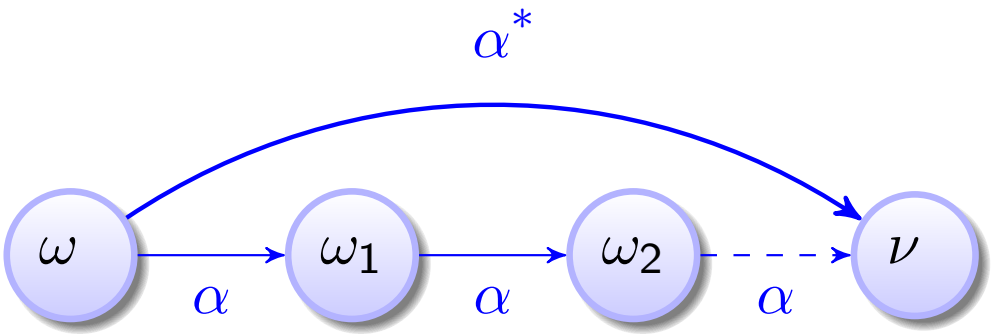


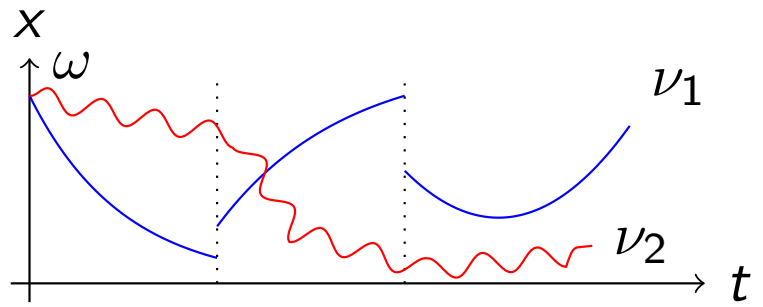


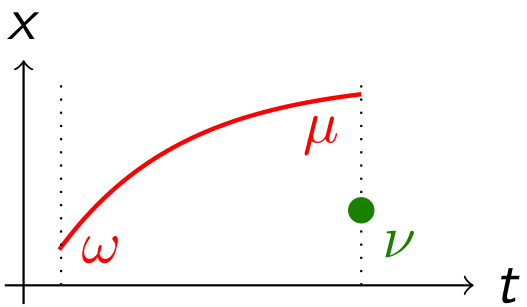
Differential Dynamic Logic dL: Transition Semantics

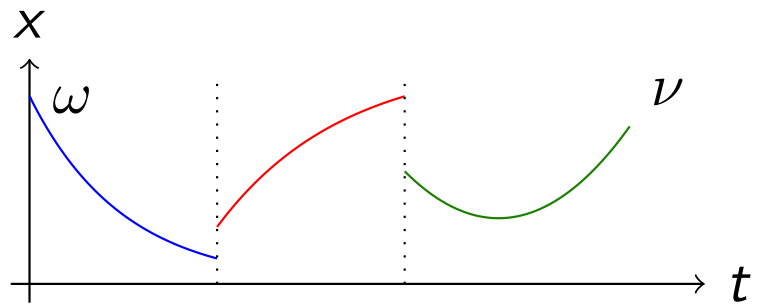




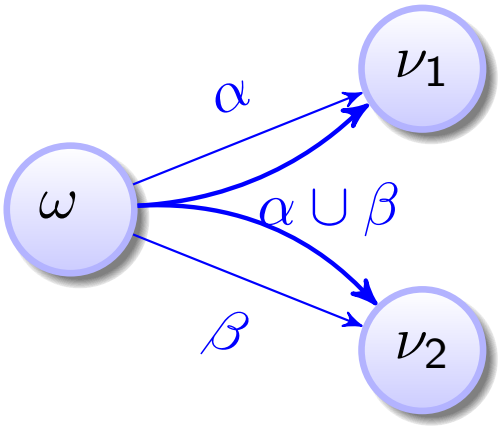


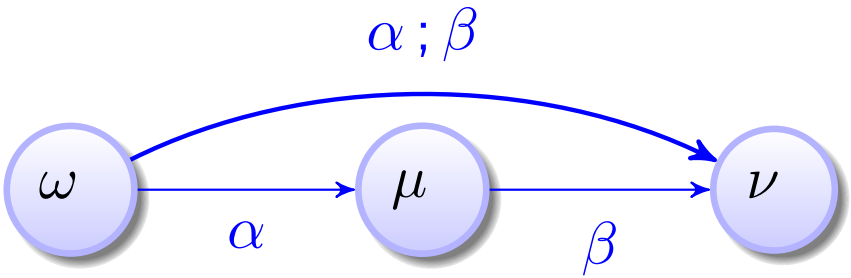


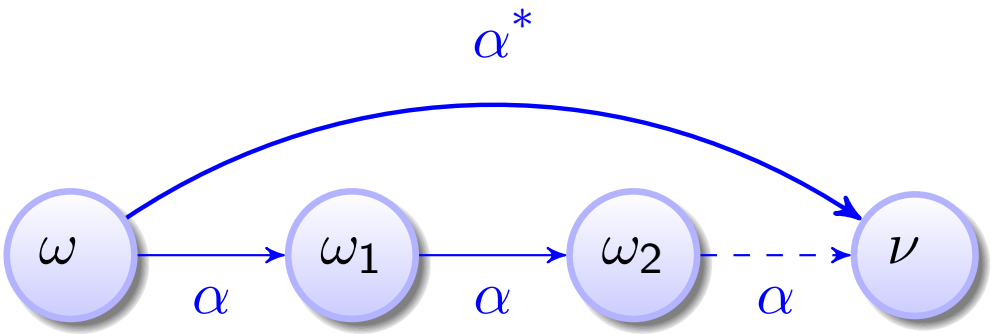


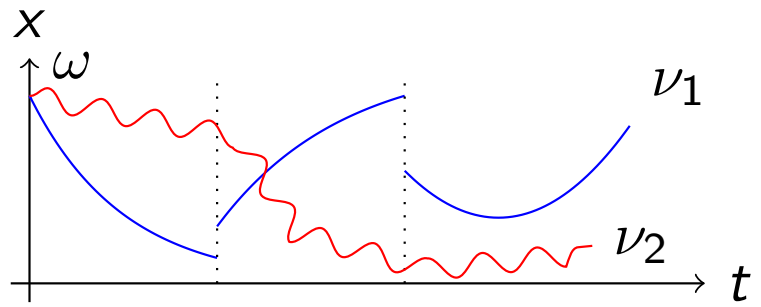


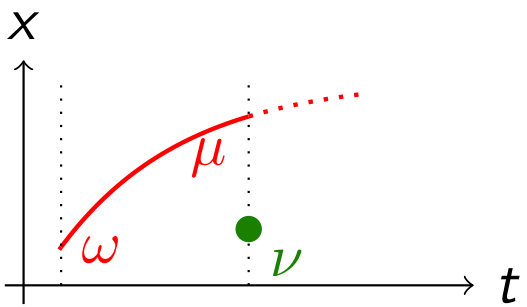
Differential Dynamic Logic dL: Transition Semantics

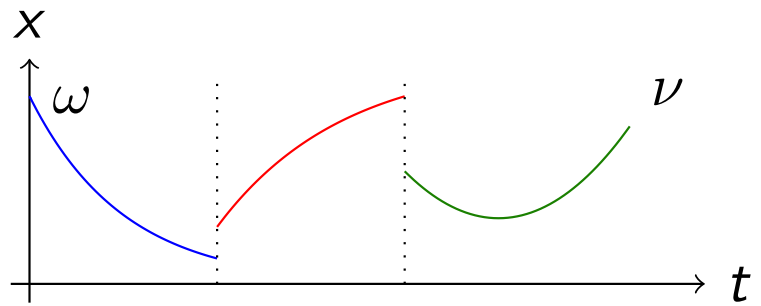




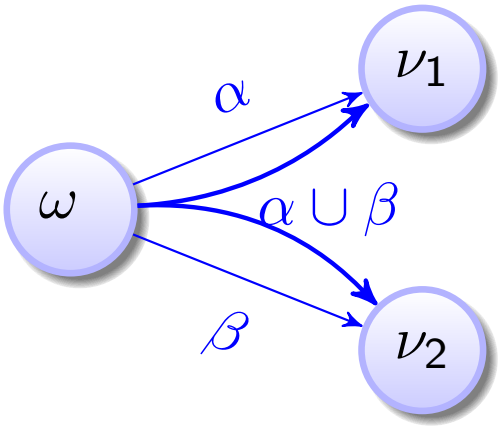


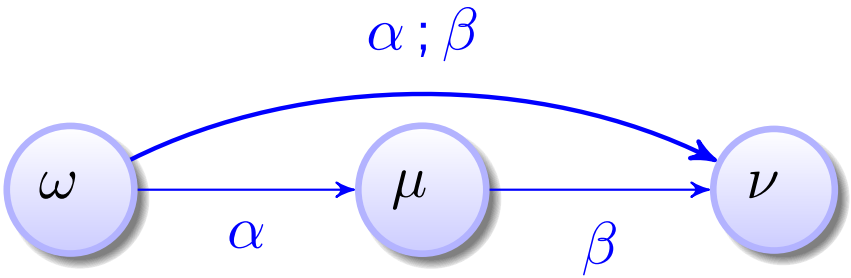


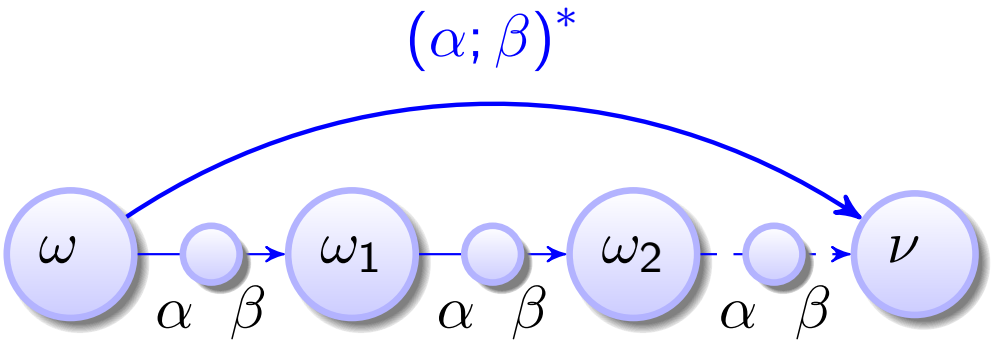


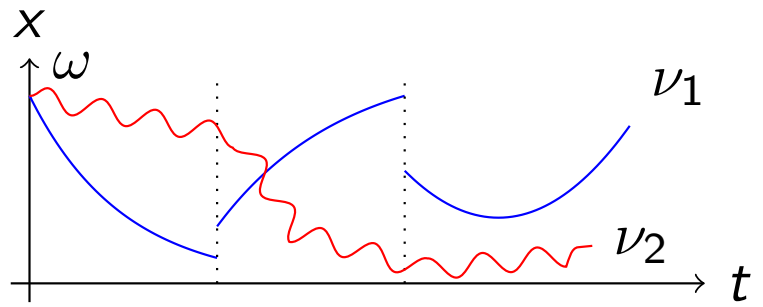


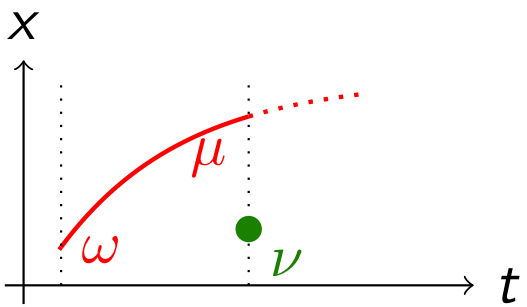
Differential Dynamic Logic dL: Transition Semantics

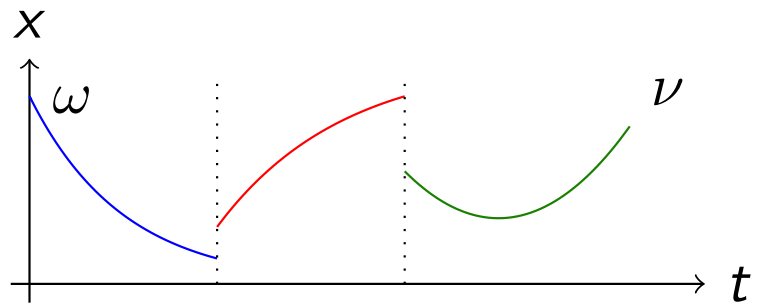






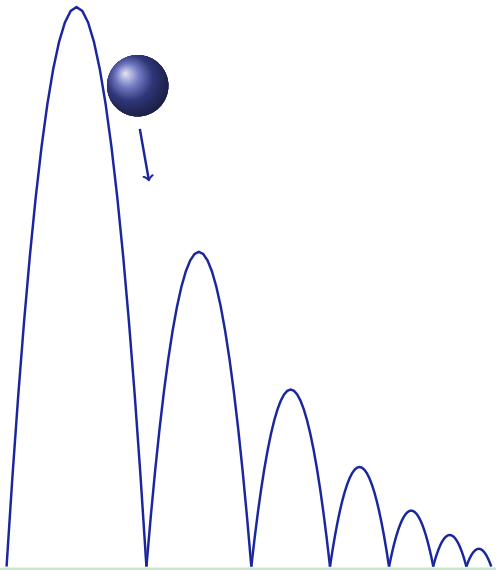






Outline

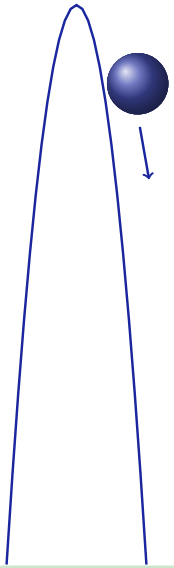
Conjecture: Quantum the Acrophobic Bouncing Ball



Example (Quantum the Bouncing Ball)

$$0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0 \rightarrow$$
$$\left[\left(x' = v, v' = -g \,\&\, x \geq 0; (?x = 0; v := -cv \cup ?x \neq 0)\right)^*\right](0 \leq x \wedge x \leq H)$$

Conjecture: Quantum the Acrophobic Bouncing Ball

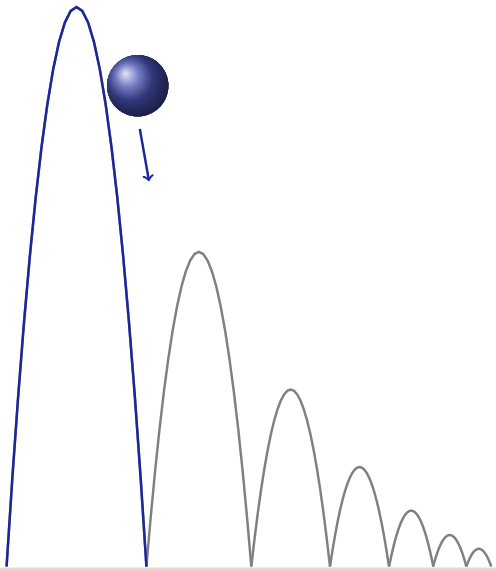


Example (Quantum the Bouncing Ball) (Single-hop)

$$0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0 \rightarrow$$
$$\left[x' = v, v' = -g \,\&\, x \geq 0; (?x = 0; v := -cv \cup ?x \neq 0) \right] (0 \leq x \wedge x \leq H)$$

Removing the repetition grotesquely changes the behavior to a single hop

Conjecture: Quantum the Acrophobic Bouncing Ball



Example (Quantum the Bouncing Ball) (Single-hop)

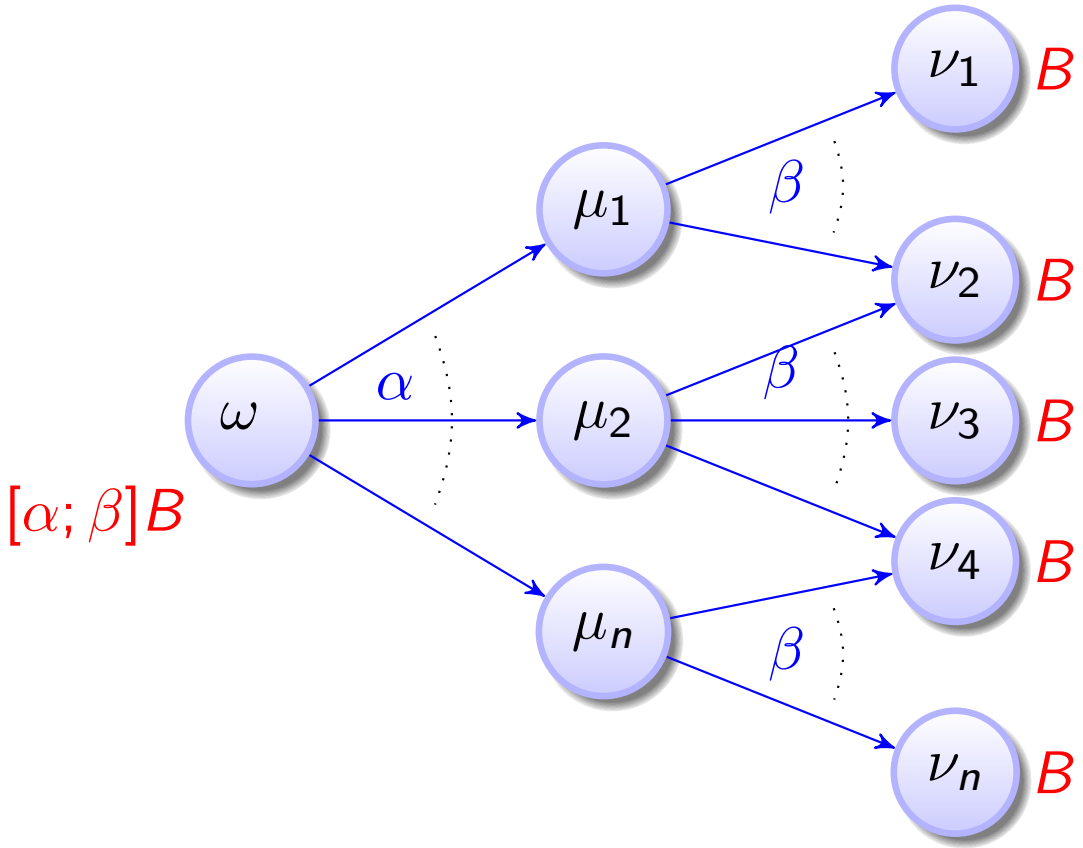
$$0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0 \rightarrow$$
$$\left[\; x' = v, v' = -g \,\&\, x \geq 0; (?x = 0; v := -cv \cup ?x \neq 0) \; \right] (0 \leq x \wedge x \leq H)$$

Removing the repetition grotesquely changes the behavior to a single hop

Outline

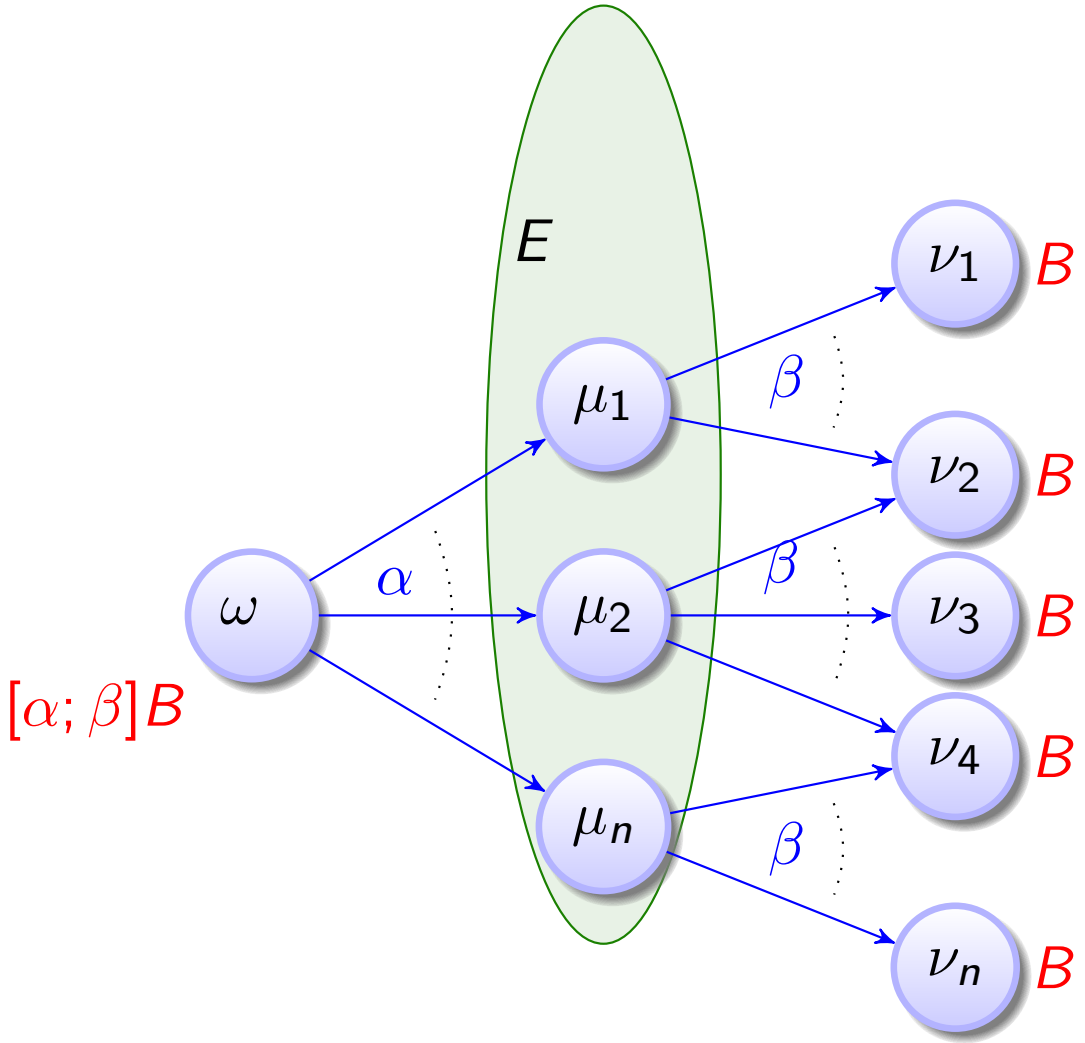
Intermediate Conditions for CPS

HM; $\dfrac{}{A \to [\alpha;\beta]B}$



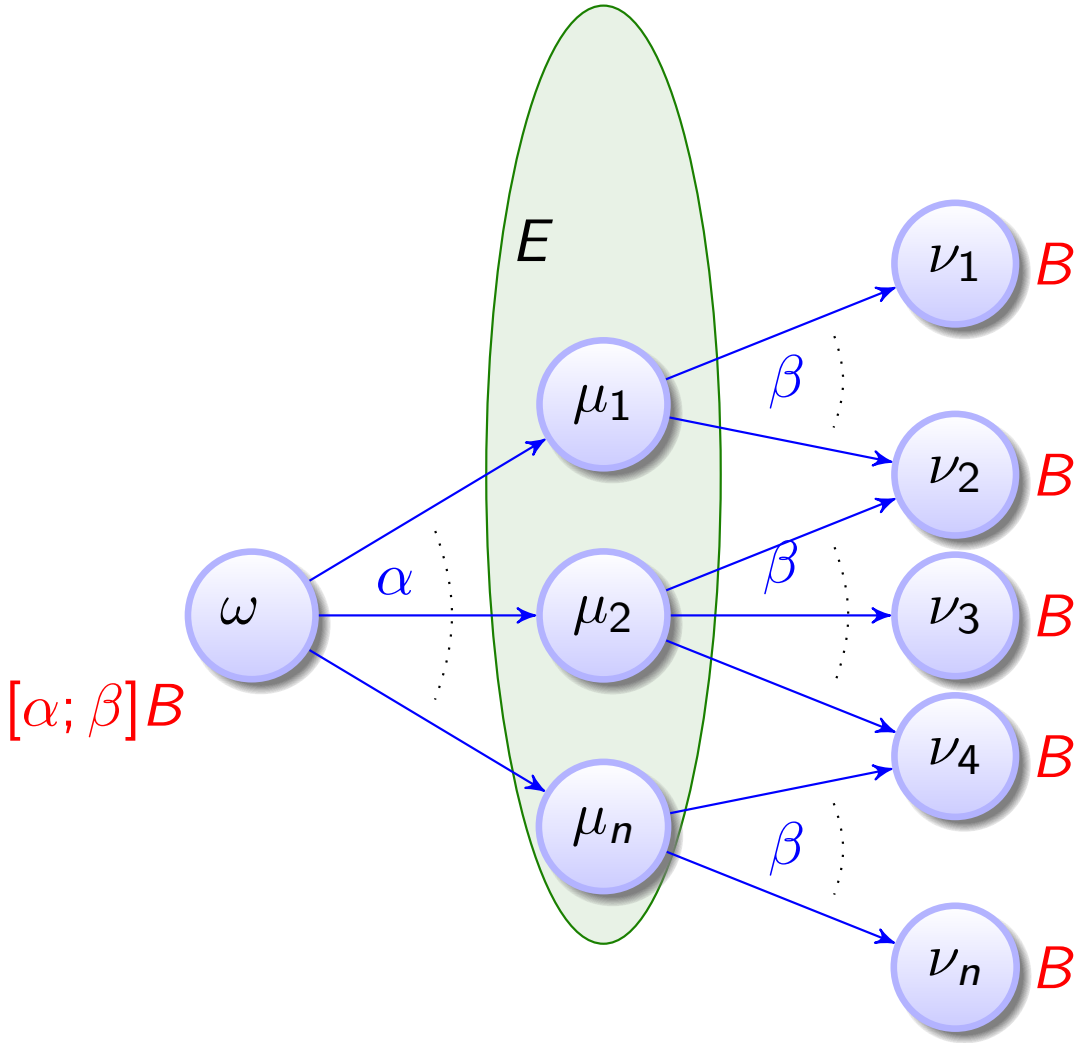
Intermediate Conditions for CPS

HM; $\dfrac{}{A \to [\alpha;\beta]B}$



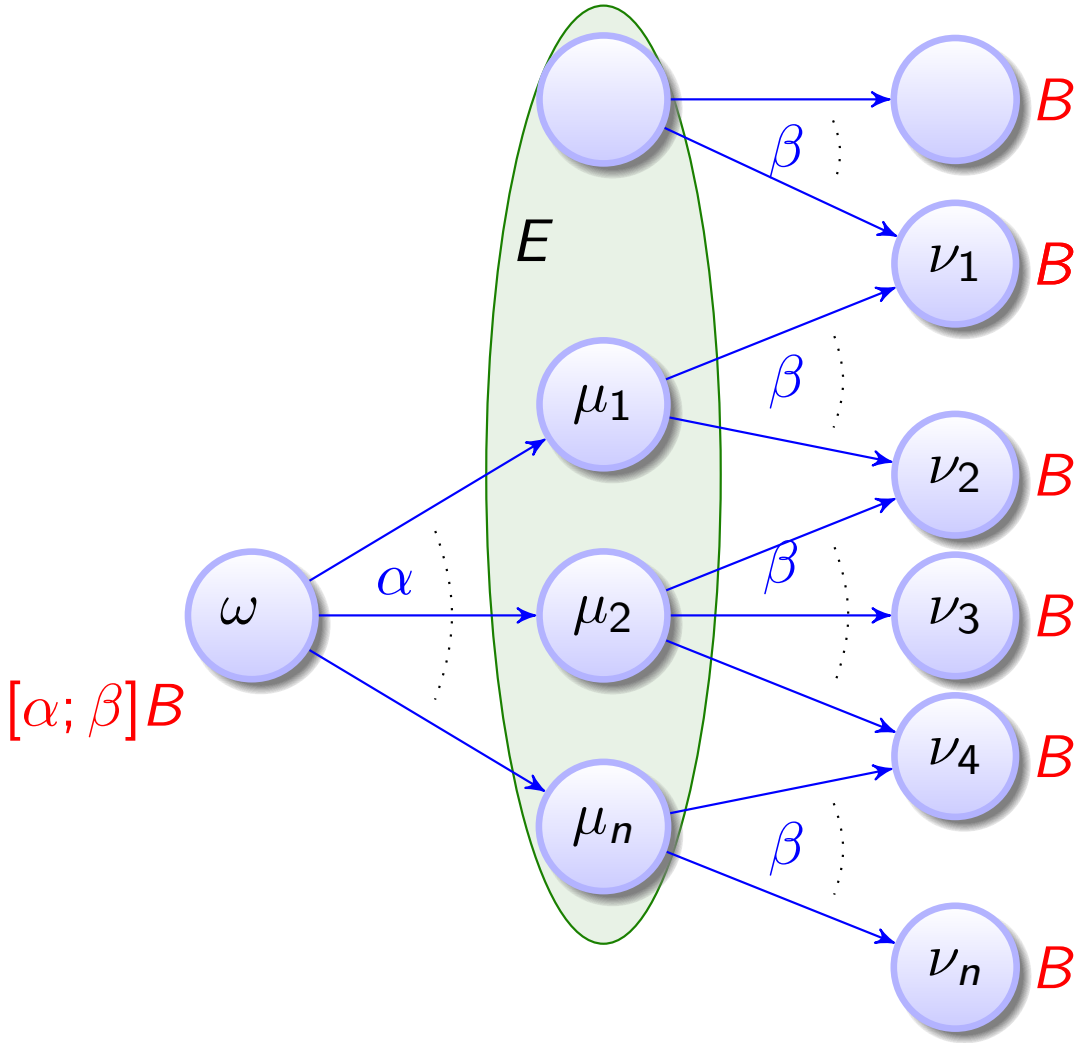
Intermediate Conditions for CPS

HM; $$\frac{A \to [\alpha]E \quad E \to [\beta]B}{A \to [\alpha;\beta]B}$$



Intermediate Conditions for CPS

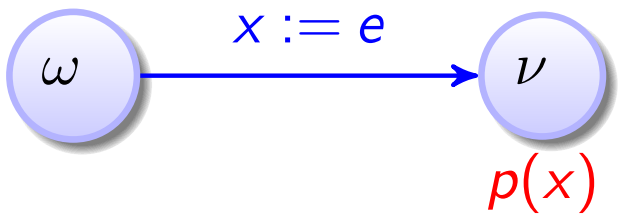
HM; $$\frac{A \to [\alpha]E \quad E \to [\beta]B}{A \to [\alpha;\beta]B}$$



Outline

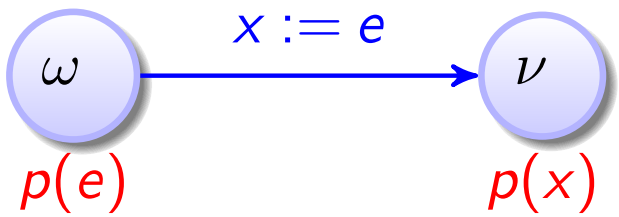
Dynamic Axioms for Dynamical Systems

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



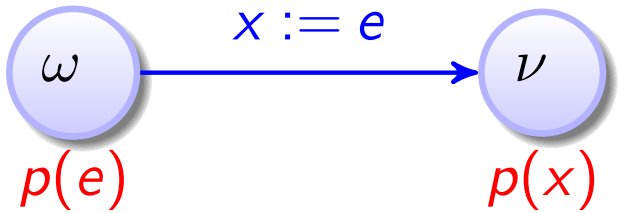
Dynamic Axioms for Dynamical Systems

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

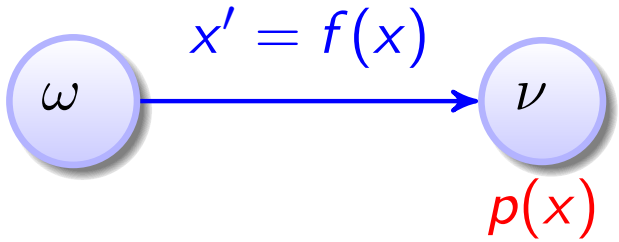


Dynamic Axioms for Dynamical Systems

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

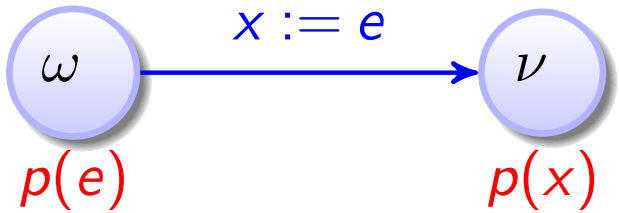


$[']$ $[x' = f(x)]p(x) \leftrightarrow$

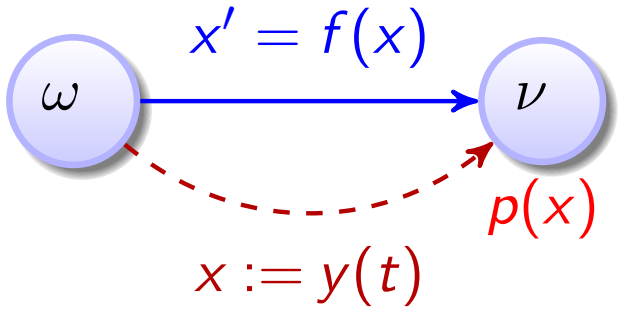


Dynamic Axioms for Dynamical Systems

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



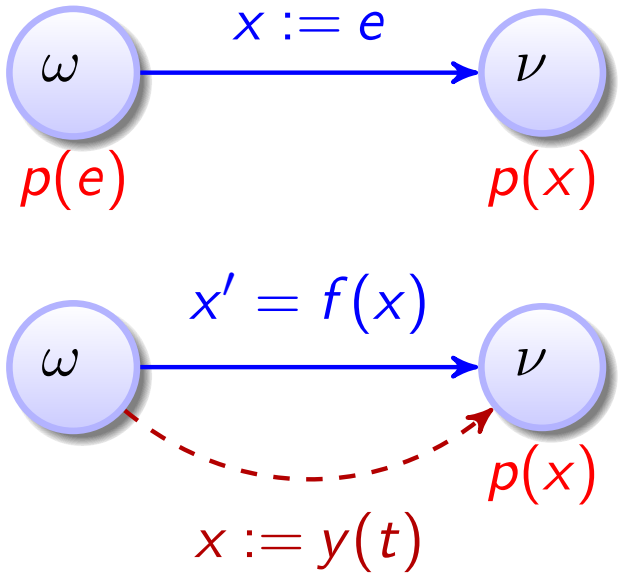
$[']$ $[x' = f(x)]p(x) \leftrightarrow$ $[x := y(t)]p(x)$



Dynamic Axioms for Dynamical Systems

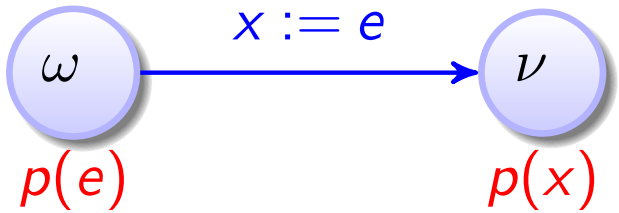
$[:=]$ $[x := e]p(x) \leftrightarrow p(e)$

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

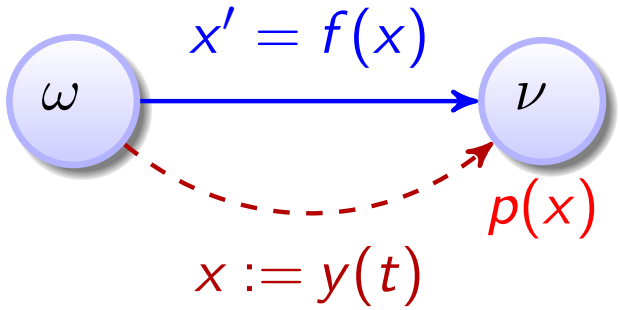


Dynamic Axioms for Dynamical Systems

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



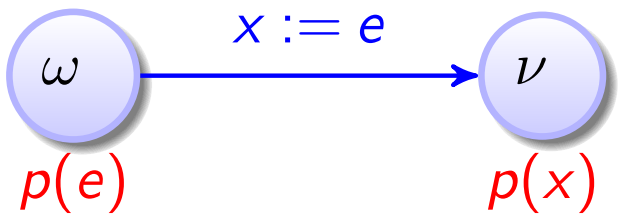
$$['] \quad [x' = f(x)]p(x) \leftrightarrow \forall t{\geq}0[x := y(t)]p(x)$$



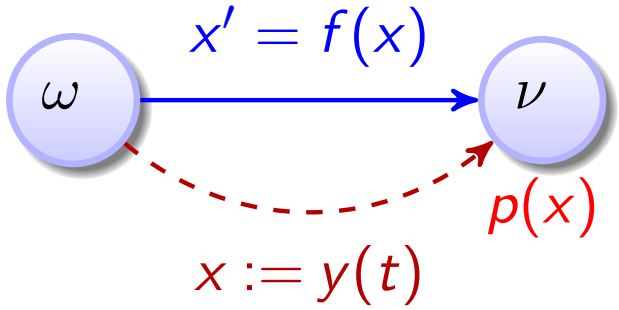
$$['] \quad [x' = f(x) \,\&\, q(x)]p(x) \leftrightarrow \forall t{\geq}0 \left([x := y(t)]p(x)\right)$$

Dynamic Axioms for Dynamical Systems

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



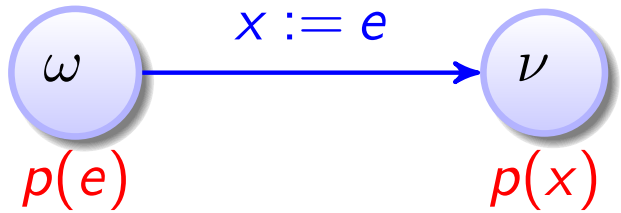
$[']$ $[x' = f(x)]p(x) \leftrightarrow \forall t{\geq}0[x := y(t)]p(x)$



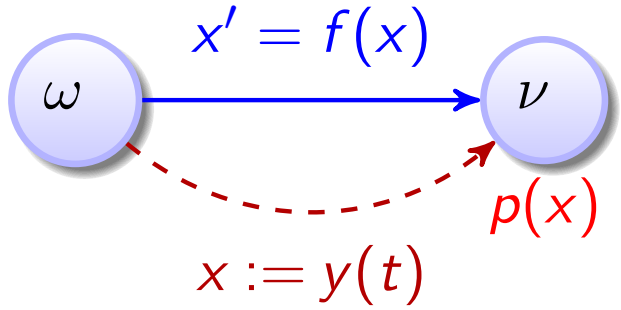
$[']$ $[x' = f(x)\,\&\,q(x)]p(x) \leftrightarrow \forall t{\geq}0\,\big(\forall 0{\leq}s{\leq}t\; q(y(s)) \rightarrow [x := y(t)]p(x)\big)$

Dynamic Axioms for Dynamical Systems

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

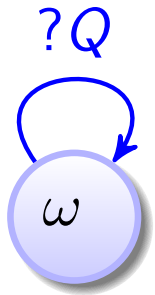


$[']$ $[x' = f(x)]p(x) \leftrightarrow \forall t{\geq}0[x := y(t)]p(x)$



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

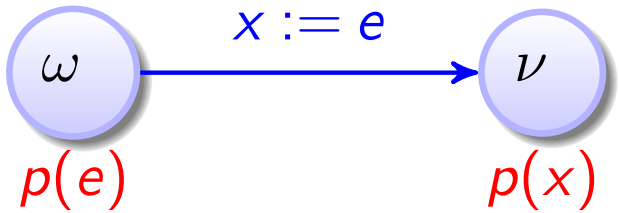
$[?]$ $[?Q]P \leftrightarrow$



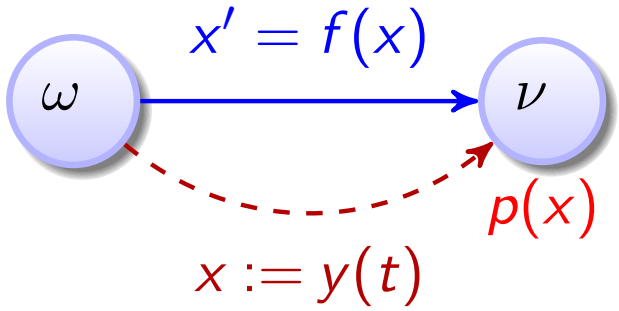
if $\omega \in [\![Q]\!]$

Dynamic Axioms for Dynamical Systems

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

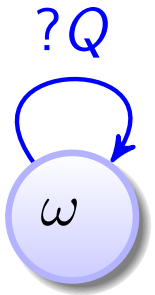


$[']$ $[x' = f(x)]p(x) \leftrightarrow \forall t{\geq}0[x := y(t)]p(x)$



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

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



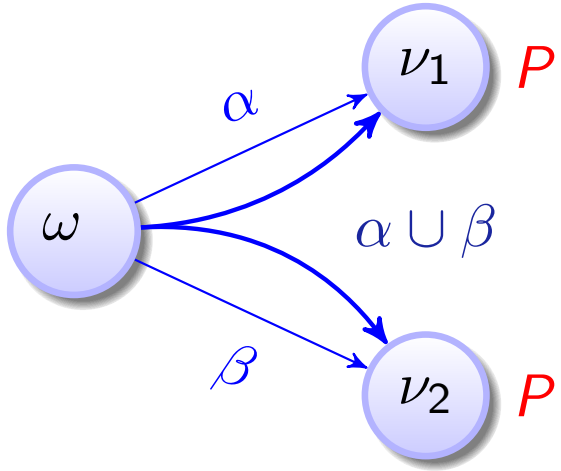
if $\omega \in [\![Q]\!]$

Dynamic Axioms for Dynamical Systems

compositional semantics $\Rightarrow$ compositional rules!

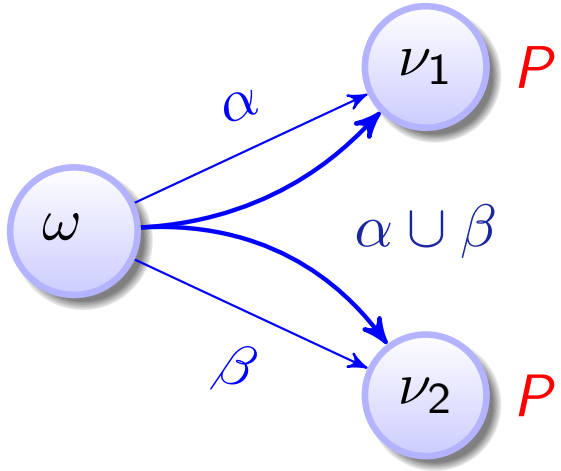
Dynamic Axioms for Dynamical Systems

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



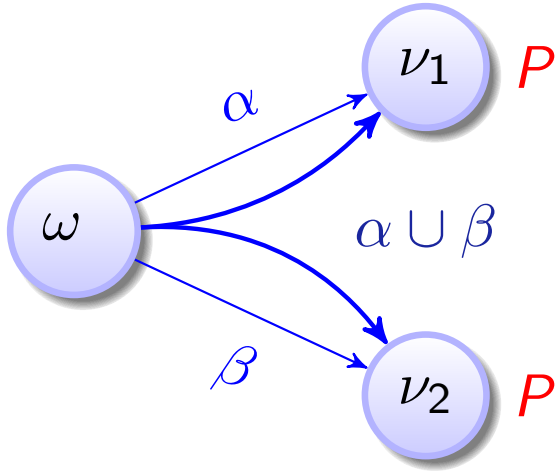
Dynamic Axioms for Dynamical Systems

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

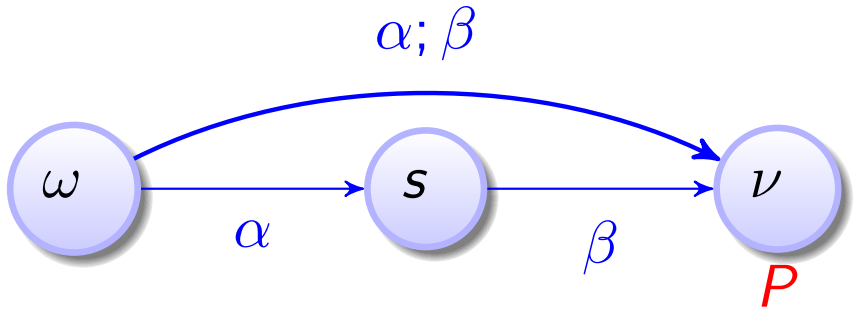


Dynamic Axioms for Dynamical Systems

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

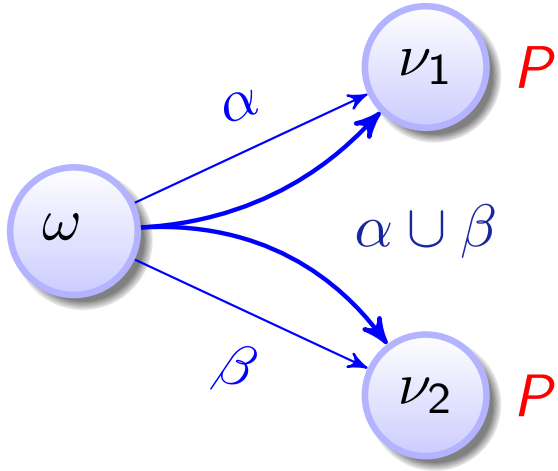


[;] $[\alpha;\beta]P \leftrightarrow$

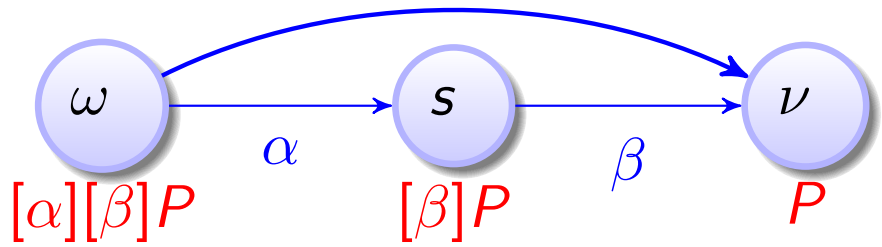


Dynamic Axioms for Dynamical Systems

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

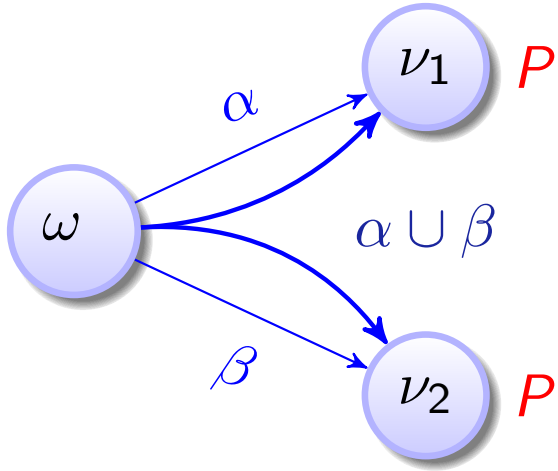


[;] $[\alpha;\beta]P \leftrightarrow [\alpha][\beta]P$

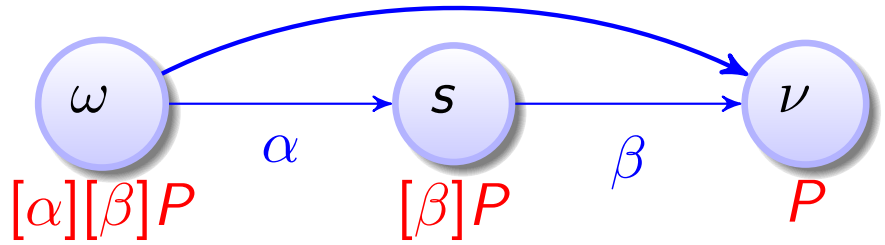


Dynamic Axioms for Dynamical Systems

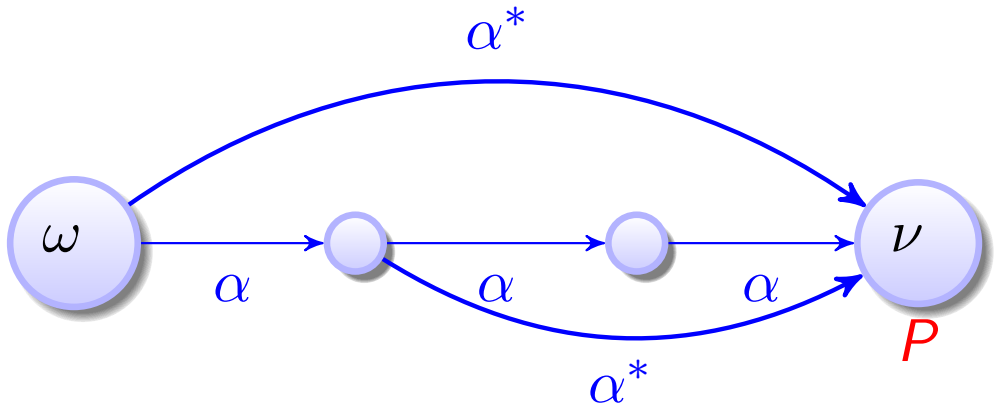
[∪] $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$



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

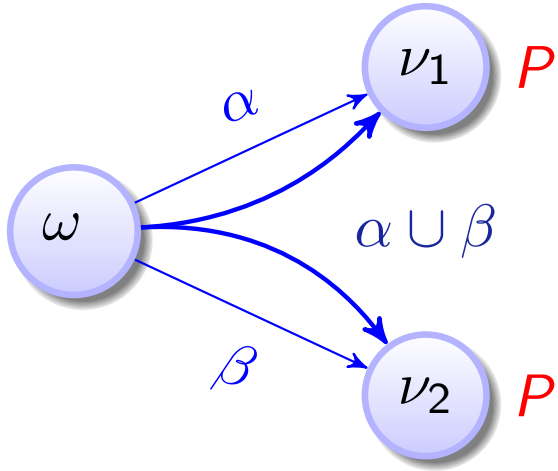


[*] $[\alpha^*]P \leftrightarrow$

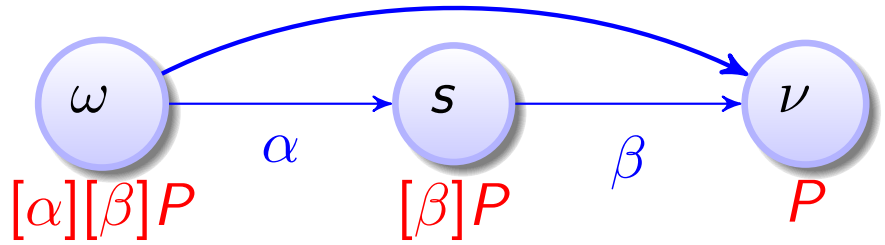


Dynamic Axioms for Dynamical Systems

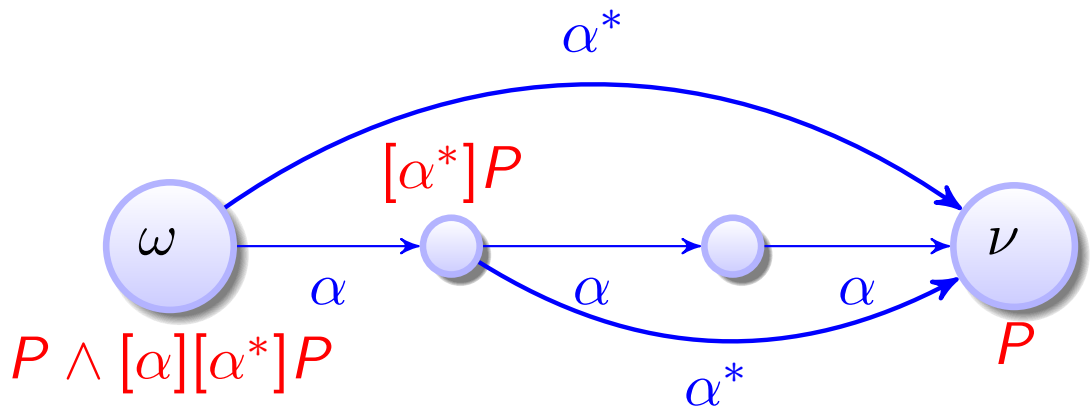
[∪] $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$



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



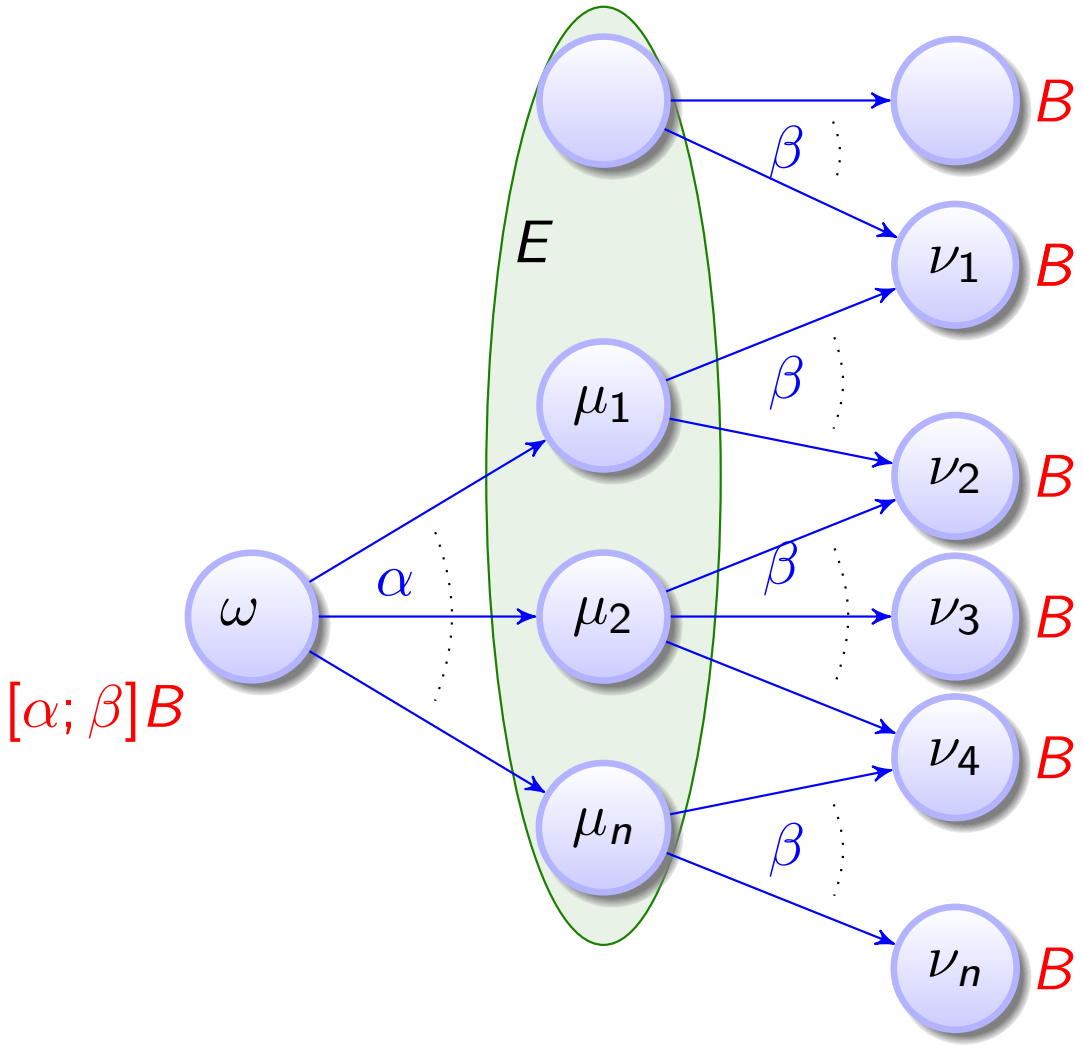
[*] $[\alpha^*]P \leftrightarrow P \wedge [\alpha][\alpha^*]P$



Outline

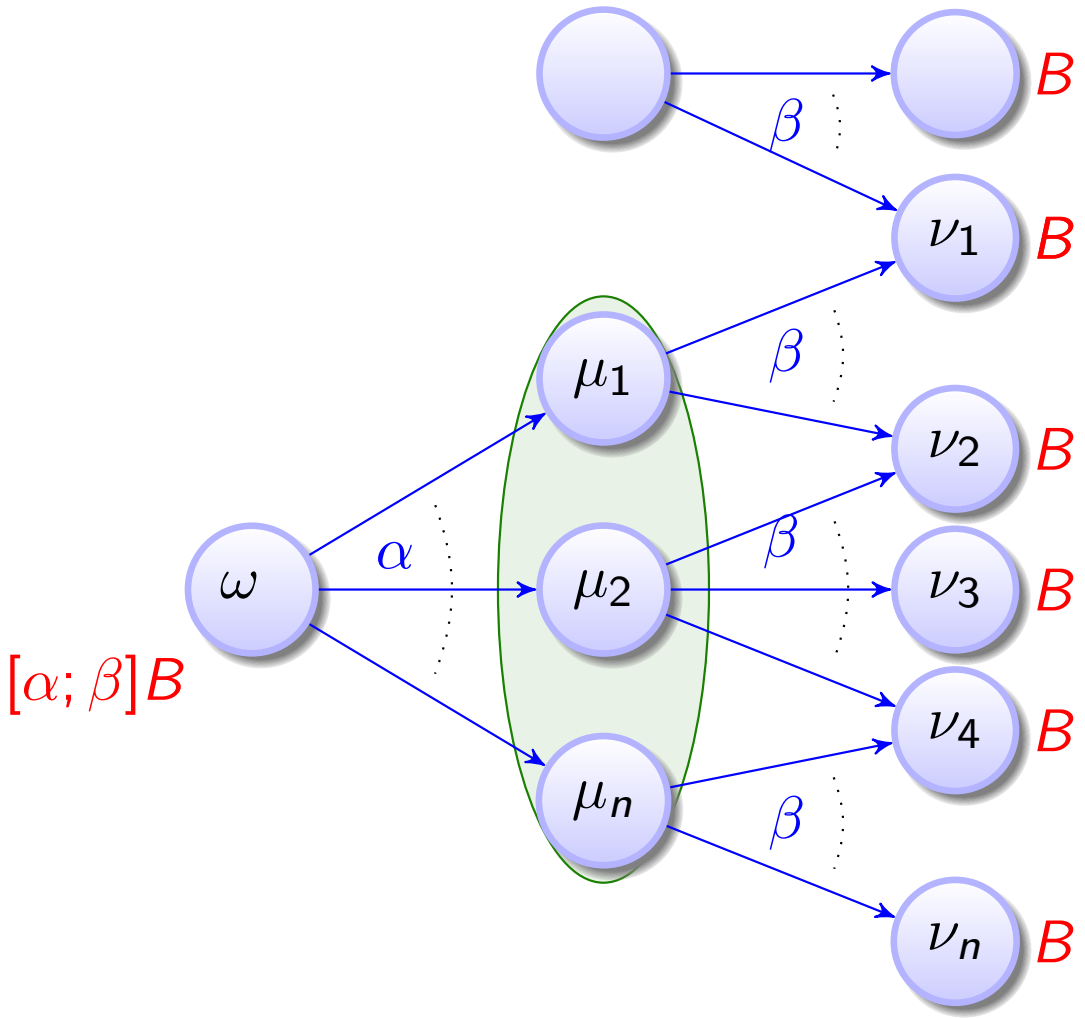
Intermediate Conditions vs. Sequential Compositions

HM; $$\frac{A \to [\alpha]E \quad E \to [\beta]B}{A \to [\alpha;\beta]B}$$



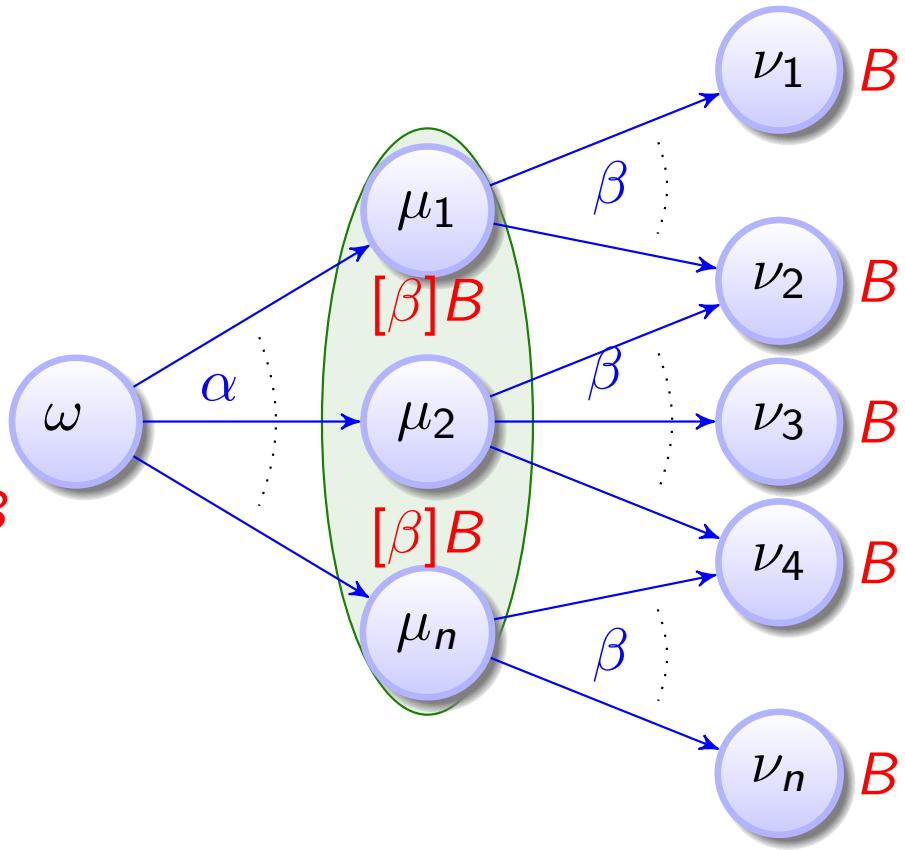
Intermediate Conditions vs. Sequential Compositions

HM; $\dfrac{A \to [\alpha]E \quad E \to [\beta]B}{A \to [\alpha;\beta]B}$



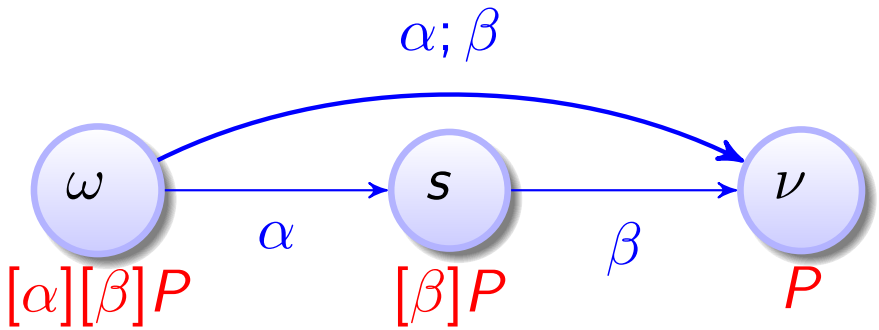
Intermediate Conditions vs. Sequential Compositions

HM; $$\frac{A \to [\alpha][\beta]B \quad [\beta]B \to [\beta]B}{A \to [\alpha;\beta]B}$$

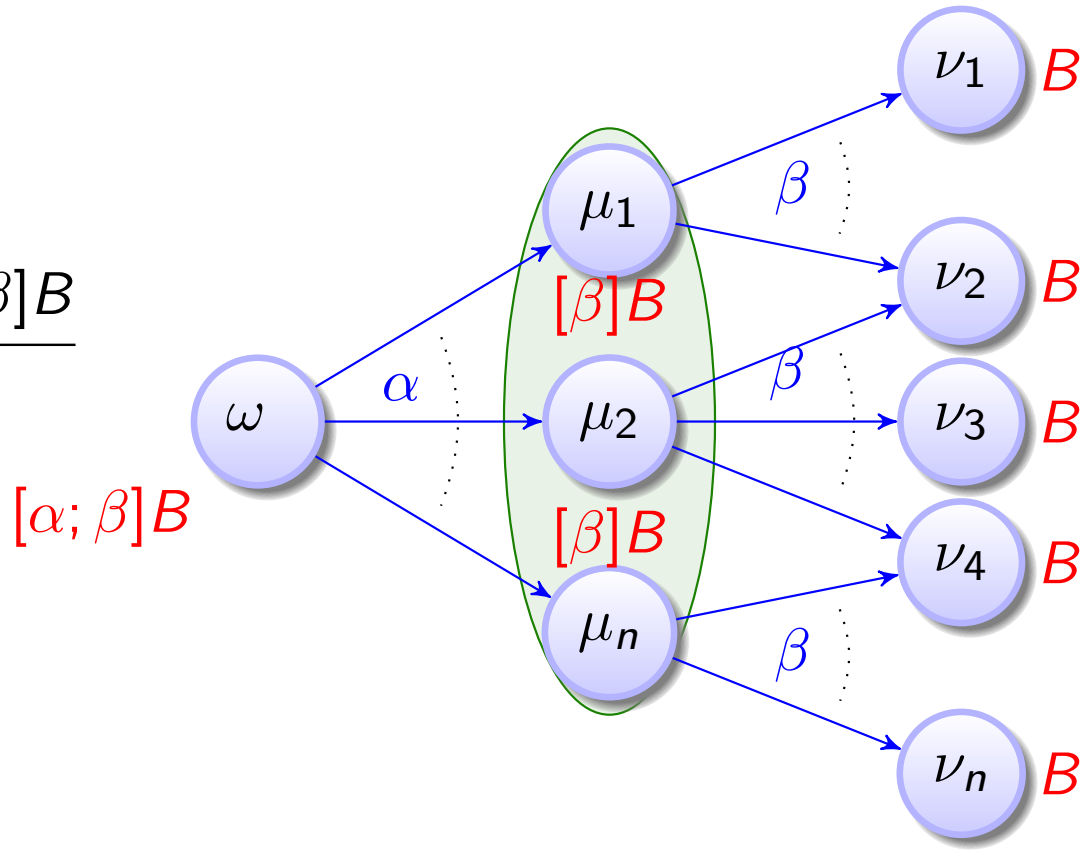


Intermediate Conditions vs. Sequential Compositions

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



HM; $\dfrac{A \to [\alpha][\beta]B \quad [\beta]B \to [\beta]B}{A \to [\alpha;\beta]B}$



Developed on the board:

1. Soundness of axioms
2. Example-driven sketch of single-hop bouncing ball proof

See lecture notes for details [1].

Outline

A Proof of a Short Single-hop Bouncing Ball

$$[;]\ \frac{}{A \vdash [x'' = -g; (?x = 0; v := -cv \cup ?x \geq 0)]B(x,v)}$$

$$A \overset{\text{def}}{\equiv} 0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0$$

$$B(x,v) \overset{\text{def}}{\equiv} 0 \leq x \wedge x \leq H$$

$$(x'' = -g) \overset{\text{def}}{\equiv} (x' = v, v' = -g)$$

A Proof of a Short Single-hop Bouncing Ball

$$[\cup]\ \frac{A \vdash [x'' = -g][?x = 0; v := -cv \cup ?x \geq 0]B(x,v)}{A \vdash [x'' = -g; (?x = 0; v := -cv \cup ?x \geq 0)]B(x,v)}\ [;]$$

$$A \overset{\text{def}}{\equiv} 0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0$$

$$B(x,v) \overset{\text{def}}{\equiv} 0 \leq x \wedge x \leq H$$

$$(x'' = -g) \overset{\text{def}}{\equiv} (x' = v, v' = -g)$$

A Proof of a Short Single-hop Bouncing Ball

$$\dfrac{\dfrac{\dfrac{}{A \vdash [x'' = -g]\big([?x = 0; v := -cv]B(x,v) \wedge [?x \geq 0]B(x,v)\big)}[;]}{A \vdash [x'' = -g][?x = 0; v := -cv \cup ?x \geq 0]B(x,v)}[\cup]}{A \vdash [x'' = -g; (?x = 0; v := -cv \cup ?x \geq 0)]B(x,v)}[;]$$

$$A \overset{\text{def}}{\equiv} 0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0$$

$$B(x,v) \overset{\text{def}}{\equiv} 0 \leq x \wedge x \leq H$$

$$(x'' = -g) \overset{\text{def}}{\equiv} (x' = v, v' = -g)$$

A Proof of a Short Single-hop Bouncing Ball

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \vdash [x'' = -g]\big([?x = 0][v := -cv]B(x,v) \wedge [?x \geq 0]B(x,v)\big)}[?],[?]}{A \vdash [x'' = -g]\big([?x = 0; v := -cv]B(x,v) \wedge [?x \geq 0]B(x,v)\big)}[;]}{A \vdash [x'' = -g][?x = 0; v := -cv \cup ?x \geq 0]B(x,v)}[\cup]}{A \vdash [x'' = -g; (?x = 0; v := -cv \cup ?x \geq 0)]B(x,v)}[;]$$

$$A \overset{\text{def}}{\equiv} 0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0$$

$$B(x,v) \overset{\text{def}}{\equiv} 0 \leq x \wedge x \leq H$$

$$(x'' = -g) \overset{\text{def}}{\equiv} (x' = v, v' = -g)$$

A Proof of a Short Single-hop Bouncing Ball

$$
\begin{array}{ll}
[:=] & \dfrac{}{A \vdash [x'' = -g]\big((x = 0 \to [v := -cv]B(x,v)) \land (x \geq 0 \to B(x,v))\big)} \\
[?],[?] & \dfrac{}{A \vdash [x'' = -g]\big([?x = 0][v := -cv]B(x,v) \land [?x \geq 0]B(x,v)\big)} \\
[;] & \dfrac{}{A \vdash [x'' = -g]\big([?x = 0; v := -cv]B(x,v) \land [?x \geq 0]B(x,v)\big)} \\
[\cup] & \dfrac{}{A \vdash [x'' = -g][?x = 0; v := -cv \cup ?x \geq 0]B(x,v)} \\
[;] & \dfrac{}{A \vdash [x'' = -g; (?x = 0; v := -cv \cup ?x \geq 0)]B(x,v)}
\end{array}
$$

$$A \overset{\text{def}}{\equiv} 0 \leq x \land x = H \land v = 0 \land g > 0 \land 1 \geq c \geq 0$$

$$B(x,v) \overset{\text{def}}{\equiv} 0 \leq x \land x \leq H$$

$$(x'' = -g) \overset{\text{def}}{\equiv} (x' = v, v' = -g)$$

A Proof of a Short Single-hop Bouncing Ball

$$
\begin{array}{ll}
['] & \dfrac{}{A \vdash [x'' = -g]\big((x = 0 \to B(x,-cv)) \wedge (x \geq 0 \to B(x,v))\big)} \\[2ex]
[:=] & \dfrac{A \vdash [x'' = -g]\big((x = 0 \to [v := -cv]B(x,v)) \wedge (x \geq 0 \to B(x,v))\big)}{A \vdash [x'' = -g]\big((x = 0 \to [v := -cv]B(x,v)) \wedge (x \geq 0 \to B(x,v))\big)} \\[2ex]
[?],[?] & \dfrac{A \vdash [x'' = -g]\big([?x = 0][v := -cv]B(x,v) \wedge [?x \geq 0]B(x,v)\big)}{A \vdash [x'' = -g]\big((x = 0 \to [v := -cv]B(x,v)) \wedge (x \geq 0 \to B(x,v))\big)} \\[2ex]
[;] & \dfrac{A \vdash [x'' = -g]\big([?x = 0; v := -cv]B(x,v) \wedge [?x \geq 0]B(x,v)\big)}{A \vdash [x'' = -g]\big([?x = 0][v := -cv]B(x,v) \wedge [?x \geq 0]B(x,v)\big)} \\[2ex]
[\cup] & \dfrac{A \vdash [x'' = -g][?x = 0; v := -cv \cup ?x \geq 0]B(x,v)}{A \vdash [x'' = -g]\big([?x = 0; v := -cv]B(x,v) \wedge [?x \geq 0]B(x,v)\big)} \\[2ex]
[;] & \dfrac{A \vdash [x'' = -g; (?x = 0; v := -cv \cup ?x \geq 0)]B(x,v)}{A \vdash [x'' = -g][?x = 0; v := -cv \cup ?x \geq 0]B(x,v)}
\end{array}
$$

$$A \overset{\text{def}}{\equiv} 0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0$$

$$B(x,v) \overset{\text{def}}{\equiv} 0 \leq x \wedge x \leq H$$

$$(x'' = -g) \overset{\text{def}}{\equiv} (x' = v, v' = -g)$$

A Proof of a Short Single-hop Bouncing Ball

$$
\begin{array}{ll}
[;] & \dfrac{A \vdash \forall t{\geq}0\,[x := H - \frac{g}{2}t^2; v := -gt]\big((x{=}0 \to B(x,-cv)) \wedge (x{\geq}0 \to B(x,v))\big)}{A \vdash [x'' = -g]\big((x = 0 \to B(x,-cv)) \wedge (x \geq 0 \to B(x,v))\big)} \\
['] & \dfrac{A \vdash [x'' = -g]\big((x = 0 \to [v := -cv]B(x,v)) \wedge (x \geq 0 \to B(x,v))\big)}{A \vdash [x'' = -g]\big([?x = 0][v := -cv]B(x,v) \wedge [?x \geq 0]B(x,v)\big)} \\
[:=] & \dfrac{A \vdash [x'' = -g]\big([?x = 0; v := -cv]B(x,v) \wedge [?x \geq 0]B(x,v)\big)}{A \vdash [x'' = -g][?x = 0; v := -cv \cup ?x \geq 0]B(x,v)} \\
[?],[?] & \dfrac{A \vdash [x'' = -g][?x = 0; v := -cv \cup ?x \geq 0)]B(x,v)}{A \vdash [x'' = -g; (?x = 0; v := -cv \cup ?x \geq 0)]B(x,v)} \\
[;] & \\
[\cup] & \\
[;] &
\end{array}
$$

$$A \overset{\text{def}}{\equiv} 0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0$$

$$B(x,v) \overset{\text{def}}{\equiv} 0 \leq x \wedge x \leq H$$

$$(x'' = -g) \overset{\text{def}}{\equiv} (x' = v, v' = -g)$$

A Proof of a Short Single-hop Bouncing Ball

$$
\begin{array}{ll}
[:=] & \dfrac{A \vdash \forall t{\geq}0\,[x := H - \frac{g}{2}t^2][v := -gt]\big((x{=}0 \to B_{(x,-cv)}) \wedge (x{\geq}0 \to B_{(x,v)})\big)}{} \\
[;] & \dfrac{A \vdash \forall t{\geq}0\,[x := H - \frac{g}{2}t^2; v := -gt]\big((x{=}0 \to B_{(x,-cv)}) \wedge (x{\geq}0 \to B_{(x,v)})\big)}{} \\
['] & \dfrac{A \vdash [x'' = -g]\big((x = 0 \to B_{(x,-cv)}) \wedge (x \geq 0 \to B_{(x,v)})\big)}{} \\
[:=] & \dfrac{A \vdash [x'' = -g]\big((x = 0 \to [v := -cv]B_{(x,v)}) \wedge (x \geq 0 \to B_{(x,v)})\big)}{} \\
[?],[?] & \dfrac{A \vdash [x'' = -g]\big([?x = 0][v := -cv]B_{(x,v)} \wedge [?x \geq 0]B_{(x,v)}\big)}{} \\
[;] & \dfrac{A \vdash [x'' = -g]\big([?x = 0; v := -cv]B_{(x,v)} \wedge [?x \geq 0]B_{(x,v)}\big)}{} \\
[\cup] & \dfrac{A \vdash [x'' = -g][?x = 0; v := -cv \cup ?x \geq 0]B_{(x,v)}}{} \\
[;] & \dfrac{A \vdash [x'' = -g; (?x = 0; v := -cv \cup ?x \geq 0)]B_{(x,v)}}{}
\end{array}
$$

$$A \overset{\text{def}}{\equiv} 0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0$$

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

$$(x'' = -g) \overset{\text{def}}{\equiv} (x' = v, v' = -g)$$

A Proof of a Short Single-hop Bouncing Ball

$$[:=]\ \frac{A \vdash \forall t{\geq}0\,[x := H - \frac{g}{2}t^2]\big((x{=}0 \to B_{(x,-c(-gt))}) \wedge (x{\geq}0 \to B_{(x,-gt)})\big)}{A \vdash \forall t{\geq}0\,[x := H - \frac{g}{2}t^2][v := -gt]\big((x{=}0 \to B_{(x,-cv)}) \wedge (x{\geq}0 \to B_{(x,v)})\big)}$$

$$[;]\ \frac{A \vdash \forall t{\geq}0\,[x := H - \frac{g}{2}t^2; v := -gt]\big((x{=}0 \to B_{(x,-cv)}) \wedge (x{\geq}0 \to B_{(x,v)})\big)}{A \vdash \forall t{\geq}0\,[x := H - \frac{g}{2}t^2; v := -gt]\big((x{=}0 \to B_{(x,-cv)}) \wedge (x{\geq}0 \to B_{(x,v)})\big)}$$

$$[']\ \frac{A \vdash [x'' = -g]\big((x = 0 \to B_{(x,-cv)}) \wedge (x \geq 0 \to B_{(x,v)})\big)}{A \vdash \forall t{\geq}0\,[x := H - \frac{g}{2}t^2; v := -gt]\big((x{=}0 \to B_{(x,-cv)}) \wedge (x{\geq}0 \to B_{(x,v)})\big)}$$

$$[:=]\ \frac{A \vdash [x'' = -g]\big((x = 0 \to [v := -cv]B_{(x,v)}) \wedge (x \geq 0 \to B_{(x,v)})\big)}{A \vdash [x'' = -g]\big((x = 0 \to B_{(x,-cv)}) \wedge (x \geq 0 \to B_{(x,v)})\big)}$$

$$[?],[?]\ \frac{A \vdash [x'' = -g]\big([?x = 0][v := -cv]B_{(x,v)} \wedge [?x \geq 0]B_{(x,v)}\big)}{A \vdash [x'' = -g]\big((x = 0 \to [v := -cv]B_{(x,v)}) \wedge (x \geq 0 \to B_{(x,v)})\big)}$$

$$[;]\ \frac{A \vdash [x'' = -g]\big([?x = 0; v := -cv]B_{(x,v)} \wedge [?x \geq 0]B_{(x,v)}\big)}{A \vdash [x'' = -g]\big([?x = 0][v := -cv]B_{(x,v)} \wedge [?x \geq 0]B_{(x,v)}\big)}$$

$$[\cup]\ \frac{A \vdash [x'' = -g][?x = 0; v := -cv \cup ?x \geq 0]B_{(x,v)}}{A \vdash [x'' = -g]\big([?x = 0; v := -cv]B_{(x,v)} \wedge [?x \geq 0]B_{(x,v)}\big)}$$

$$[;]\ \frac{A \vdash [x'' = -g; (?x = 0; v := -cv \cup ?x \geq 0)]B_{(x,v)}}{A \vdash [x'' = -g][?x = 0; v := -cv \cup ?x \geq 0]B_{(x,v)}}$$

$$A \overset{\text{def}}{\equiv} 0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0$$

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

$$(x'' = -g) \overset{\text{def}}{\equiv} (x' = v, v' = -g)$$

A Proof of a Short Single-hop Bouncing Ball

$$\frac{A \vdash \forall t{\geq}0\,\big((H-\frac{g}{2}t^2{=}0 \to B(H-\frac{g}{2}t^2,-c(-gt))) \wedge (H-\frac{g}{2}t^2{\geq}0 \to B(H-\frac{g}{2}t^2,-gt))\big)}{A \vdash \forall t{\geq}0\,[x := H-\frac{g}{2}t^2]\big((x{=}0 \to B(x,-c(-gt))) \wedge (x{\geq}0 \to B(x,-gt))\big)}\,[:=]$$

$$\frac{A \vdash \forall t{\geq}0\,[x := H-\frac{g}{2}t^2][v := -gt]\big((x{=}0 \to B(x,-cv)) \wedge (x{\geq}0 \to B(x,v))\big)}{A \vdash \forall t{\geq}0\,[x := H-\frac{g}{2}t^2; v := -gt]\big((x{=}0 \to B(x,-cv)) \wedge (x{\geq}0 \to B(x,v))\big)}\,[;]$$

$$\frac{A \vdash [x'' = -g]\big((x = 0 \to B(x,-cv)) \wedge (x \geq 0 \to B(x,v))\big)}{A \vdash \forall t{\geq}0\,[x := H-\frac{g}{2}t^2; v := -gt]\big((x{=}0 \to B(x,-cv)) \wedge (x{\geq}0 \to B(x,v))\big)}\,[']$$

$$\frac{A \vdash [x'' = -g]\big((x = 0 \to [v := -cv]B(x,v)) \wedge (x \geq 0 \to B(x,v))\big)}{A \vdash [x'' = -g]\big((x = 0 \to B(x,-cv)) \wedge (x \geq 0 \to B(x,v))\big)}\,[:=]$$

$$\frac{A \vdash [x'' = -g]\big([?x = 0][v := -cv]B(x,v) \wedge [?x \geq 0]B(x,v)\big)}{A \vdash [x'' = -g]\big((x = 0 \to [v := -cv]B(x,v)) \wedge (x \geq 0 \to B(x,v))\big)}\,[?],[?]$$

$$\frac{A \vdash [x'' = -g]\big([?x = 0; v := -cv]B(x,v) \wedge [?x \geq 0]B(x,v)\big)}{A \vdash [x'' = -g]\big([?x = 0][v := -cv]B(x,v) \wedge [?x \geq 0]B(x,v)\big)}\,[;]$$

$$\frac{A \vdash [x'' = -g][?x = 0; v := -cv \cup ?x \geq 0]B(x,v)}{A \vdash [x'' = -g]\big([?x = 0; v := -cv]B(x,v) \wedge [?x \geq 0]B(x,v)\big)}\,[\cup]$$

$$\frac{A \vdash [x'' = -g; (?x = 0; v := -cv \cup ?x \geq 0)]B(x,v)}{A \vdash [x'' = -g][?x = 0; v := -cv \cup ?x \geq 0]B(x,v)}\,[;]$$

$$A \overset{\text{def}}{\equiv} 0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0$$

$$B(x,v) \overset{\text{def}}{\equiv} 0 \leq x \wedge x \leq H$$

$$(x'' = -g) \overset{\text{def}}{\equiv} (x' = v, v' = -g)$$

A Proof of a Short Single-hop Bouncing Ball

$$A \vdash \forall t{\geq}0\,\big((H{-}\tfrac{g}{2}t^2{=}0{\to}B(H{-}\tfrac{g}{2}t^2,{-}c(-gt)))\wedge(H{-}\tfrac{g}{2}t^2{\geq}0{\to}B(H{-}\tfrac{g}{2}t^2,{-}gt)\big)$$

[:=] $$A \vdash \forall t{\geq}0\,[x := H - \tfrac{g}{2}t^2]\big((x{=}0 \to B(x,-c(-gt)))\wedge(x{\geq}0 \to B(x,-gt))\big)$$

[:=] $$A \vdash \forall t{\geq}0\,[x := H - \tfrac{g}{2}t^2][v := -gt]\big((x{=}0 \to B(x,-cv))\wedge(x{\geq}0 \to B(x,v))\big)$$

[;] $$A \vdash \forall t{\geq}0\,[x := H - \tfrac{g}{2}t^2; v := -gt]\big((x{=}0 \to B(x,-cv))\wedge(x{\geq}0 \to B(x,v))\big)$$

[′] $$A \vdash [x'' = -g]\big((x = 0 \to B(x,-cv))\wedge(x \geq 0 \to B(x,v))\big)$$

[:=] $$A \vdash [x'' = -g]\big((x = 0 \to [v := -cv]B(x,v))\wedge(x \geq 0 \to B(x,v))\big)$$

[?],[?] $$A \vdash [x'' = -g]\big([?x = 0][v := -cv]B(x,v)\wedge[?x \geq 0]B(x,v)\big)$$

[;] $$A \vdash [x'' = -g]\big([?x = 0; v := -cv]B(x,v)\wedge[?x \geq 0]B(x,v)\big)$$

[∪] $$A \vdash [x'' = -g][?x = 0; v := -cv \cup ?x \geq 0]B(x,v)$$

[;] $$A \vdash [x'' = -g; (?x = 0; v := -cv \cup ?x \geq 0)]B(x,v)$$

$$A \overset{\text{def}}{\equiv} 0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0$$

$$B(x,v) \overset{\text{def}}{\equiv} 0 \leq x \wedge x \leq H$$

$$(x'' = -g) \overset{\text{def}}{\equiv} (x' = v, v' = -g)$$

A Proof of a Short Single-hop Bouncing Ball

Resolving abbreviations at the premise yields:

$$0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0 \rightarrow$$
$$\forall t \geq 0 \left((H - \frac{g}{2}t^2 = 0 \rightarrow 0 \leq H - \frac{g}{2}t^2 \wedge H - \frac{g}{2}t^2 \leq H) \right.$$
$$\left. \wedge (H - \frac{g}{2}t^2 \geq 0 \rightarrow 0 \leq H - \frac{g}{2}t^2 \wedge H - \frac{g}{2}t^2 \leq H) \right)$$

which is provable by arithmetic (since $g > 0$ and $t^2 \geq 0$).

A Proof of a Short Single-hop Bouncing Ball

Resolving abbreviations at the premise yields:

$$0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0 \rightarrow$$
$$\forall t \geq 0 \left((H - \frac{g}{2} t^2 = 0 \rightarrow 0 \leq H - \frac{g}{2} t^2 \wedge H - \frac{g}{2} t^2 \leq H) \right.$$
$$\left. \wedge (H - \frac{g}{2} t^2 \geq 0 \rightarrow 0 \leq H - \frac{g}{2} t^2 \wedge H - \frac{g}{2} t^2 \leq H) \right)$$

which is provable by arithmetic (since $g > 0$ and $t^2 \geq 0$).

A Proof of a Short Single-hop Bouncing Ball

Resolving abbreviations at the premise yields:

$$0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0 \rightarrow$$
$$\forall t{\geq}0 \left((H - \frac{g}{2}t^2 = 0 \rightarrow 0 \leq H - \frac{g}{2}t^2 \wedge H - \frac{g}{2}t^2 \leq H) \right.$$
$$\left. \wedge (H - \frac{g}{2}t^2 \geq 0 \rightarrow 0 \leq H - \frac{g}{2}t^2 \wedge H - \frac{g}{2}t^2 \leq H) \right)$$

which is provable by arithmetic (since $g > 0$ and $t^2 \geq 0$).

Exciting!

We have just formally verified our very first CPS!

A Proof of a Short Single-hop Bouncing Ball

Resolving abbreviations at the premise yields:

$$0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0 \rightarrow$$
$$\forall t \geq 0 \left((H - \frac{g}{2}t^2 = 0 \rightarrow 0 \leq H - \frac{g}{2}t^2 \wedge H - \frac{g}{2}t^2 \leq H) \right.$$
$$\left. \wedge (H - \frac{g}{2}t^2 \geq 0 \rightarrow 0 \leq H - \frac{g}{2}t^2 \wedge H - \frac{g}{2}t^2 \leq H) \right)$$

which is provable by arithmetic (since $g > 0$ and $t^2 \geq 0$).

Exciting!

We have just formally verified our very first CPS!

Okay, alright, it was a grotesquely simplified single-hop bouncing ball. But the axioms of our proof technique were completely general and not specific to bouncing balls, so they should carry us forward to true CPS.

Outline

Differential Dynamic Logic: Axiomatization

equations of truth

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

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

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

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

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

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

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

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

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'16


André Platzer.
Foundations of cyber-physical systems.
Lecture Notes 15-424/624/824, Carnegie Mellon University, 2017.
URL: http://www.cs.cmu.edu/~aplatzer/course/fcps17.html.


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


André Platzer.
Differential dynamic logic for hybrid systems.
J. Autom. Reas., 41(2):143–189, 2008.
doi:10.1007/s10817-008-9103-8.


André Platzer.
The complete proof theory of hybrid systems.
In LICS [7], pages 541–550.
doi:10.1109/LICS.2012.64.


André Platzer.
Logics of dynamical systems.
In LICS [7], pages 13–24.
doi:10.1109/LICS.2012.13.


André Platzer.
A complete uniform substitution calculus for differential dynamic logic.

J. Autom. Reas., 2016.
doi:10.1007/s10817-016-9385-1.


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