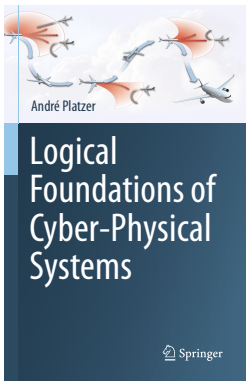


05: Dynamical Systems & Dynamic Axioms

Logical Foundations of Cyber-Physical Systems



André Platzer

Karlsruhe Institute of Technology
Department of Informatics

Computer Science Department
Carnegie Mellon University

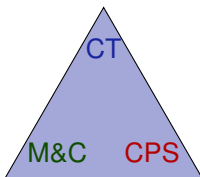
- 1 Learning Objectives
- 2 Approach & Reminder
- 3 Intermediate Conditions for CPS
- 4 Dynamic Axioms for Dynamical Systems
 - Nondeterministic Choices
 - Assignments
 - Differential Equations
 - Tests
 - Sequential Compositions
 - Loops
 - Soundness
 - Diamonds
- 5 First Bouncing Ball Proof
- 6 Summary



- 1 Learning Objectives
- 2 Approach & Reminder
- 3 Intermediate Conditions for CPS
- 4 Dynamic Axioms for Dynamical Systems
 - Nondeterministic Choices
 - Assignments
 - Differential Equations
 - Tests
 - Sequential Compositions
 - Loops
 - Soundness
 - Diamonds
- 5 First Bouncing Ball Proof
- 6 Summary

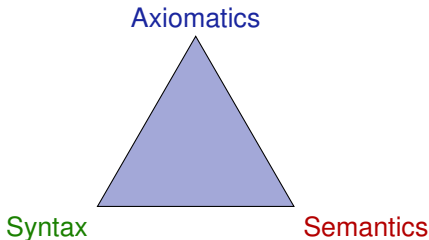


rigorous reasoning about CPS
dL as verification language



cyber+physics interaction
relate discrete+continuous

align semantics+reasoning
operational CPS effects



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?

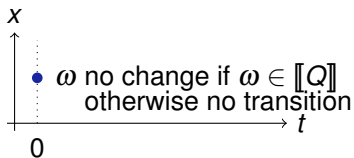
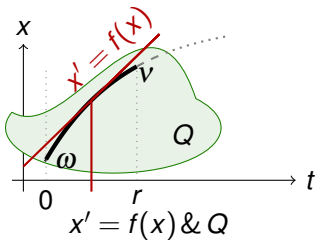
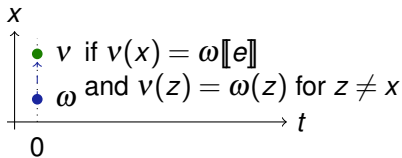
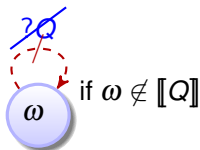
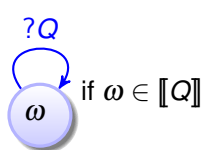
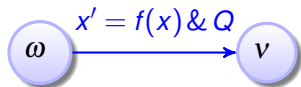
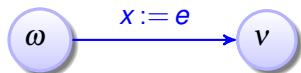
Axiomatics internalizes semantic relations into universal syntactic transformations.

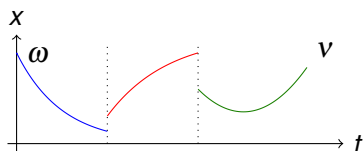
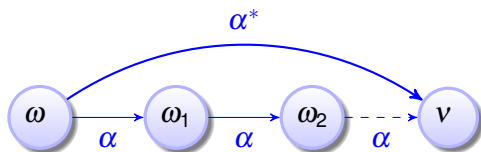
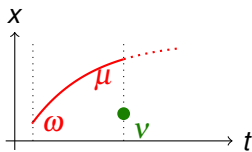
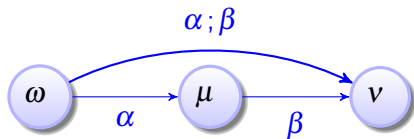
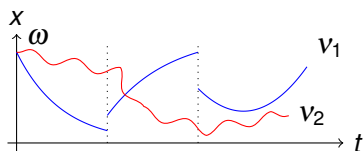
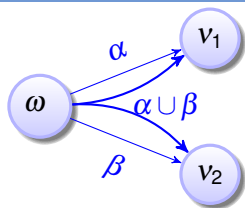
How does the semantics of A relate to semantics of $A \wedge B$, syntactically? If A is true, is $A \wedge B$ true, too? Conversely?

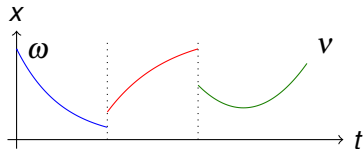
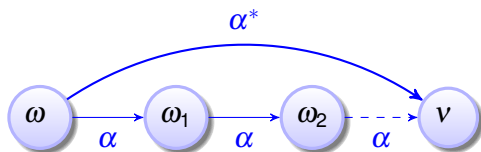
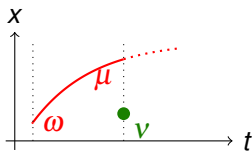
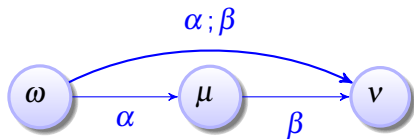
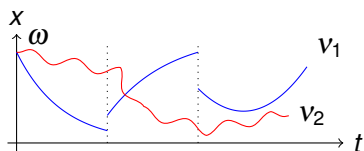
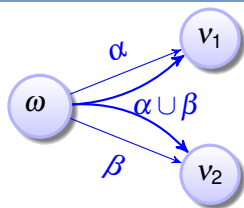
- 1 Learning Objectives
- 2 Approach & Reminder
- 3 Intermediate Conditions for CPS
- 4 Dynamic Axioms for Dynamical Systems
 - Nondeterministic Choices
 - Assignments
 - Differential Equations
 - Tests
 - Sequential Compositions
 - Loops
 - Soundness
 - Diamonds
- 5 First Bouncing Ball Proof
- 6 Summary

Logical guiding principle: Compositionality

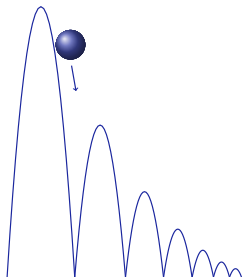
- 1 Every CPS is modeled by a hybrid program (or game ...)
- 2 All hybrid programs are combinations of simpler hybrid programs (by a program operator such as \cup and $;$ and $*$)
- 3 All CPS can be analyzed if only we identify one suitable analysis technique for each operator.
- 4 Analysis of a big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







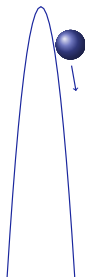
compositional semantics \Rightarrow compositional proofs!



Example (Quantum the Bouncing Ball)

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

$$[(\{x' = v, v' = -g \wedge x \geq 0\}; (?x=0; v := -cv \cup ?x \neq 0))^*] (0 \leq x \wedge x \leq H)$$



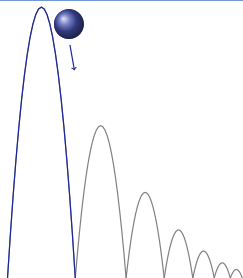
Example (Quantum the Bouncing Ball)

(Single-hop)

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

$$\left[\{x' = v, v' = -g \wedge x \geq 0\}; (?x=0; v := -cv \cup ?x \neq 0) \right] (0 \leq x \wedge x \leq H)$$

Removing the repetition grotesquely changes the behavior to a single hop



Example (Quantum the Bouncing Ball)

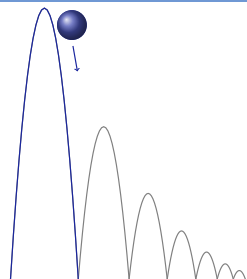
(Single-hop)

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

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

Removing the repetition grotesquely changes the behavior to a single hop

Conjecture: Quantum the Acrophobic Bouncing Ball



How to prove ;

Example (Quantum the Bouncing Ball)

(Single-hop)

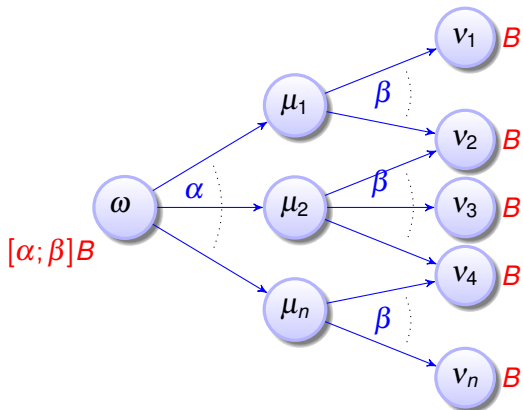
$$0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0 \rightarrow$$

$$\left[\{x' = v, v' = -g \wedge x \geq 0\}; (?x=0; v := -cv \cup ?x \neq 0) \right] (0 \leq x \wedge x \leq H)$$

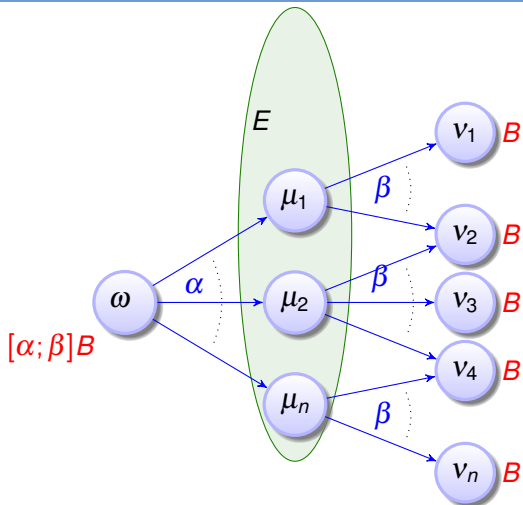
Removing the repetition grotesquely changes the behavior to a single hop

- 1 Learning Objectives
- 2 Approach & Reminder
- 3 Intermediate Conditions for CPS**
- 4 Dynamic Axioms for Dynamical Systems
 - Nondeterministic Choices
 - Assignments
 - Differential Equations
 - Tests
 - Sequential Compositions
 - Loops
 - Soundness
 - Diamonds
- 5 First Bouncing Ball Proof
- 6 Summary

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

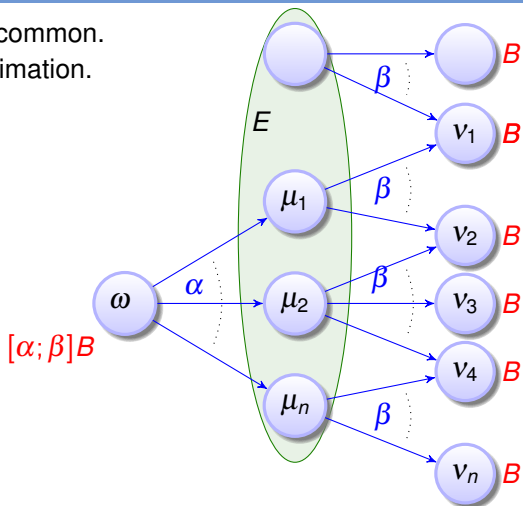


$$H; \frac{}{A \rightarrow [\alpha; \beta]B}$$



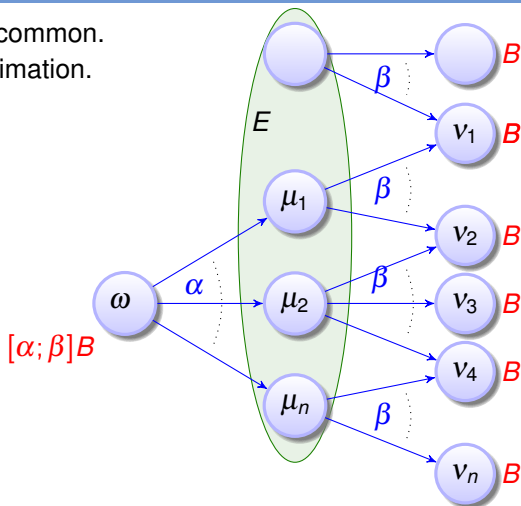
E summarizes what μ_i have in common.
 E is often imprecise overapproximation.

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



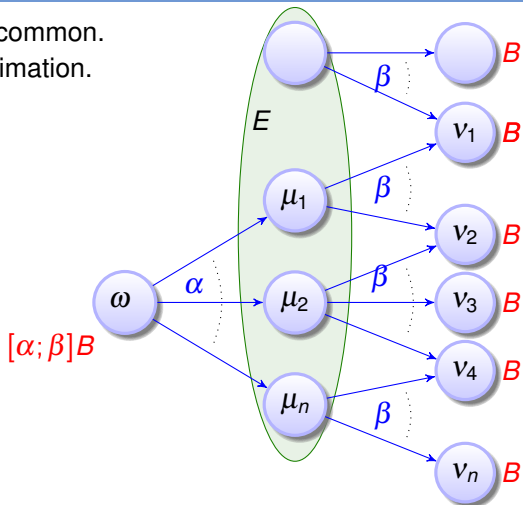
E summarizes what μ_i have in common.
 E is often imprecise overapproximation.
 Just need to find this E ...

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



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

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



Example (Quantum the Bouncing Ball)

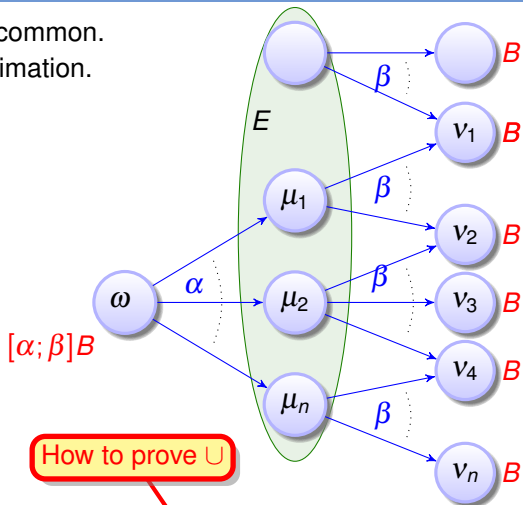
(Single-hop)

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

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

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

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



Example (Quantum the Bouncing Ball)

(Single-hop)

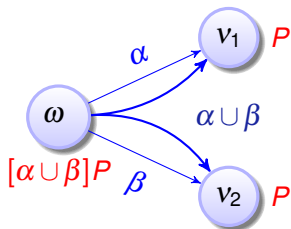
$$0 \leq x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0 \rightarrow [x' = v, v' = -g \ \& \ x \geq 0] E$$

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

- 1 Learning Objectives
- 2 Approach & Reminder
- 3 Intermediate Conditions for CPS
- 4 Dynamic Axioms for Dynamical Systems**
 - Nondeterministic Choices
 - Assignments
 - Differential Equations
 - Tests
 - Sequential Compositions
 - Loops
 - Soundness
 - Diamonds
- 5 First Bouncing Ball Proof
- 6 Summary

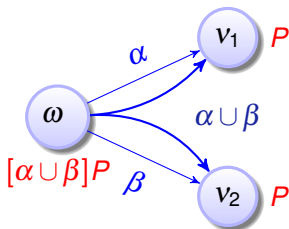
Semantics

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



Semantics

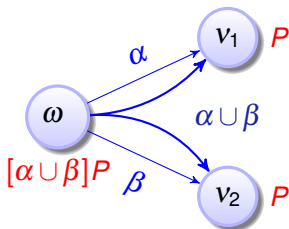
$$\llbracket \alpha \cup \beta \rrbracket = \llbracket \alpha \rrbracket \cup \llbracket \beta \rrbracket$$



- $\omega \in \llbracket \llbracket \alpha \cup \beta \rrbracket P \rrbracket$ iff $v \in \llbracket P \rrbracket$ for all v with $(\omega, v) \in \llbracket \alpha \cup \beta \rrbracket = \llbracket \alpha \rrbracket \cup \llbracket \beta \rrbracket$

Semantics

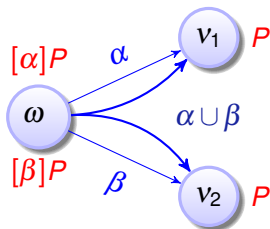
$$\llbracket \alpha \cup \beta \rrbracket = \llbracket \alpha \rrbracket \cup \llbracket \beta \rrbracket$$



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

Semantics

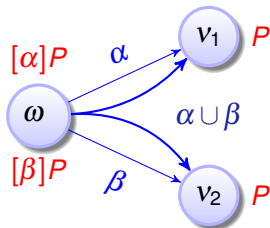
$$\llbracket \alpha \cup \beta \rrbracket = \llbracket \alpha \rrbracket \cup \llbracket \beta \rrbracket$$



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

Semantics

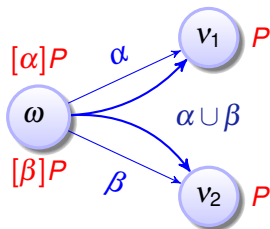
$$\llbracket \alpha \cup \beta \rrbracket = \llbracket \alpha \rrbracket \cup \llbracket \beta \rrbracket$$



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

Semantics

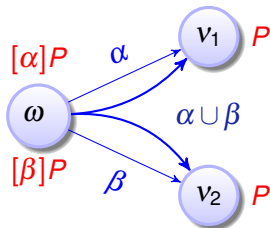
$$\llbracket \alpha \cup \beta \rrbracket = \llbracket \alpha \rrbracket \cup \llbracket \beta \rrbracket$$



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

Semantics

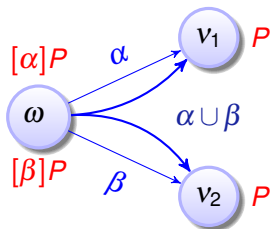
$$\llbracket \alpha \cup \beta \rrbracket = \llbracket \alpha \rrbracket \cup \llbracket \beta \rrbracket$$



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

Semantics

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

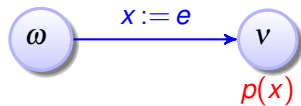


- $\omega \in \llbracket [\alpha \cup \beta]P \rrbracket$ iff $v \in \llbracket P \rrbracket$ for all v with $(\omega, v) \in \llbracket \alpha \cup \beta \rrbracket = \llbracket \alpha \rrbracket \cup \llbracket \beta \rrbracket$
- Then $v \in \llbracket P \rrbracket$ for all v with $(\omega, v) \in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

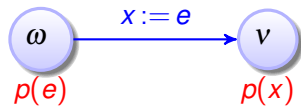
Lemma

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

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

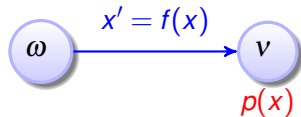
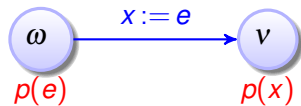


$[:=] [x := e]p(x) \leftrightarrow p(e)$



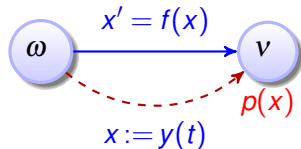
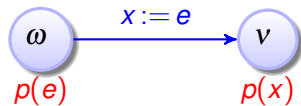
$$[:=] [x := e]p(x) \leftrightarrow p(e)$$

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



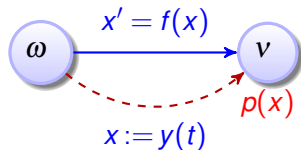
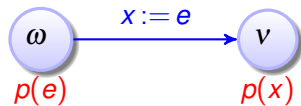
$$[:=] [x := e]p(x) \leftrightarrow p(e)$$

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



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

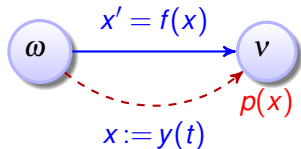
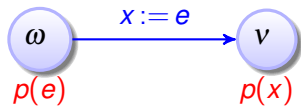
$$['] [x' = f(x)]p(x) \leftrightarrow \forall t \geq 0 [x := y(t)]p(x)$$



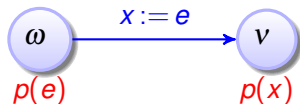
$$[:=] [x := e]p(x) \leftrightarrow p(e)$$

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

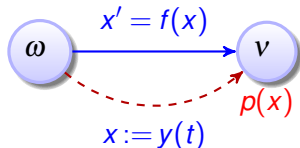
$$['] [x' = f(x) \& q(x)]p(x) \leftrightarrow \forall t \geq 0 ([x := y(t)]p(x))$$



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

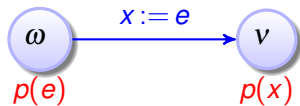


$$['] [x' = f(x)]p(x) \leftrightarrow \forall t \geq 0 [x := y(t)]p(x)$$

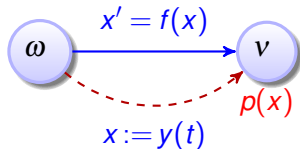


$$['] [x' = f(x) \& q(x)]p(x) \leftrightarrow \forall t \geq 0 (\forall 0 \leq s \leq t q(y(s)) \rightarrow [x := y(t)]p(x))$$

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



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



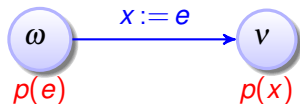
$$['] [x' = f(x) \& q(x)]p(x) \leftrightarrow \forall t \geq 0 (\forall 0 \leq s \leq t q(y(s)) \rightarrow [x := y(t)]p(x))$$

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

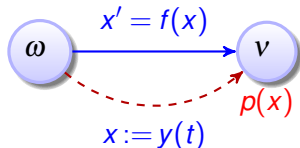


if $\omega \in \llbracket Q \rrbracket$

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



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



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

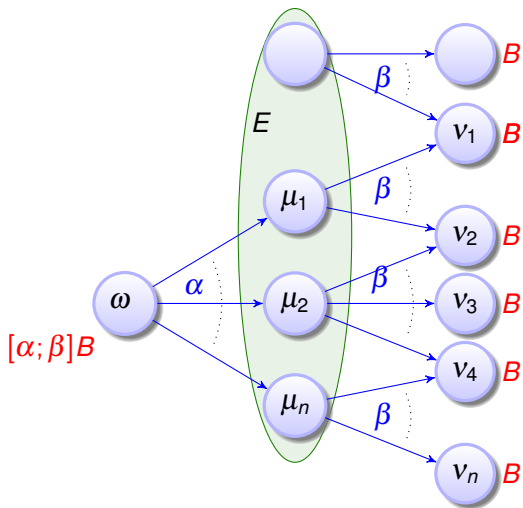
$$[?] [?Q]P \leftrightarrow (Q \rightarrow P)$$



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

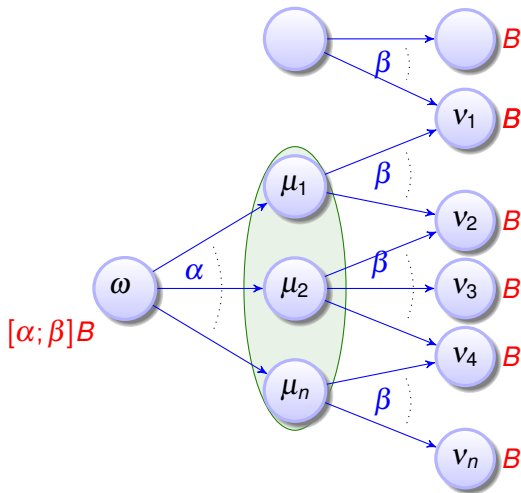
What is the most precise E summary?

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



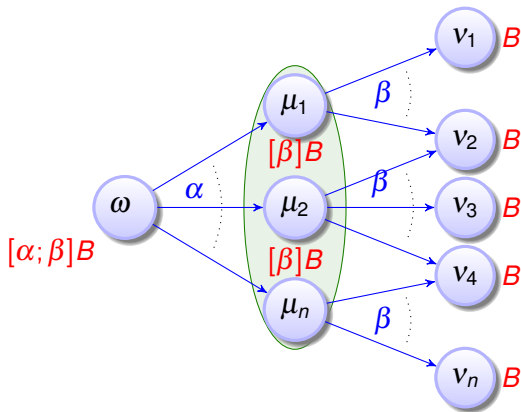
What is the most precise E summary?

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



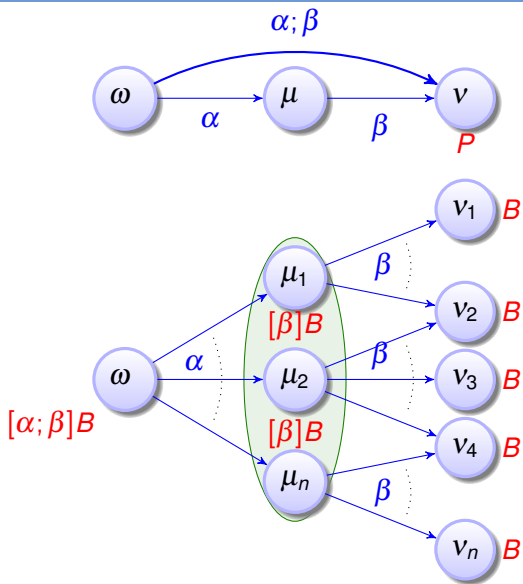
What is the most precise E summary? $[\beta]B$

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



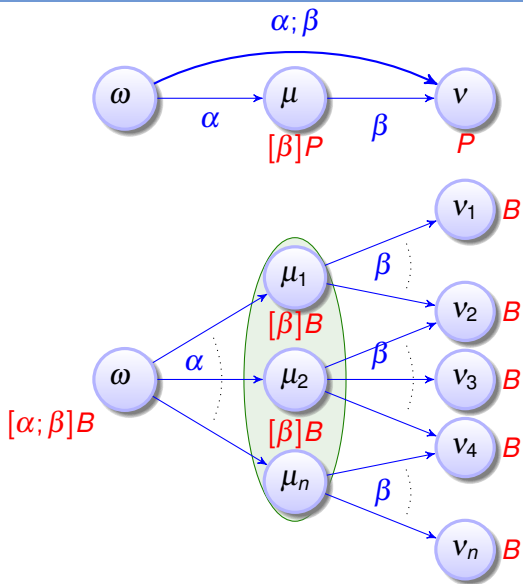
$[\cdot] [\alpha; \beta]P \leftrightarrow$

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



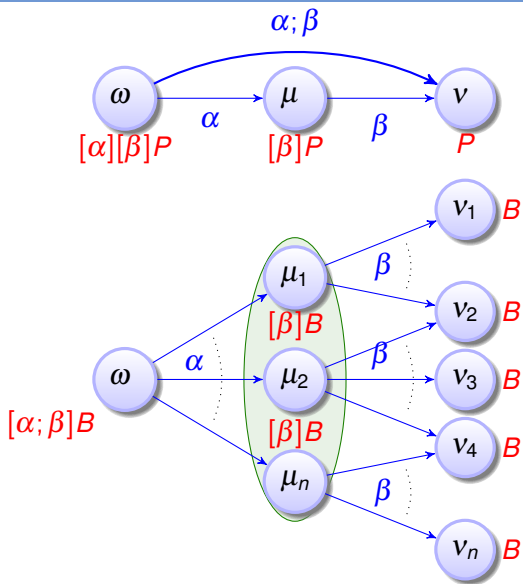
$[\cdot] [\alpha; \beta] P \leftrightarrow$

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



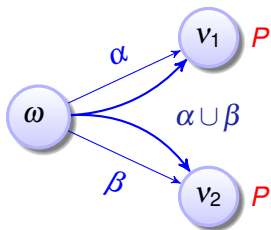
$$[;] [\alpha; \beta]P \leftrightarrow [\alpha][\beta]P$$

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

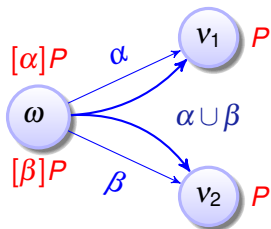


compositional semantics \Rightarrow compositional axioms!

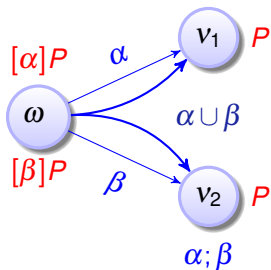
$[\cup] [\alpha \cup \beta] P \leftrightarrow$



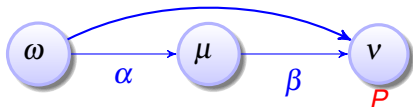
$$[U] [\alpha \cup \beta] P \leftrightarrow [\alpha] P \wedge [\beta] P$$



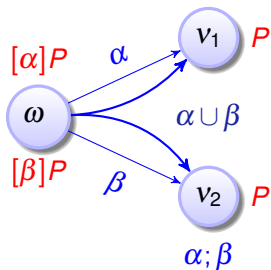
$$[\cup] [\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$$



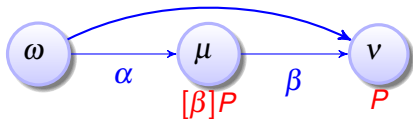
$$[;] [\alpha; \beta]P \leftrightarrow$$



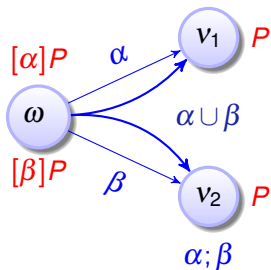
$$[\cup] [\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$$



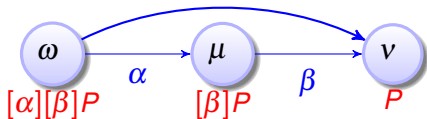
$$[;] [\alpha; \beta]P \leftrightarrow$$



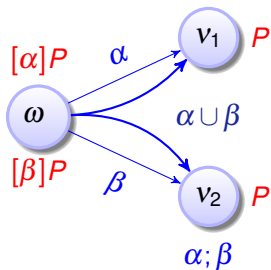
$$[\cup] [\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$$



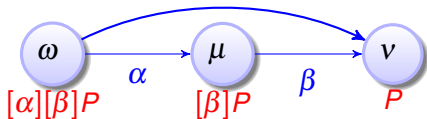
$$[;] [\alpha; \beta]P \leftrightarrow [\alpha][\beta]P$$



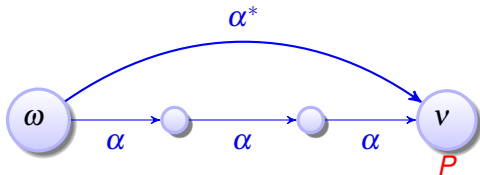
$$[U] [\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$$



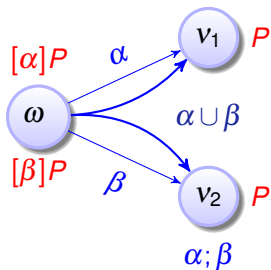
$$[;] [\alpha; \beta]P \leftrightarrow [\alpha][\beta]P$$



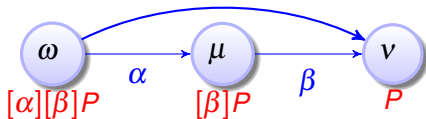
$$[*] [\alpha^*]P \leftrightarrow$$



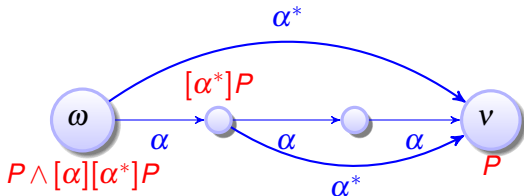
$$[U] [\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$$



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



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



Lemma

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

Lemma

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

Lemma

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

Proof

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

$(\omega, \nu) \in \llbracket \alpha \cup \beta \rrbracket$ iff $(\omega, \nu) \in \llbracket \alpha \rrbracket$ or $(\omega, \nu) \in \llbracket \beta \rrbracket$.

Thus, $\omega \in \llbracket [\alpha \cup \beta]P \rrbracket$ iff both $\omega \in \llbracket [\alpha]P \rrbracket$ and $\omega \in \llbracket [\beta]P \rrbracket$. □

Lemma

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

Lemma

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

Proof

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

$(\omega, \nu) \in \llbracket \alpha \cup \beta \rrbracket$ iff $(\omega, \nu) \in \llbracket \alpha \rrbracket$ or $(\omega, \nu) \in \llbracket \beta \rrbracket$.

Thus, $\omega \in \llbracket [\alpha \cup \beta]P \rrbracket$ iff both $\omega \in \llbracket [\alpha]P \rrbracket$ and $\omega \in \llbracket [\beta]P \rrbracket$. □

Lemma

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

Proof

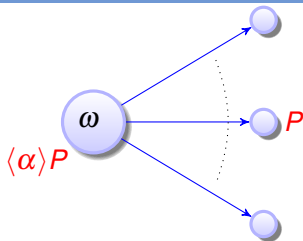
using $\llbracket \alpha; \beta \rrbracket = \llbracket \alpha \rrbracket \circ \llbracket \beta \rrbracket$.

$(\omega, \nu) \in \llbracket \alpha; \beta \rrbracket$ iff $(\omega, \mu) \in \llbracket \alpha \rrbracket$ and $(\mu, \nu) \in \llbracket \beta \rrbracket$ for some state μ .

Thus, $\omega \in \llbracket [\alpha; \beta]P \rrbracket$ iff $\mu \in \llbracket [\beta]P \rrbracket$ for all μ with $(\omega, \mu) \in \llbracket \alpha \rrbracket$.

That is, $\omega \in \llbracket [\alpha; \beta]P \rrbracket$ iff $\omega \in \llbracket [\alpha][\beta]P \rrbracket$. □

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

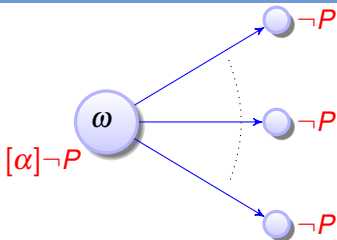


Semantics

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

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

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

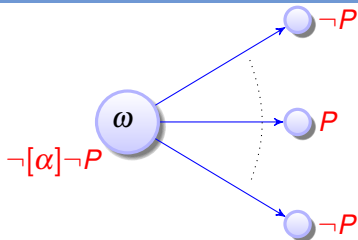


Semantics

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

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

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

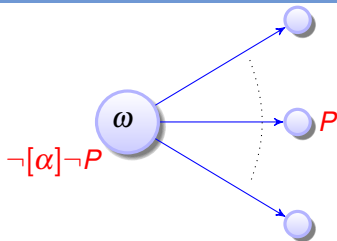


Semantics

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

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

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

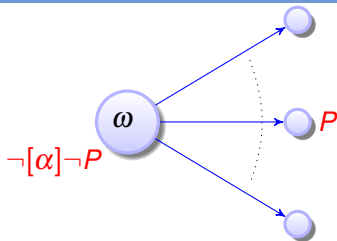


Semantics

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

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

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



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

Semantics

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

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

- 1 Learning Objectives
- 2 Approach & Reminder
- 3 Intermediate Conditions for CPS
- 4 Dynamic Axioms for Dynamical Systems
 - Nondeterministic Choices
 - Assignments
 - Differential Equations
 - Tests
 - Sequential Compositions
 - Loops
 - Soundness
 - Diamonds
- 5 First Bouncing Ball Proof**
- 6 Summary

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

A Proof of a Single-hop Bouncing Ball

$$\begin{array}{l}
 A \rightarrow \forall t \geq 0 \left(\left(H - \frac{g}{2}t^2 = 0 \rightarrow B\left(H - \frac{g}{2}t^2, -c(-gt)\right) \right) \wedge \left(H - \frac{g}{2}t^2 \geq 0 \rightarrow B\left(H - \frac{g}{2}t^2, -gt\right) \right) \right) \\
 \text{[:=]} \frac{A \rightarrow \forall t \geq 0 [x := H - \frac{g}{2}t^2] \left((x=0 \rightarrow B(x, -c(-gt))) \wedge (x \geq 0 \rightarrow B(x, -gt)) \right)}{A \rightarrow \forall t \geq 0 [x := H - \frac{g}{2}t^2][v := -gt] \left((x=0 \rightarrow B(x, -cv)) \wedge (x \geq 0 \rightarrow B(x, v)) \right)} \\
 \text{[:=]} \frac{A \rightarrow \forall t \geq 0 [x := H - \frac{g}{2}t^2][v := -gt] \left((x=0 \rightarrow B(x, -cv)) \wedge (x \geq 0 \rightarrow B(x, v)) \right)}{A \rightarrow \forall t \geq 0 [x := H - \frac{g}{2}t^2; v := -gt] \left((x=0 \rightarrow B(x, -cv)) \wedge (x \geq 0 \rightarrow B(x, v)) \right)} \\
 \text{[I]} \frac{A \rightarrow \forall t \geq 0 [x := H - \frac{g}{2}t^2; v := -gt] \left((x=0 \rightarrow B(x, -cv)) \wedge (x \geq 0 \rightarrow B(x, v)) \right)}{A \rightarrow [x'' = -g] \left((x=0 \rightarrow B(x, -cv)) \wedge (x \geq 0 \rightarrow B(x, v)) \right)} \\
 \text{[:=]} \frac{A \rightarrow [x'' = -g] \left((x=0 \rightarrow B(x, -cv)) \wedge (x \geq 0 \rightarrow B(x, v)) \right)}{A \rightarrow [x'' = -g] \left((x=0 \rightarrow [v := -cv]B(x, v)) \wedge (x \geq 0 \rightarrow B(x, v)) \right)} \\
 \text{[?],[?]} \frac{A \rightarrow [x'' = -g] \left((x=0 \rightarrow [v := -cv]B(x, v)) \wedge (x \geq 0 \rightarrow B(x, v)) \right)}{A \rightarrow [x'' = -g] \left([?x = 0][v := -cv]B(x, v) \wedge [?x \geq 0]B(x, v) \right)} \\
 \text{[I]} \frac{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)} \\
 \text{[U]} \frac{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)} \\
 \text{[I]} \frac{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

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

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

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

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

Resolving abbreviations at the top premise yields provable arithmetic:

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

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

A Proof of a Single-hop Bouncing Ball

Resolving abbreviations at the top premise yields provable arithmetic:

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

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

A Proof of a Single-hop Bouncing Ball

Resolving abbreviations at the top premise yields provable arithmetic:

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

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

Resolving abbreviations at the top premise yields provable arithmetic:

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

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

Exciting!

We have just formally verified our very first CPS!

A Proof of a Single-hop Bouncing Ball

Resolving abbreviations at the top premise yields provable arithmetic:

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

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.

- 1 Learning Objectives
- 2 Approach & Reminder
- 3 Intermediate Conditions for CPS
- 4 Dynamic Axioms for Dynamical Systems
 - Nondeterministic Choices
 - Assignments
 - Differential Equations
 - Tests
 - Sequential Compositions
 - Loops
 - Soundness
 - Diamonds
- 5 First Bouncing Ball Proof
- 6 Summary

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

equations of truth

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

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

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

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

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

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

One axiom for each HP operator

Using an axiom from left to right simplifies the HP structure

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

equations of truth

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

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

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

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

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

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

One axiom for each HP operator

Using an axiom from left to right simplifies the HP structure

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

equations of truth

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

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

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

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

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

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

One axiom for each HP operator

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

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

equations of truth

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

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

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

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

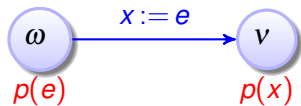
$$[*] [\alpha^*]P \leftrightarrow P \wedge [\alpha][\alpha^*]P$$

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

One axiom for each HP operator

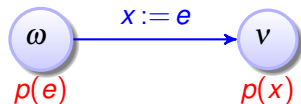
Using an axiom from left to right simplifies the HP structure except ...

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



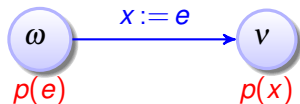
- ▶ Elegant understanding is via uniform substitutions in Part IV. Till then:

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



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

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

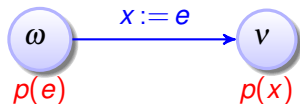


▶ Elegant understanding is via uniform substitutions in Part IV. Till then:

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

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

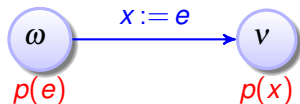
$$[:=] [x := e]p(x) \leftrightarrow p(e)$$



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

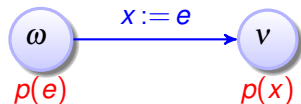
$$[:=] [x := e]p(x) \leftrightarrow p(e)$$



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

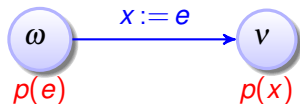
$$[:=] [x := e]p(x) \leftrightarrow p(e)$$



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

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



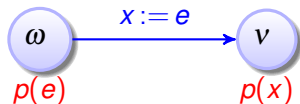
► Elegant understanding is via uniform substitutions in Part IV. Till then:

- 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 $[:=]$

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

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



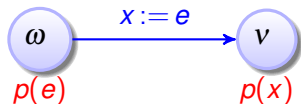
► Elegant understanding is via uniform substitutions in Part IV. Till then:

- 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 $[:=]$

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

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



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

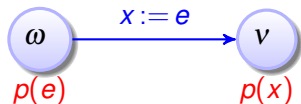
- 1 $p(e)$ stands for the same formula as $p(x)$
- 2 except **all** free occurrences of x are replaced by e
- 3 but x cannot occur in $p(x)$ bound in a quantifier or a modality with an assignment or ODE for x **or** any variable of e

✓ $[x := x + y]x \leq y^2 \leftrightarrow x + y \leq y^2$ 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:

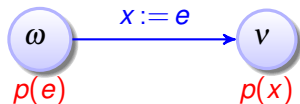
- 1 $p(e)$ stands for the same formula as $p(x)$
- 2 except **all** free occurrences of x are replaced by e
- 3 but x cannot occur in $p(x)$ bound in a quantifier or a modality with an assignment or ODE for x **or** any variable of e

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

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

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

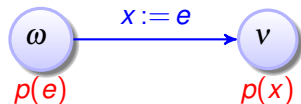
$$[:=] [x := e]p(x) \leftrightarrow p(e)$$



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

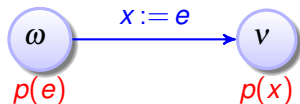
$$[:=] [x := e]p(x) \leftrightarrow p(e)$$



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

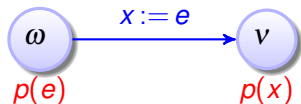
$$[:=] [x := e]p(x) \leftrightarrow p(e)$$



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

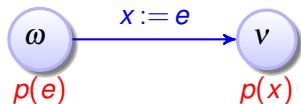
$$[:=] [x := e]p(x) \leftrightarrow p(e)$$



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

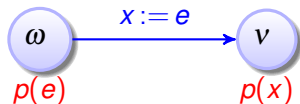
$$[:=] [x := e]p(x) \leftrightarrow p(e)$$



▶ 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

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



- ▶ 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, Cham, 2018.

[doi:10.1007/978-3-319-63588-0](https://doi.org/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](https://doi.org/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](https://doi.org/10.1109/LICS.2012.13).



André Platzer.

A complete uniform substitution calculus for differential dynamic logic.

J. Autom. Reas., 59(2):219–265, 2017.

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



André Platzer.

The complete proof theory of hybrid systems.

In LICS [6], pages 541–550.

[doi:10.1109/LICS.2012.64](https://doi.org/10.1109/LICS.2012.64).



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