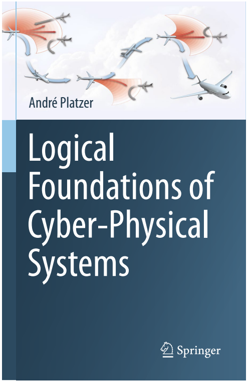
05: Dynamical Systems & Dynamic Axioms

Logical Foundations of Cyber-Physical Systems

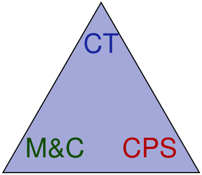


André Platzer
Carnegie Mellon University
Computer Science Department

Outline

Outline

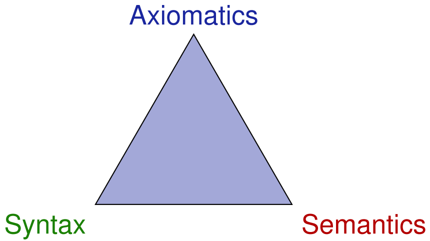
rigorous reasoning about CPS
dL as verification language



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 $A \land B$, syntactically? If A is true, is $A \land B$ true, too? Conversely?

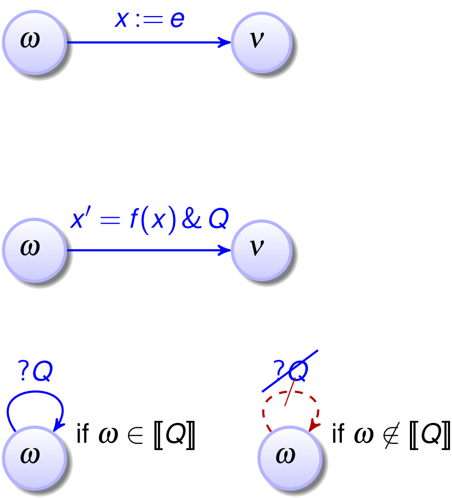
Outline

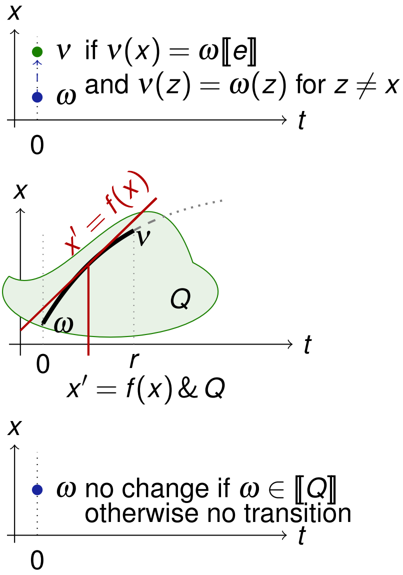
Approach

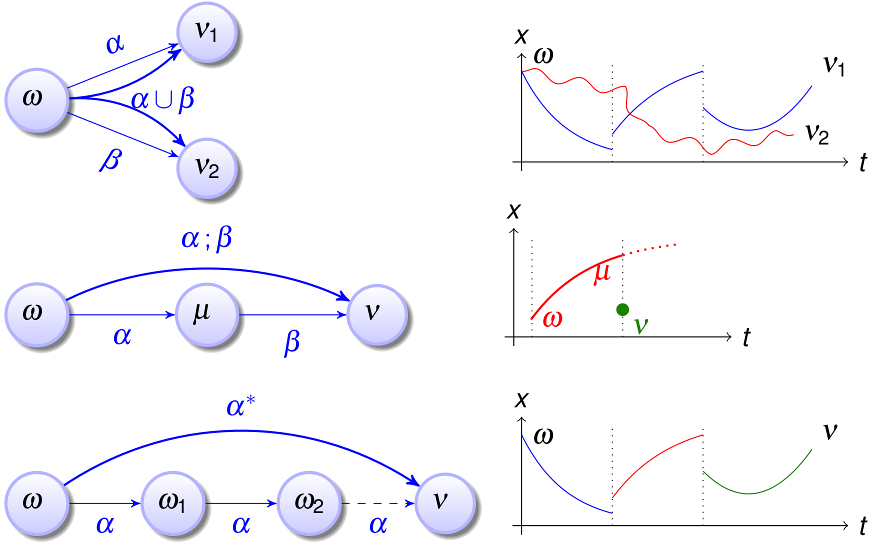
Logical guiding principle: Compositionality

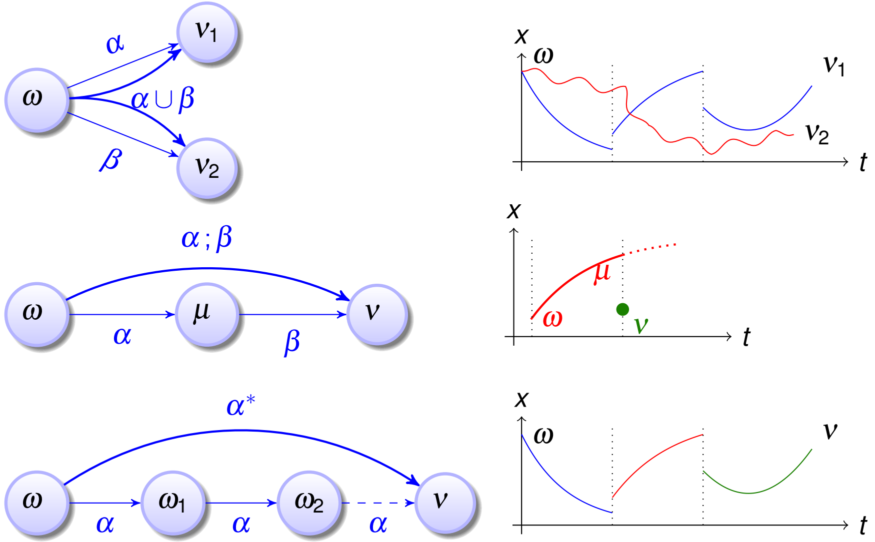
1. Every CPS is modeled by a hybrid program (or game ...)
2. All hybrid programs are combinations of simpler hybrid programs (by a program operator such as $\cup$ and ; and *)
3. All CPS can be analyzed if only we identify one suitable analysis technique for each operator.
4. Analysis of a big CPS is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

Hybrid Programs: Semantics

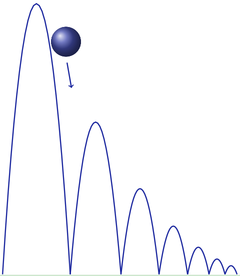





ω
ν_1
ν_2
α
β
$\alpha \cup \beta$
μ
ν
$\alpha ; \beta$
ω_1
ω_2
α^*
x
t

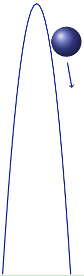


compositional semantics ⇒ compositional proofs!



Example (Quantum the Bouncing Ball)

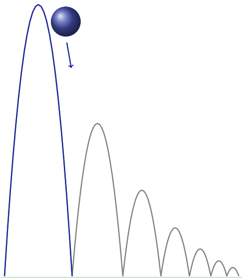
$$0 \le x \land x = H \land v = 0 \land g > 0 \land 1 \ge c \ge 0 \to$$
$$\left[\left(\{x' = v, v' = -g \,\&\, x \ge 0\}; (?x{=}0; v := -cv \cup ?x{\ne}0)\right)^*\right] (0 \le x \land x \le H)$$



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

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

Removing the repetition grotesquely changes the behavior to a single hop

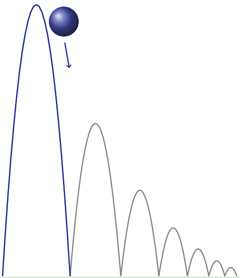


Example (Quantum the Bouncing Ball) (Single-hop)

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

Removing the repetition grotesquely changes the behavior to a single hop

Conjecture: Quantum the Acrophobic Bouncing Ball



How to prove ;

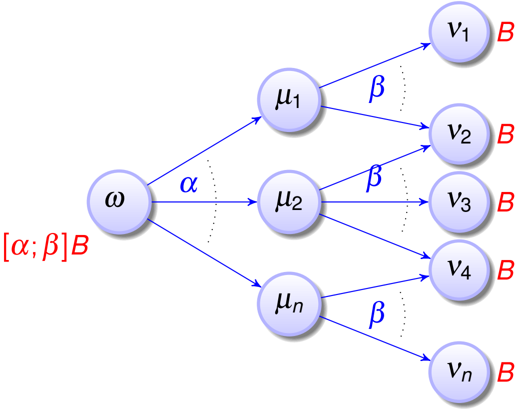
Example (Quantum the Bouncing Ball) (Single-hop)

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

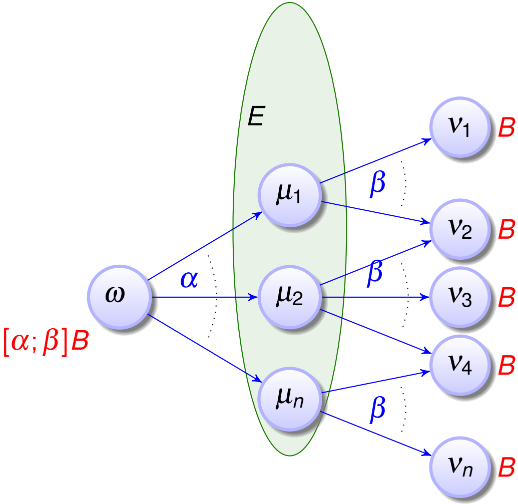
Removing the repetition grotesquely changes the behavior to a single hop

Outline

$$\text{H;}\quad \frac{}{A \rightarrow [\alpha;\beta]B}$$

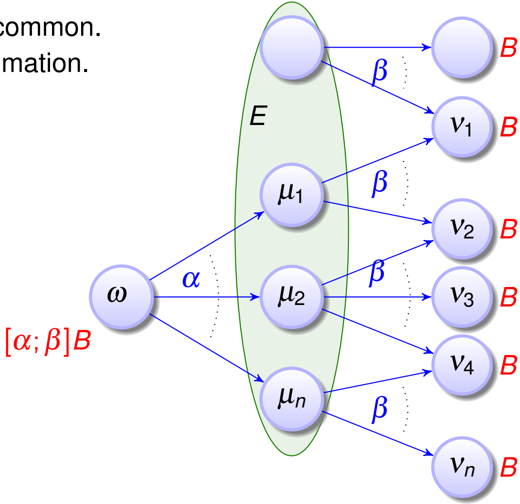


H; $\dfrac{}{A \rightarrow [\alpha;\beta]B}$



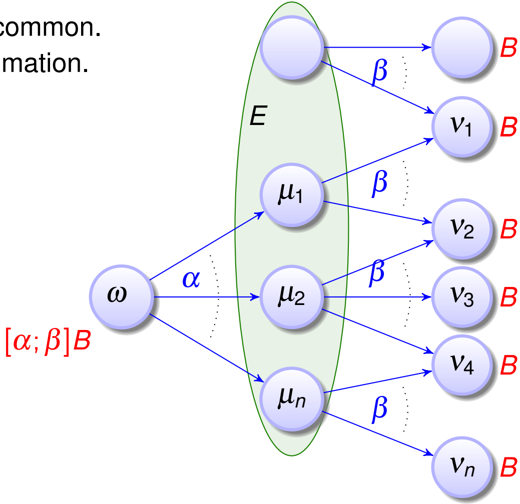
E summarizes what μ_i have in common.
E is often imprecise overapproximation.

$$\text{H;}\ \frac{A \rightarrow [\alpha]E \quad E \rightarrow [\beta]B}{A \rightarrow [\alpha;\beta]B}$$



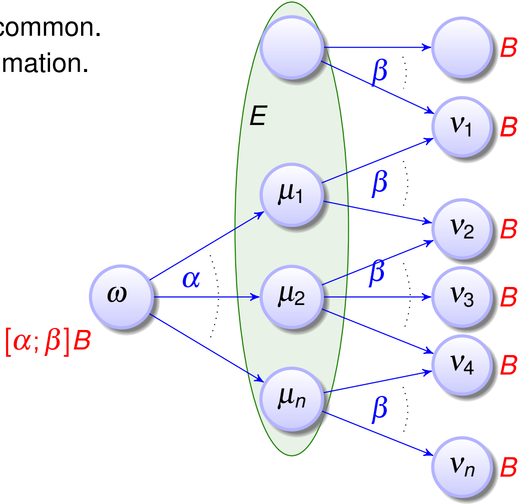
E summarizes what μ_i have in common.
E is often imprecise overapproximation.
Just need to find this E ...

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



E summarizes what μ_i have in common.
E is often imprecise overapproximation.
Just need to find this E ...

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



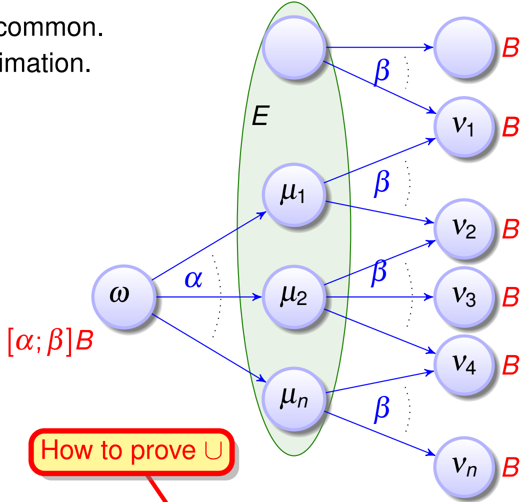
Example (Quantum the Bouncing Ball) (Single-hop)

$$0\le x=H\wedge v=0\wedge g>0\wedge 1\ge c\ge 0 \to \left[x'=v, v'=-g \,\&\, x\ge 0\right]E$$

$$E \to \left[?x=0; v:=-cv \cup ?x\ne 0\right](0\le x \wedge x\le H)$$

E summarizes what μ_i have in common.
E is often imprecise overapproximation.
Just need to find this E ...

$$\text{H;}\quad \frac{A \rightarrow [\alpha]E \quad E \rightarrow [\beta]B}{A \rightarrow [\alpha;\beta]B}$$



How to prove $\cup$

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

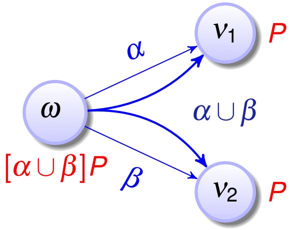
$$0 \le x = H \wedge v = 0 \wedge g > 0 \wedge 1 \ge c \ge 0 \rightarrow [x' = v, v' = -g \,\&\, x \ge 0]E$$

$$E \rightarrow [?x = 0; v := -cv \cup ?x \ne 0](0 \le x \wedge x \le H)$$

Outline

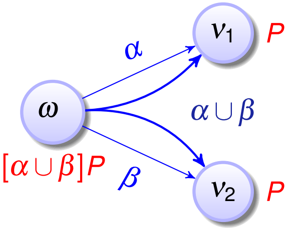
Semantics

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



Semantics

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

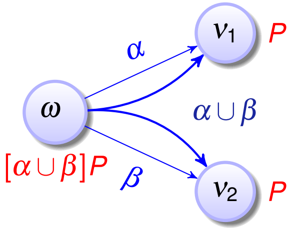


- $\omega \in [\![[\alpha \cup \beta]P]\!]$ iff $v \in [\![P]\!]$ for all v with $(\omega, v) \in [\![\alpha \cup \beta]\!] = [\![\alpha]\!] \cup [\![\beta]\!]$

Motivating Proofs for Nondeterministic Choices

Semantics

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

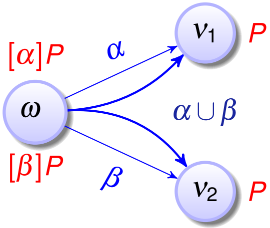


- $\omega \in [\![[\alpha \cup \beta]P]\!]$ iff $\nu \in [\![P]\!]$ for all ν with $(\omega, \nu) \in [\![\alpha \cup \beta]\!] = [\![\alpha]\!] \cup [\![\beta]\!]$
- Then $\nu \in [\![P]\!]$ for all ν with $(\omega, \nu) \in [\![\alpha]\!]$
- and $\nu \in [\![P]\!]$ for all ν with $(\omega, \nu) \in [\![\beta]\!]$

Motivating Proofs for Nondeterministic Choices

Semantics

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

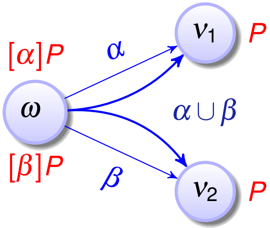


- $\omega \in [\![[\alpha \cup \beta]P]\!]$ iff $\nu \in [\![P]\!]$ for all ν with $(\omega, \nu) \in [\![\alpha \cup \beta]\!] = [\![\alpha]\!] \cup [\![\beta]\!]$
- Then $\nu \in [\![P]\!]$ for all ν with $(\omega, \nu) \in [\![\alpha]\!]$ i.e., $\omega \in [\![[\alpha]P]\!]$
- and $\nu \in [\![P]\!]$ for all ν with $(\omega, \nu) \in [\![\beta]\!]$ i.e., $\omega \in [\![[\beta]P]\!]$

Motivating Proofs for Nondeterministic Choices

Semantics

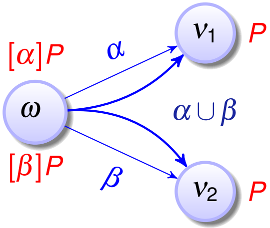
$[\![\alpha \cup \beta]\!] = [\![\alpha]\!] \cup [\![\beta]\!]$



- $\omega \in [\![[\alpha \cup \beta]P]\!]$ iff $\nu \in [\![P]\!]$ for all ν with $(\omega, \nu) \in [\![\alpha \cup \beta]\!] = [\![\alpha]\!] \cup [\![\beta]\!]$
- Then $\nu \in [\![P]\!]$ for all ν with $(\omega, \nu) \in [\![\alpha]\!]$ i.e., $\omega \in [\![[\alpha]P]\!]$
- and $\nu \in [\![P]\!]$ for all ν with $(\omega, \nu) \in [\![\beta]\!]$ i.e., $\omega \in [\![[\beta]P]\!]$
- And vice versa.

Semantics

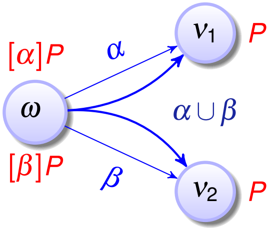
$[\![\alpha \cup \beta]\!] = [\![\alpha]\!] \cup [\![\beta]\!]$



- $\omega \in [\![[\alpha \cup \beta]P]\!]$ iff $\nu \in [\![P]\!]$ for all ν with $(\omega, \nu) \in [\![\alpha \cup \beta]\!] = [\![\alpha]\!] \cup [\![\beta]\!]$
- Then $\nu \in [\![P]\!]$ for all ν with $(\omega, \nu) \in [\![\alpha]\!]$ i.e., $\omega \in [\![[\alpha]P]\!]$
- and $\nu \in [\![P]\!]$ for all ν with $(\omega, \nu) \in [\![\beta]\!]$ i.e., $\omega \in [\![[\beta]P]\!]$
- And vice versa. So $\omega \in [\![[\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P]\!]$

Semantics

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

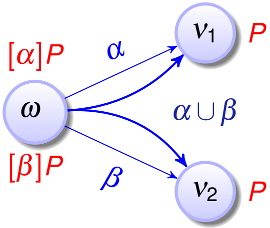


- $\omega \in [\![[\alpha \cup \beta]P]\!]$ iff $v \in [\![P]\!]$ for all v with $(\omega, v) \in [\![\alpha \cup \beta]\!] = [\![\alpha]\!] \cup [\![\beta]\!]$
- Then $v \in [\![P]\!]$ for all v with $(\omega, v) \in [\![\alpha]\!]$ i.e., $\omega \in [\![[\alpha]P]\!]$
- and $v \in [\![P]\!]$ for all v with $(\omega, v) \in [\![\beta]\!]$ i.e., $\omega \in [\![[\beta]P]\!]$
- And vice versa. So $\omega \in [\![[\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P]\!]$ for all states ω

Motivating Proofs for Nondeterministic Choices

Semantics

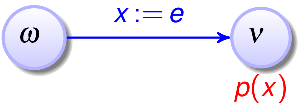
$[\![\alpha \cup \beta]\!] = [\![\alpha]\!] \cup [\![\beta]\!]$



- $\omega \in [\![[\alpha \cup \beta]P]\!]$ iff $\nu \in [\![P]\!]$ for all ν with $(\omega, \nu) \in [\![\alpha \cup \beta]\!] = [\![\alpha]\!] \cup [\![\beta]\!]$
- Then $\nu \in [\![P]\!]$ for all ν with $(\omega, \nu) \in [\![\alpha]\!]$ i.e., $\omega \in [\![[\alpha]P]\!]$
- and $\nu \in [\![P]\!]$ for all ν with $(\omega, \nu) \in [\![\beta]\!]$ i.e., $\omega \in [\![[\beta]P]\!]$
- And vice versa. So $\omega \in [\![[\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P]\!]$ for all states ω

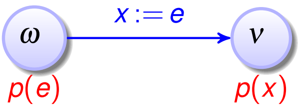
Lemma

$[\cup]$ $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$ *is a sound axiom, i.e., all its instances valid.*

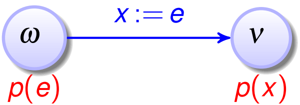


$[:=]\quad [x := e]p(x) \leftrightarrow$

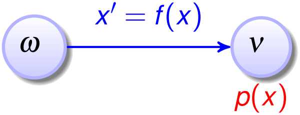
$[:=]\quad [x := e]p(x) \leftrightarrow p(e)$



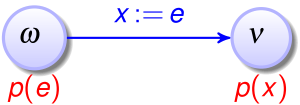
[:=] $[x := e]p(x) \leftrightarrow p(e)$



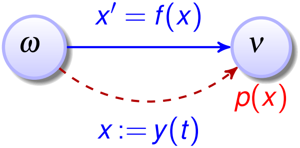
['] $[x' = f(x)]p(x) \leftrightarrow$



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

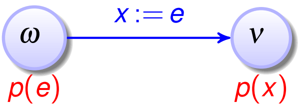


$[']\ \ [x' = f(x)]p(x) \leftrightarrow \qquad [x := y(t)]p(x)$

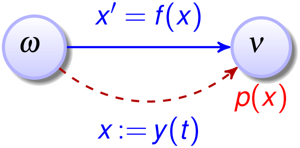


Dynamic Axioms for Dynamical Systems

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

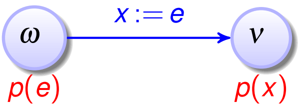


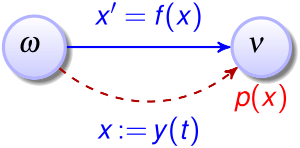
['] $[x' = f(x)]p(x) \leftrightarrow \forall t \geq 0 [x := y(t)]p(x)$



Dynamic Axioms for Dynamical Systems

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



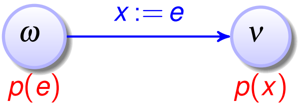


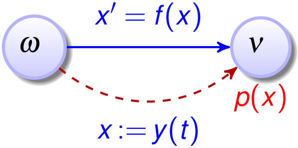
$[']$ $[x' = f(x)]p(x) \leftrightarrow \forall t{\geq}0[x := y(t)]p(x)$

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

Dynamic Axioms for Dynamical Systems

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

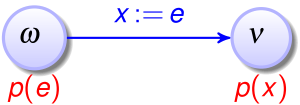


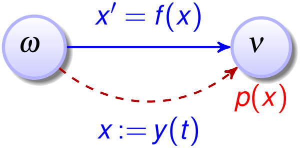


$[']$ $[x' = f(x)]p(x) \leftrightarrow \forall t \geq 0 [x := y(t)]p(x)$

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

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

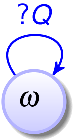




$['']$ $[x' = f(x)]p(x) \leftrightarrow \forall t \geq 0 [x := y(t)]p(x)$

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

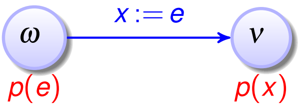
$[?]$ $[?Q]P \leftrightarrow$

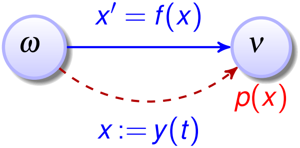


if $\omega \in [\![Q]\!]$

Dynamic Axioms for Dynamical Systems

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

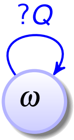




$[']$ $[x' = f(x)]p(x) \leftrightarrow \forall t{\geq}0\,[x := y(t)]p(x)$

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

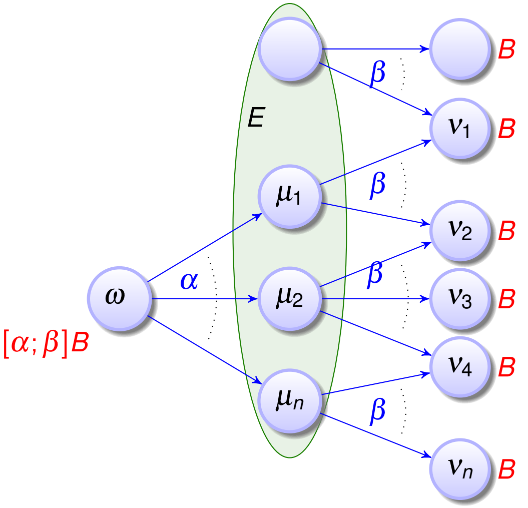
$[?]$ $[?Q]P \leftrightarrow (Q \rightarrow P)$



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

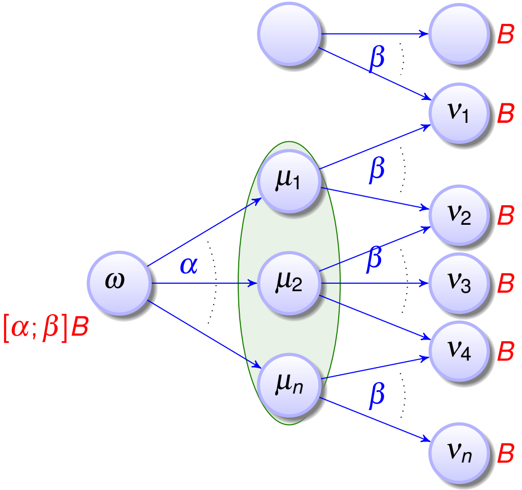
What is the most precise E summary?

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



What is the most precise E summary?

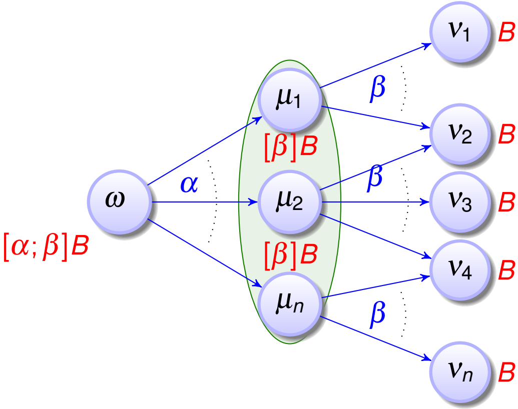
$$\text{H;}\quad \frac{A \rightarrow [\alpha]E \quad E \rightarrow [\beta]B}{A \rightarrow [\alpha;\beta]B}$$



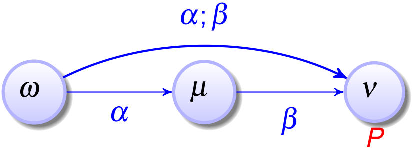
Sequential Compositions via Intermediate Conditions

What is the most precise E summary? $[\beta]B$

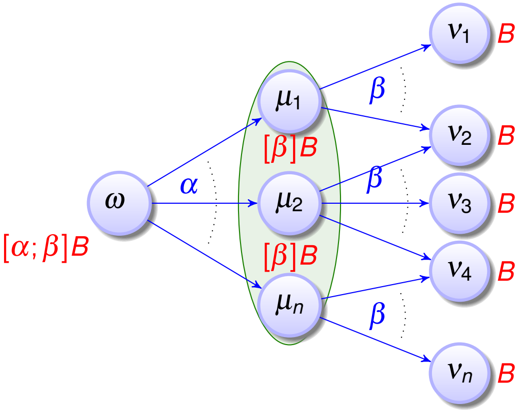
$$\text{H;}\ \frac{A \rightarrow [\alpha][\beta]B \quad [\beta]B \rightarrow [\beta]B}{A \rightarrow [\alpha;\beta]B}$$



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

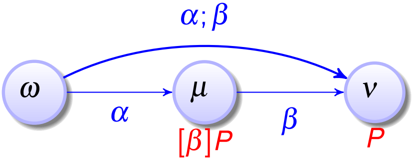


H; $\dfrac{A \rightarrow [\alpha][\beta]B \quad [\beta]B \rightarrow [\beta]B}{A \rightarrow [\alpha;\beta]B}$

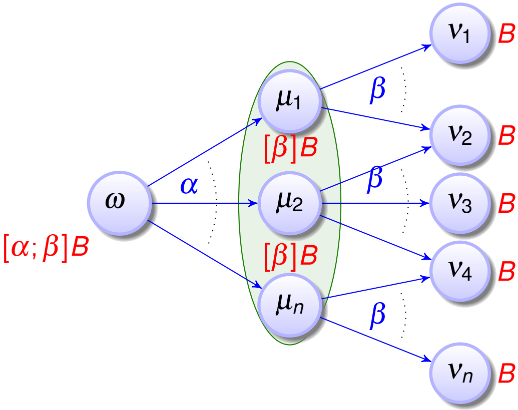


Sequential Compositions via Intermediate Conditions

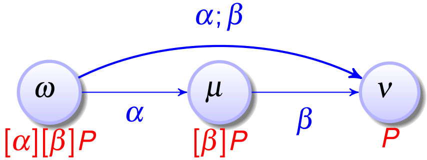
[;] $[\alpha;\beta]P \leftrightarrow$



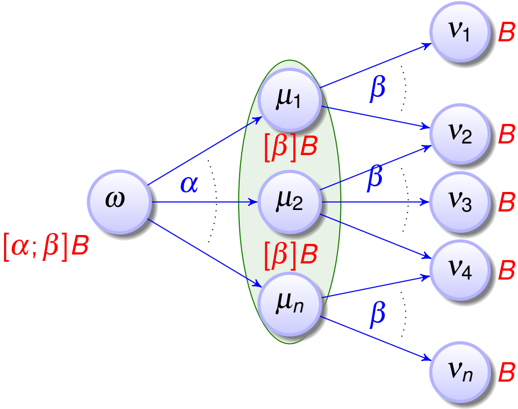
H; $\dfrac{A \rightarrow [\alpha][\beta]B \quad [\beta]B \rightarrow [\beta]B}{A \rightarrow [\alpha;\beta]B}$



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



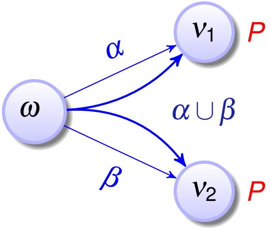
H; $\dfrac{A \rightarrow [\alpha][\beta]B \quad [\beta]B \rightarrow [\beta]B}{A \rightarrow [\alpha;\beta]B}$



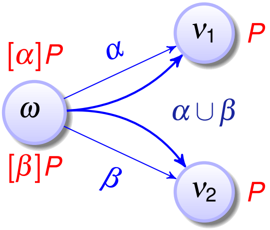
Dynamic Axioms for Dynamical Systems

compositional semantics $\Rightarrow$ compositional axioms!

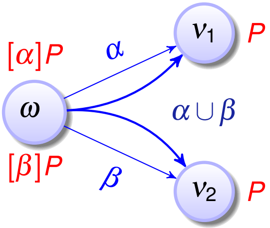
$[\cup]\quad [\alpha \cup \beta]P \leftrightarrow$



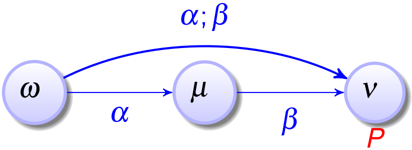
$[\cup]$ $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$



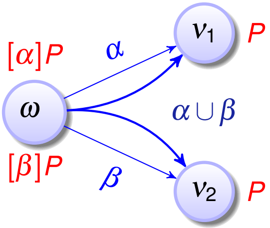
[∪] $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$



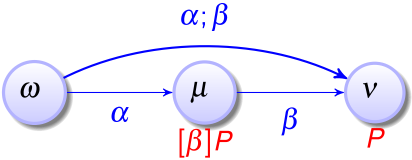
[;] $[\alpha;\beta]P \leftrightarrow$



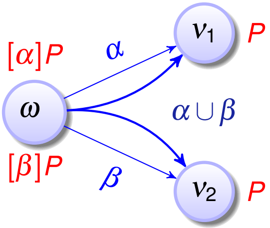
[∪] $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \land [\beta]P$



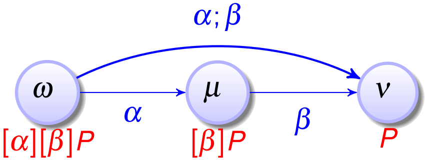
[;] $[\alpha;\beta]P \leftrightarrow$



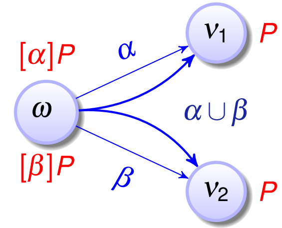
$[\cup]$ $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \land [\beta]P$



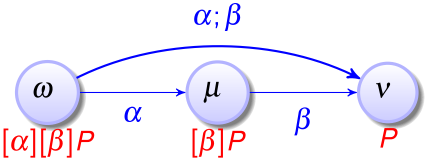
$[;]$ $[\alpha;\beta]P \leftrightarrow [\alpha][\beta]P$



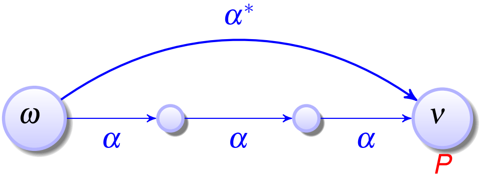
$[\cup]$ $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$



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

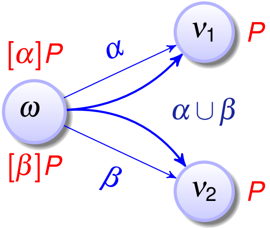


$[^*]$ $[\alpha^*]P \leftrightarrow$

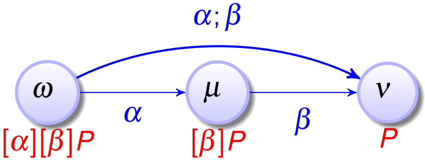


Dynamic Axioms for Dynamical Systems

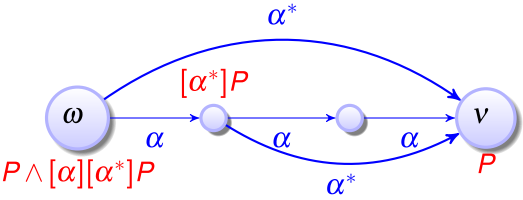
$[\cup]$ $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$



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



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



Lemma

[$\cup$] $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$ *is sound.*

Lemma

[;] $[\alpha;\beta]P \leftrightarrow [\alpha][\beta]P$ *is sound.*

Lemma

$[\cup]$ $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$ *is sound.*

Proof using $[\![\alpha \cup \beta]\!] = [\![\alpha]\!] \cup [\![\beta]\!]$.

$(\omega, \nu) \in [\![\alpha \cup \beta]\!]$ iff $(\omega, \nu) \in [\![\alpha]\!]$ or $(\omega, \nu) \in [\![\beta]\!]$.
Thus, $\omega \in [\![[\alpha \cup \beta]P]\!]$ iff both $\omega \in [\![[\alpha]P]\!]$ and $\omega \in [\![[\beta]P]\!]$. $\square$

Lemma

$[;]$ $[\alpha; \beta]P \leftrightarrow [\alpha][\beta]P$ *is sound.*

Soundness of Dynamic Axioms

Lemma

$[\cup]$ $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$ *is sound.*

Proof using $[\![\alpha \cup \beta]\!] = [\![\alpha]\!] \cup [\![\beta]\!]$.

$(\omega, \nu) \in [\![\alpha \cup \beta]\!]$ iff $(\omega, \nu) \in [\![\alpha]\!]$ or $(\omega, \nu) \in [\![\beta]\!]$.
Thus, $\omega \in [\![[\alpha \cup \beta]P]\!]$ iff both $\omega \in [\![[\alpha]P]\!]$ and $\omega \in [\![[\beta]P]\!]$. $\square$

Lemma

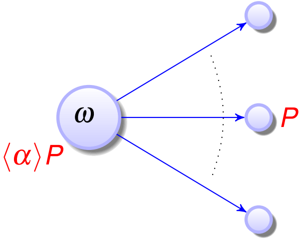
$[;]$ $[\alpha;\beta]P \leftrightarrow [\alpha][\beta]P$ *is sound.*

Proof using $[\![\alpha;\beta]\!] = [\![\alpha]\!] \circ [\![\beta]\!]$.

$(\omega, \nu) \in [\![\alpha;\beta]\!]$ iff $(\omega, \mu) \in [\![\alpha]\!]$ and $(\mu, \nu) \in [\![\beta]\!]$ for some state μ.
Thus, $\omega \in [\![[\alpha;\beta]P]\!]$ iff $\mu \in [\![[\beta]P]\!]$ for all μ with $(\omega, \mu) \in [\![\alpha]\!]$.
That is, $\omega \in [\![[\alpha;\beta]P]\!]$ iff $\omega \in [\![[\alpha][\beta]P]\!]$. $\square$

Axioms for Diamonds

$\langle\cdot\rangle \quad \langle\alpha\rangle P \leftrightarrow$

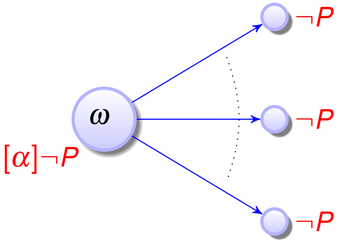


Semantics

$$\begin{aligned} [\![\langle\alpha\rangle P]\!] &= \{\omega : \nu \in [\![P]\!] \text{ for some } \nu : (\omega,\nu) \in [\![\alpha]\!]\} \\ [\![[\alpha]P]\!] &= \{\omega : \nu \in [\![P]\!] \text{ for all } \nu : (\omega,\nu) \in [\![\alpha]\!]\} \end{aligned}$$

Axioms for Diamonds

$\langle\cdot\rangle \quad \langle\alpha\rangle P \leftrightarrow$

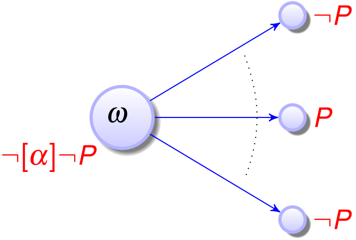


Semantics

$$\begin{aligned}
[\![\langle\alpha\rangle P]\!] &= \{\omega : \nu \in [\![P]\!] \text{ for some } \nu : \ (\omega,\nu) \in [\![\alpha]\!]\} \\
[\![[\alpha]P]\!] &= \{\omega : \nu \in [\![P]\!] \text{ for all } \nu : \ (\omega,\nu) \in [\![\alpha]\!]\}
\end{aligned}$$

Axioms for Diamonds

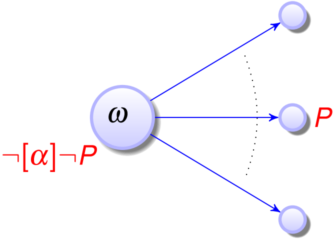
$\langle\cdot\rangle \quad \langle\alpha\rangle P \leftrightarrow$



Semantics

$$\begin{aligned}
[\![\langle\alpha\rangle P]\!] &= \{\omega : \nu \in [\![P]\!] \text{ for some } \nu : (\omega,\nu) \in [\![\alpha]\!]\} \\
[\![[\alpha]P]\!] &= \{\omega : \nu \in [\![P]\!] \text{ for all } \nu : (\omega,\nu) \in [\![\alpha]\!]\}
\end{aligned}$$

$\langle\cdot\rangle \quad \langle\alpha\rangle P \leftrightarrow \neg[\alpha]\neg P$

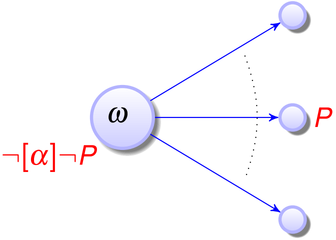


Semantics

$$\begin{aligned}
[\![\langle\alpha\rangle P]\!] &= \{\omega : \nu \in [\![P]\!] \text{ for some } \nu : (\omega,\nu) \in [\![\alpha]\!]\} \\
[\![[\alpha]P]\!] &= \{\omega : \nu \in [\![P]\!] \text{ for all } \nu : (\omega,\nu) \in [\![\alpha]\!]\}
\end{aligned}$$

Axioms for Diamonds: Duality

$\langle\cdot\rangle$ $\langle\alpha\rangle P \leftrightarrow \neg[\alpha]\neg P$



Duality axiom $\langle\cdot\rangle$ relates $\langle\alpha\rangle$ to $[\alpha]$ for arbitrary HP α

Semantics

$$[\![\langle\alpha\rangle P]\!] = \{\omega : \nu \in [\![P]\!] \text{ for some } \nu : (\omega,\nu) \in [\![\alpha]\!]\}$$
$$[\![[\alpha]P]\!] = \{\omega : \nu \in [\![P]\!] \text{ for all } \nu : (\omega,\nu) \in [\![\alpha]\!]\}$$

Outline

A Proof of a Single-hop Bouncing Ball

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

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

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

$$\{x'' = -g\} \stackrel{\text{def}}{\equiv} \{x' = v, v' = -g\}$$

A Proof of a Single-hop Bouncing Ball

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

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

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

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

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

A Proof of a Single-hop Bouncing Ball

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

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

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

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

$$\{x'' = -g\} \stackrel{\text{def}}{\equiv} \{x' = v, v' = -g\}$$

A Proof of a Single-hop Bouncing Ball

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

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

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

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

$$\{x''=-g\} \stackrel{\text{def}}{\equiv} \{x'=v, v'=-g\}$$

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

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

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

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

$$\{x'' = -g\} \stackrel{\text{def}}{\equiv} \{x' = v, v' = -g\}$$

A Proof of a Single-hop Bouncing Ball

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

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

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

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

$$\{x'' = -g\} \stackrel{\text{def}}{\equiv} \{x' = v, v' = -g\}$$

A Proof of a Single-hop Bouncing Ball

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

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

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

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

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

A Proof of a Single-hop Bouncing Ball

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

$$
\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{A \rightarrow \forall t{\geq}0\,[x:=H-\frac{g}{2}t^2][v:=-gt]\big((x{=}0 \rightarrow B(x,-cv)) \land (x{\geq}0 \rightarrow B(x,v))\big)}{A \rightarrow \forall t{\geq}0\,[x:=H-\frac{g}{2}t^2;v:=-gt]\big((x{=}0 \rightarrow B(x,-cv)) \land (x{\geq}0 \rightarrow B(x,v))\big)}[;]}{A \rightarrow [x''=-g]\big((x=0 \rightarrow B(x,-cv)) \land (x \geq 0 \rightarrow B(x,v))\big)}[']}{A \rightarrow [x''=-g]\big((x=0 \rightarrow [v:=-cv]B(x,v)) \land (x \geq 0 \rightarrow B(x,v))\big)}[:=]}{A \rightarrow [x''=-g]\big([?x=0][v:=-cv]B(x,v) \land [?x \geq 0]B(x,v)\big)}[?],[?]}{A \rightarrow [x''=-g]\big([?x=0;v:=-cv]B(x,v) \land [?x \geq 0]B(x,v)\big)}[;]}{A \rightarrow [x''=-g][?x=0;v:=-cv \cup ?x \geq 0]B(x,v)}[\cup]}{A \rightarrow [x''=-g;(?x=0;v:=-cv \cup ?x \geq 0)]B(x,v)}[;]
$$

Rule labels from top to bottom: [:=], [;], ['], [:=], [?],[?], [;], [∪], [;]

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

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

$$\{x''=-g\} \stackrel{\text{def}}{\equiv} \{x'=v, v'=-g\}$$

A Proof of a Single-hop Bouncing Ball

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

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

A Proof of a Single-hop Bouncing Ball

$$
\begin{array}{rl}
 & A \rightarrow \forall t{\geq}0 \left(\left(H - \frac{g}{2}t^2 = 0 \rightarrow B(H - \frac{g}{2}t^2, -c(-gt))\right) \land \left(H - \frac{g}{2}t^2 \geq 0 \rightarrow B(H - \frac{g}{2}t^2, -gt)\right)\right) \\ \hline
[:=] & A \rightarrow \forall t{\geq}0 \, [x := H - \frac{g}{2}t^2] \left(\left(x = 0 \rightarrow B(x, -c(-gt))\right) \land \left(x \geq 0 \rightarrow B(x, -gt)\right)\right) \\ \hline
[:=] & A \rightarrow \forall t{\geq}0 \, [x := H - \frac{g}{2}t^2][v := -gt] \left(\left(x = 0 \rightarrow B(x, -cv)\right) \land \left(x \geq 0 \rightarrow B(x, v)\right)\right) \\ \hline
[;] & A \rightarrow \forall t{\geq}0 \, [x := H - \frac{g}{2}t^2; v := -gt] \left(\left(x = 0 \rightarrow B(x, -cv)\right) \land \left(x \geq 0 \rightarrow B(x, v)\right)\right) \\ \hline
['] & A \rightarrow [x'' = -g] \left(\left(x = 0 \rightarrow B(x, -cv)\right) \land \left(x \geq 0 \rightarrow B(x, v)\right)\right) \\ \hline
[:=] & A \rightarrow [x'' = -g] \left(\left(x = 0 \rightarrow [v := -cv]B(x, v)\right) \land \left(x \geq 0 \rightarrow B(x, v)\right)\right) \\ \hline
[?],[?] & A \rightarrow [x'' = -g] \left([?x = 0][v := -cv]B(x, v) \land [?x \geq 0]B(x, v)\right) \\ \hline
[;] & A \rightarrow [x'' = -g] \left([?x = 0; v := -cv]B(x, v) \land [?x \geq 0]B(x, v)\right) \\ \hline
[\cup] & A \rightarrow [x'' = -g][?x = 0; v := -cv \cup ?x \geq 0]B(x, v) \\ \hline
[;] & A \rightarrow [x'' = -g; (?x = 0; v := -cv \cup ?x \geq 0)]B(x, v)
\end{array}
$$

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

A Proof of a Single-hop Bouncing Ball

$$A \rightarrow \forall t \geq 0 \left(\left(H - \frac{g}{2}t^2 = 0 \rightarrow B(H - \tfrac{g}{2}t^2, -c(-gt))\right) \wedge \left(H - \frac{g}{2}t^2 \geq 0 \rightarrow B(H - \tfrac{g}{2}t^2, -gt)\right)\right)$$

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

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

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

['] $$A \rightarrow [x'' = -g]\left(\left(x = 0 \rightarrow B(x, -cv)\right) \wedge \left(x \geq 0 \rightarrow B(x, v)\right)\right)$$

[:=] $$A \rightarrow [x'' = -g]\left(\left(x = 0 \rightarrow [v := -cv]B(x, v)\right) \wedge \left(x \geq 0 \rightarrow B(x, v)\right)\right)$$

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

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

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

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

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

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

$$\{x'' = -g\} \stackrel{\text{def}}{\equiv} \{x' = v, v' = -g\}$$

Resolving abbreviations at the top premise yields provable arithmetic:

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

A Proof of a Single-hop Bouncing Ball

Resolving abbreviations at the top premise yields provable arithmetic:

$$
\begin{aligned}
&0 \le x \land x = H \land v = 0 \land g > 0 \land 1 \ge c \ge 0 \to \\
&\qquad \forall t{\ge}0 \Big(\big(H - \frac{g}{2}t^2 = 0 \to 0 \le H - \frac{g}{2}t^2 \land H - \frac{g}{2}t^2 \le H\big) \\
&\qquad\qquad \land \big(H - \frac{g}{2}t^2 \ge 0 \to 0 \le H - \frac{g}{2}t^2 \land H - \frac{g}{2}t^2 \le H\big)\Big)
\end{aligned}
$$

A Proof of a Single-hop Bouncing Ball

Resolving abbreviations at the top premise yields provable arithmetic:

$$0 \le x \land x = H \land v = 0 \land g > 0 \land 1 \ge c \ge 0 \to$$
$$\forall t{\ge}0\, \Big(\big(H - \frac{g}{2}t^2 = 0 \to 0 \le H - \frac{g}{2}t^2 \land H - \frac{g}{2}t^2 \le H\big)$$
$$\land \big(H - \frac{g}{2}t^2 \ge 0 \to 0 \le H - \frac{g}{2}t^2 \land H - \frac{g}{2}t^2 \le H\big)\Big)$$

A Proof of a Single-hop Bouncing Ball

Resolving abbreviations at the top premise yields provable arithmetic:

$$
\begin{aligned}
&0 \le x \land x = H \land v = 0 \land g > 0 \land 1 \ge c \ge 0 \rightarrow \\
&\qquad \forall t{\ge}0 \Big(\big(H - \frac{g}{2}t^2 = 0 \rightarrow 0 \le H - \frac{g}{2}t^2 \land H - \frac{g}{2}t^2 \le H\big) \\
&\qquad\qquad \land \big(H - \frac{g}{2}t^2 \ge 0 \rightarrow 0 \le H - \frac{g}{2}t^2 \land H - \frac{g}{2}t^2 \le H\big)\Big)
\end{aligned}
$$

Exciting!

We have just formally verified our very first CPS!

Resolving abbreviations at the top premise yields provable arithmetic:

$$0 \le x \land x = H \land v = 0 \land g > 0 \land 1 \ge c \ge 0 \rightarrow \forall t{\ge}0 \big((H - \frac{g}{2}t^2 = 0 \rightarrow 0 \le H - \frac{g}{2}t^2 \land H - \frac{g}{2}t^2 \le H) \land (H - \frac{g}{2}t^2 \ge 0 \rightarrow 0 \le H - \frac{g}{2}t^2 \land H - \frac{g}{2}t^2 \le H) \big)$$

Exciting!

We have just formally verified our very first CPS!

Okay, it was a grotesquely simplified single-hop bouncing ball.
But the axioms of our proof technique were completely general, so they carry us forward to true CPSs.

Outline

Summary: Important Differential Dynamic Logic Axioms

equations of truth

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

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

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

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

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

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

$\langle\cdot\rangle$ $\langle\alpha\rangle P \leftrightarrow \neg[\alpha]\neg P$

One axiom for each HP operator
Using an axiom from left to right simplifies the HP structure

Summary: Important Differential Dynamic Logic Axioms

equations of truth

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

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

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

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

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

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

$\langle\cdot\rangle$ $\langle\alpha\rangle P \leftrightarrow \neg[\alpha]\neg P$

One axiom for each HP operator

Using an axiom from left to right simplifies the HP structure

Summary: Important Differential Dynamic Logic Axioms

equations of truth

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

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

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

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

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

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

$\langle\cdot\rangle\quad \langle\alpha\rangle P \leftrightarrow \neg[\alpha]\neg P$

One axiom for each HP operator

Using an axiom from left to right simplifies the HP structure except . . .

equations of truth

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

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

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

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

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

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

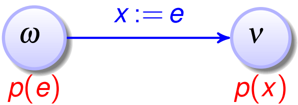
$\langle\cdot\rangle\ \langle\alpha\rangle P \leftrightarrow \neg[\alpha]\neg P$

One axiom for each HP operator

Using an axiom from left to right simplifies the HP structure except . . .

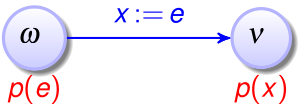
Admissibility Caveats

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



- Elegant understanding is via uniform substitutions in Part IV. Till then:

Admissibility Caveats

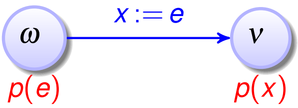


$[:=]\quad [x := e]p(x) \leftrightarrow p(e)$

- Elegant understanding is via uniform substitutions in Part IV. Till then:
  1. $p(e)$ stands for the same formula as $p(x)$

Admissibility Caveats

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



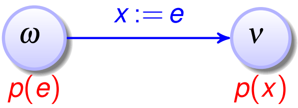
Elegant understanding is via uniform substitutions in Part IV. Till then:

1. $p(e)$ stands for the same formula as $p(x)$
2. except all free occurrences of x are replaced by e

- $[x := x + y]\, x \leq y^2 \leftrightarrow x + y \leq y^2$
- $[x := x^2]\forall x\, (x \geq 0) \leftrightarrow \forall x\, (x^2 \geq 0)$
- $[x := x + y]\forall y\, (x \leq y^2) \leftrightarrow \forall y\, (x + y \leq y^2)$
- $[x := x + y][y := 5]x \geq 0 \leftrightarrow [y := 5]x + y \geq 0$
- $[y := 2b][(x := x+y; x' = y)^*]x \geq y \leftrightarrow [(x := x+2b; x' = 2b)^*]x \geq 2b$

Admissibility Caveats

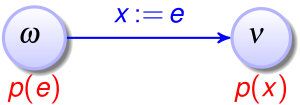
[:=] $[x := e]p(x) \leftrightarrow p(e)$



- Elegant understanding is via uniform substitutions in Part IV. Till then:
  1. $p(e)$ stands for the same formula as $p(x)$
  2. except all free occurrences of x are replaced by e
  3. but x cannot occur in $p(x)$ bound in a quantifier or a modality with an assignment or ODE for x
  - $[x := x + y]\, x \leq y^2 \leftrightarrow x + y \leq y^2$
  - $[x := x^2]\forall x\, (x \geq 0) \leftrightarrow \forall x\, (x^2 \geq 0)$
  - $[x := x + y]\forall y\, (x \leq y^2) \leftrightarrow \forall y\, (x + y \leq y^2)$
  - $[x := x + y][y := 5]x \geq 0 \leftrightarrow [y := 5]x + y \geq 0$
  - $[y := 2b][(x := x+y; x' = y)^*]x \geq y \leftrightarrow [(x := x+2b; x' = 2b)^*]x \geq 2b$

Admissibility Caveats

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



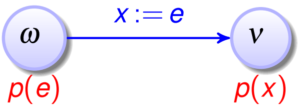
- Elegant understanding is via uniform substitutions in Part IV. Till then:

1. $p(e)$ stands for the same formula as $p(x)$
2. except all free occurrences of x are replaced by e
3. but x cannot occur in $p(x)$ bound in a quantifier or a modality with an assignment or ODE for x or any variable of e

- $[x := x + y]\, x \leq y^2 \leftrightarrow x + y \leq y^2$
- $[x := x^2]\forall x\, (x \geq 0) \leftrightarrow \forall x\, (x^2 \geq 0)$
- $[x := x + y]\forall y\, (x \leq y^2) \leftrightarrow \forall y\, (x + y \leq y^2)$
- $[x := x + y][y := 5]x \geq 0 \leftrightarrow [y := 5]x + y \geq 0$
- $[y := 2b][(x := x+y; x' = y)^*]x \geq y \leftrightarrow [(x := x+2b; x' = 2b)^*]x \geq 2b$

Admissibility Caveats

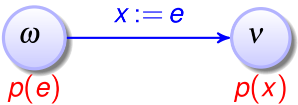
$[:=]$ $[x := e]p(x) \leftrightarrow p(e)$



- Elegant understanding is via uniform substitutions in Part IV. Till then:
  1. $p(e)$ stands for the same formula as $p(x)$
  2. except all free occurrences of x are replaced by e
  3. but x cannot occur in $p(x)$ bound in a quantifier or a modality with an assignment or ODE for x or any variable of e

- $[x := x + y]\, x \leq y^2 \leftrightarrow x + y \leq y^2$
- $[x := x^2]\forall x\, (x \geq 0) \leftrightarrow \forall x\, (x^2 \geq 0)$
- $[x := x + y]\forall y\, (x \leq y^2) \leftrightarrow \forall y\, (x + y \leq y^2)$
- $[x := x + y][y := 5]x \geq 0 \leftrightarrow [y := 5]x + y \geq 0$
- $[y := 2b][(x := x+y; x' = y)^*]x \geq y \leftrightarrow [(x := x+2b; x' = 2b)^*]x \geq 2b$

Admissibility Caveats



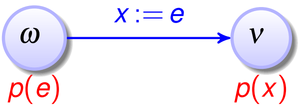
$[:=]$ $[x := e]p(x) \leftrightarrow p(e)$

- Elegant understanding is via uniform substitutions in Part IV. Till then:
  1. $p(e)$ stands for the same formula as $p(x)$
  2. except all free occurrences of x are replaced by e
  3. but x cannot occur in $p(x)$ bound in a quantifier or a modality with an assignment or ODE for x or any variable of e

  ✓ $[x := x + y]\, x \leq y^2 \leftrightarrow x + y \leq y^2$ is instance of $[:=]$

  - $[x := x^2]\forall x\, (x \geq 0) \leftrightarrow \forall x\, (x^2 \geq 0)$
  - $[x := x + y]\forall y\, (x \leq y^2) \leftrightarrow \forall y\, (x + y \leq y^2)$
  - $[x := x + y][y := 5]x \geq 0 \leftrightarrow [y := 5]x + y \geq 0$
  - $[y := 2b][(x := x+y; x' = y)^*]x \geq y \leftrightarrow [(x := x+2b; x' = 2b)^*]x \geq 2b$

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



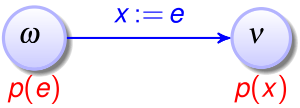
- Elegant understanding is via uniform substitutions in Part IV. Till then:
  1. $p(e)$ stands for the same formula as $p(x)$
  2. except all free occurrences of x are replaced by e
  3. but x cannot occur in $p(x)$ bound in a quantifier or a modality with an assignment or ODE for x or any variable of e

✓ $[x := x + y]\, x \leq y^2 \leftrightarrow x + y \leq y^2$ is instance of $[:=]$

- $[x := x^2]\forall x\, (x \geq 0) \leftrightarrow \forall x\, (x^2 \geq 0)$
- $[x := x + y]\forall y\, (x \leq y^2) \leftrightarrow \forall y\, (x + y \leq y^2)$
- $[x := x + y][y := 5]x \geq 0 \leftrightarrow [y := 5]x + y \geq 0$
- $[y := 2b][(x := x + y; x' = y)^*]x \geq y \leftrightarrow [(x := x + 2b; x' = 2b)^*]x \geq 2b$

Admissibility Caveats

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



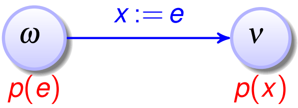
- Elegant understanding is via uniform substitutions in Part IV. Till then:
  1. $p(e)$ stands for the same formula as $p(x)$
  2. except all free occurrences of x are replaced by e
  3. but x cannot occur in $p(x)$ bound in a quantifier or a modality with an assignment or ODE for x or any variable of e

✓ $[x := x + y]\, x \leq y^2 \leftrightarrow x + y \leq y^2$ is instance of $[:=]$

× $[x := x^2]\forall x\,(x \geq 0) \leftrightarrow \forall x\,(x^2 \geq 0)$ x bound by $\forall x$

- $[x := x + y]\forall y\,(x \leq y^2) \leftrightarrow \forall y\,(x + y \leq y^2)$
- $[x := x + y][y := 5]x \geq 0 \leftrightarrow [y := 5]x + y \geq 0$
- $[y := 2b][(x := x+y; x' = y)^*]x \geq y \leftrightarrow [(x := x+2b; x' = 2b)^*]x \geq 2b$

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



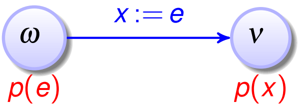
- Elegant understanding is via uniform substitutions in Part IV. Till then:
  1. $p(e)$ stands for the same formula as $p(x)$
  2. except all free occurrences of x are replaced by e
  3. but x cannot occur in $p(x)$ bound in a quantifier or a modality with an assignment or ODE for x or any variable of e

✓ $[x := x+y]\, x \leq y^2 \leftrightarrow x+y \leq y^2$ is instance of $[:=]$

× $[x := x^2]\forall x\,(x \geq 0) \leftrightarrow \forall x\,(x^2 \geq 0)$ x bound by $\forall x$

- $[x := x+y]\forall y\,(x \leq y^2) \leftrightarrow \forall y\,(x+y \leq y^2)$
- $[x := x+y][y := 5]x \geq 0 \leftrightarrow [y := 5]x+y \geq 0$
- $[y := 2b][(x := x+y; x' = y)^*]x \geq y \leftrightarrow [(x := x+2b; x' = 2b)^*]x \geq 2b$

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

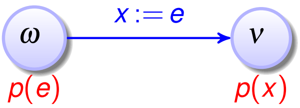


- Elegant understanding is via uniform substitutions in Part IV. Till then:
  1. $p(e)$ stands for the same formula as $p(x)$
  2. except all free occurrences of x are replaced by e
  3. but x cannot occur in $p(x)$ bound in a quantifier or a modality with an assignment or ODE for x or any variable of e

- ✓ $[x := x + y]\, x \leq y^2 \leftrightarrow x + y \leq y^2$ is instance of [:=]
- × $[x := x^2]\forall x\, (x \geq 0) \leftrightarrow \forall x\, (x^2 \geq 0)$ x bound by $\forall x$
- × $[x := x + y]\forall y\, (x \leq y^2) \leftrightarrow \forall y\, (x + y \leq y^2)$ var of $x{+}y$ bound by $\forall y$
- $[x := x + y][y := 5]x{\geq}0 \leftrightarrow [y := 5]x + y{\geq}0$
- $[y := 2b][(x := x{+}y; x' = y)^*]x{\geq}y \leftrightarrow [(x := x{+}2b; x' = 2b)^*]x{\geq}2b$

Admissibility Caveats

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



- Elegant understanding is via uniform substitutions in Part IV. Till then:

1. $p(e)$ stands for the same formula as $p(x)$
2. except all free occurrences of x are replaced by e
3. but x cannot occur in $p(x)$ bound in a quantifier or a modality with an assignment or ODE for x or any variable of e

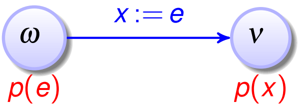
✓ $[x := x + y]\, x \leq y^2 \leftrightarrow x + y \leq y^2$ is instance of [:=]

× $[x := x^2]\forall x\, (x \geq 0) \leftrightarrow \forall x\, (x^2 \geq 0)$ x bound by $\forall x$

× $[x := x + y]\forall y\, (x \leq y^2) \leftrightarrow \forall y\, (x + y \leq y^2)$ var of $x+y$ bound by $\forall y$

- $[x := x + y][y := 5]x \geq 0 \leftrightarrow [y := 5]x + y \geq 0$
- $[y := 2b][(x := x+y; x' = y)^*]x \geq y \leftrightarrow [(x := x+2b; x' = 2b)^*]x \geq 2b$

Admissibility Caveats



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

- Elegant understanding is via uniform substitutions in Part IV. Till then:

1. $p(e)$ stands for the same formula as $p(x)$
2. except all free occurrences of x are replaced by e
3. but x cannot occur in $p(x)$ bound in a quantifier or a modality with an assignment or ODE for x or any variable of e

✓ $[x := x + y]\, x \leq y^2 \leftrightarrow x + y \leq y^2$ is instance of [:=]

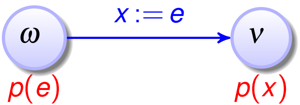
× $[x := x^2]\forall x\, (x \geq 0) \leftrightarrow \forall x\, (x^2 \geq 0)$ x bound by $\forall x$

× $[x := x + y]\forall y\, (x \leq y^2) \leftrightarrow \forall y\, (x + y \leq y^2)$ var of $x{+}y$ bound by $\forall y$

× $[x := x + y][y := 5]x{\geq}0 \leftrightarrow [y := 5]x + y{\geq}0$ var of $x{+}y$ bound $y := 5$

- $[y := 2b][(x := x{+}y; x' = y)^*]x{\geq}y \leftrightarrow [(x := x{+}2b; x' = 2b)^*]x{\geq}2b$

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



- Elegant understanding is via uniform substitutions in Part IV. Till then:

1. $p(e)$ stands for the same formula as $p(x)$
2. except all free occurrences of x are replaced by e
3. but x cannot occur in $p(x)$ bound in a quantifier or a modality with an assignment or ODE for x or any variable of e

✓ $[x := x + y]\, x \leq y^2 \leftrightarrow x + y \leq y^2$ is instance of $[:=]$

× $[x := x^2]\forall x\, (x \geq 0) \leftrightarrow \forall x\, (x^2 \geq 0)$ x bound by $\forall x$

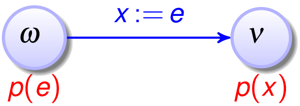
× $[x := x + y]\forall y\, (x \leq y^2) \leftrightarrow \forall y\, (x + y \leq y^2)$ var of $x{+}y$ bound by $\forall y$

× $[x := x + y][y := 5]x{\geq}0 \leftrightarrow [y := 5]x + y{\geq}0$ var of $x{+}y$ bound $y := 5$

- $[y := 2b][(x := x{+}y; x' = y)^*]x{\geq}y \leftrightarrow [(x := x{+}2b; x' = 2b)^*]x{\geq}2b$

Admissibility Caveats

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



- Elegant understanding is via uniform substitutions in Part IV. Till then:
  1. $p(e)$ stands for the same formula as $p(x)$
  2. except all free occurrences of x are replaced by e
  3. but x cannot occur in $p(x)$ bound in a quantifier or a modality with an assignment or ODE for x or any variable of e

✓ $[x := x + y]\, x \leq y^2 \leftrightarrow x + y \leq y^2$ is instance of $[:=]$

× $[x := x^2]\forall x\, (x \geq 0) \leftrightarrow \forall x\, (x^2 \geq 0)$ x bound by $\forall x$

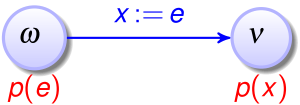
× $[x := x + y]\forall y\, (x \leq y^2) \leftrightarrow \forall y\, (x + y \leq y^2)$ var of $x+y$ bound by $\forall y$

× $[x := x + y][y := 5]x \geq 0 \leftrightarrow [y := 5]x + y \geq 0$ var of $x+y$ bound $y := 5$

✓ $[y := 2b][(x := x+y; x' = y)^*]x \geq y \leftrightarrow [(x := x+2b; x' = 2b)^*]x \geq 2b$ ok

Admissibility Caveats

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



- Elegant understanding is via uniform substitutions in Part IV. Till then:
  1. $p(e)$ stands for the same formula as $p(x)$
  2. except all free occurrences of x are replaced by e
  3. but x cannot occur in $p(x)$ bound in a quantifier or a modality with an assignment or ODE for x or any variable of e

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

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

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.
Logics of dynamical systems.
In LICS [6], 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.
The complete proof theory of hybrid systems.
In LICS [6], pages 541–550.
doi:10.1109/LICS.2012.64.

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