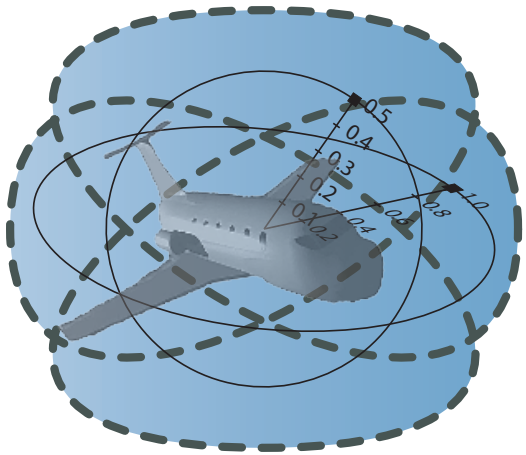
07: Control Loops & Invariants

15-424: Foundations of Cyber-Physical Systems

André Platzer

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



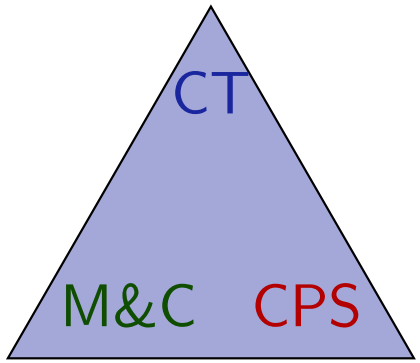
Outline

Outline

Learning Objectives

Control Loops & Invariants

rigorous reasoning for repetitions
identifying and expressing invariants
global vs. local reasoning
relating iterations to invariants
finitely accessible infinities
operationalize invariant construction
splitting & generalizations



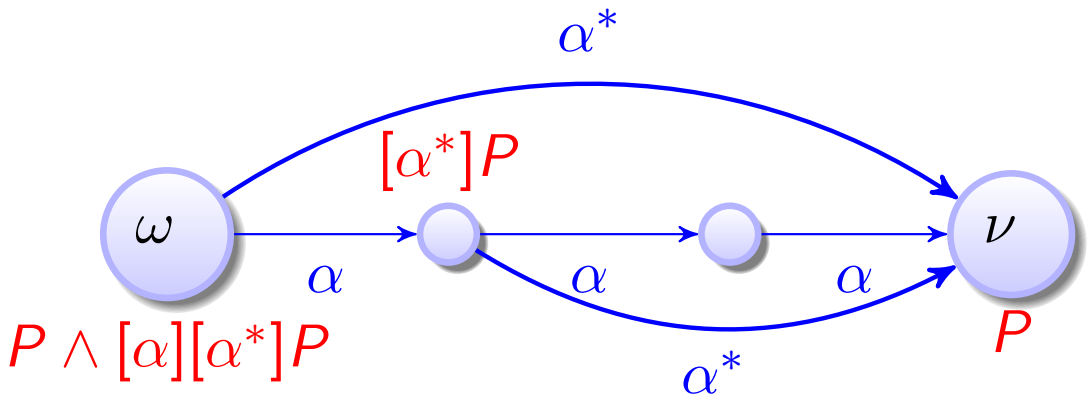
control loops
feedback mechanisms
dynamics of iteration

semantics of control loops
operational effects of control

Outline

Iteration Axiom

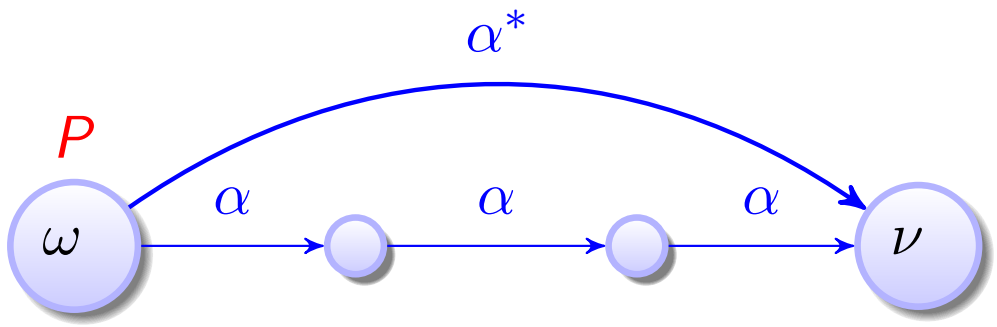
$$[^*]\quad [\alpha^*]P \leftrightarrow P \wedge [\alpha][\alpha^*]P$$



Induction Axiom

Lemma (I is sound)

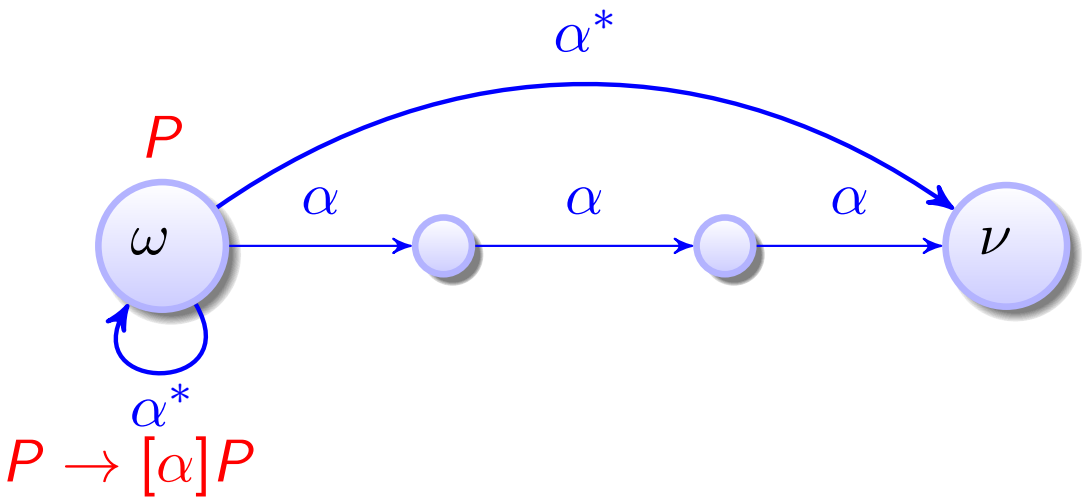
$$I \quad [\alpha^*]P \leftrightarrow P \wedge [\alpha^*](P \rightarrow [\alpha]P)$$



Induction Axiom

Lemma (I is sound)

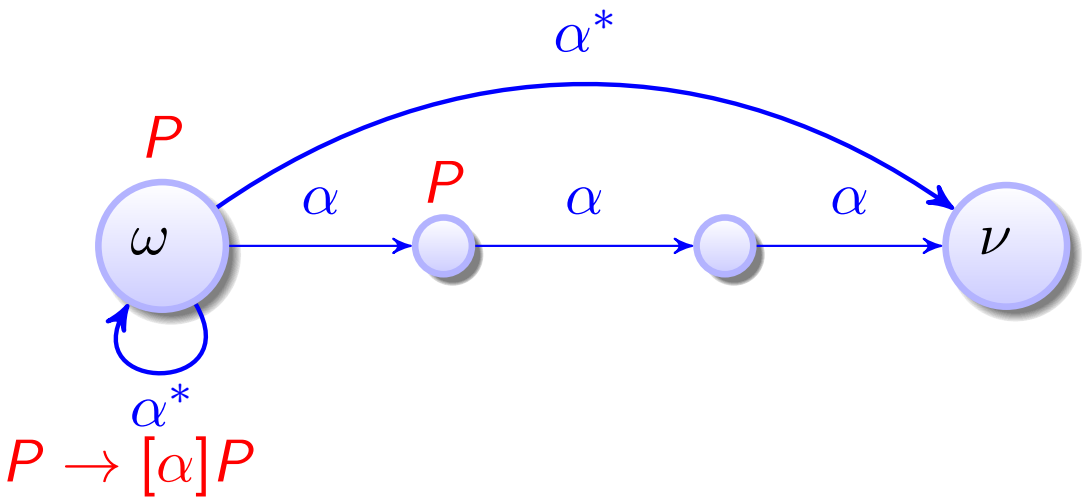
$$I \quad [\alpha^*]P \leftrightarrow P \wedge [\alpha^*](P \rightarrow [\alpha]P)$$



Induction Axiom

Lemma (I is sound)

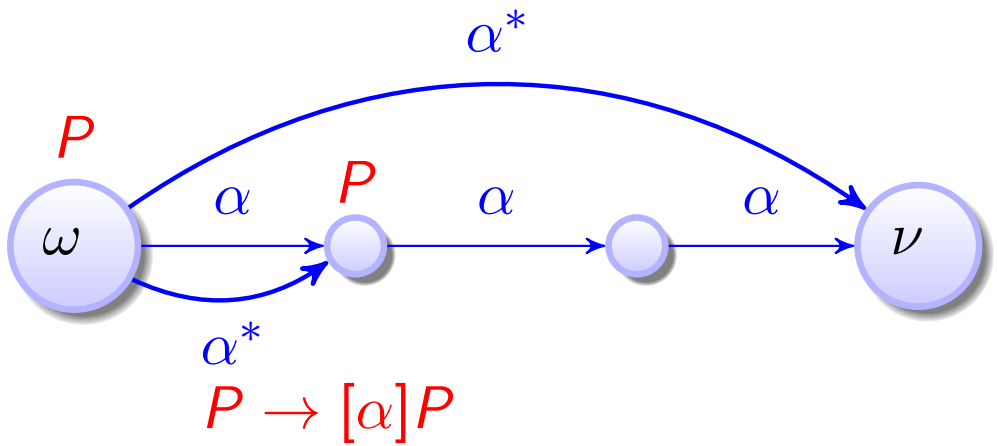
$$I \quad [\alpha^*]P \leftrightarrow P \wedge [\alpha^*](P \rightarrow [\alpha]P)$$



Induction Axiom

Lemma (I is sound)

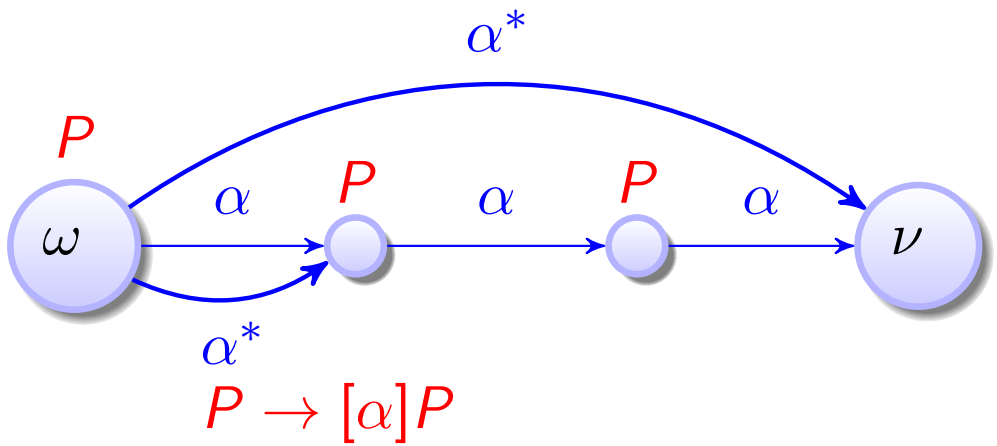
$$I \quad [\alpha^*]P \leftrightarrow P \wedge [\alpha^*](P \rightarrow [\alpha]P)$$



Induction Axiom

Lemma (I is sound)

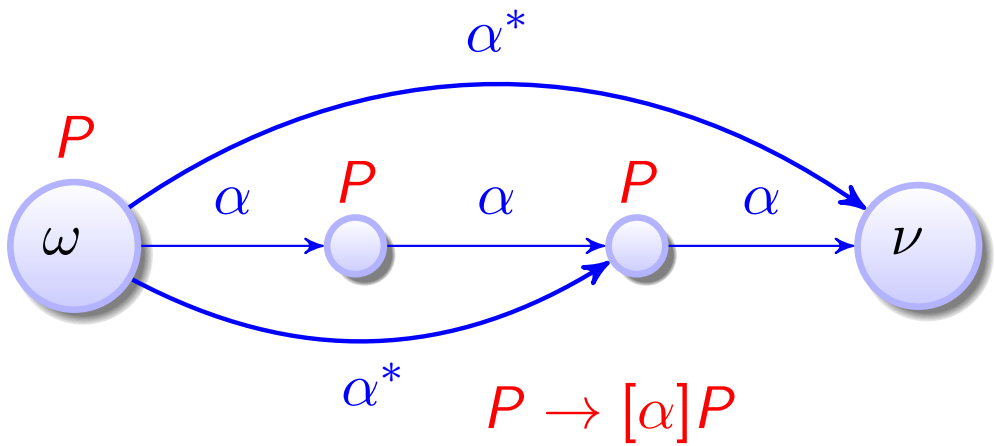
$$I \quad [\alpha^*]P \leftrightarrow P \wedge [\alpha^*](P \rightarrow [\alpha]P)$$



Induction Axiom

Lemma (I is sound)

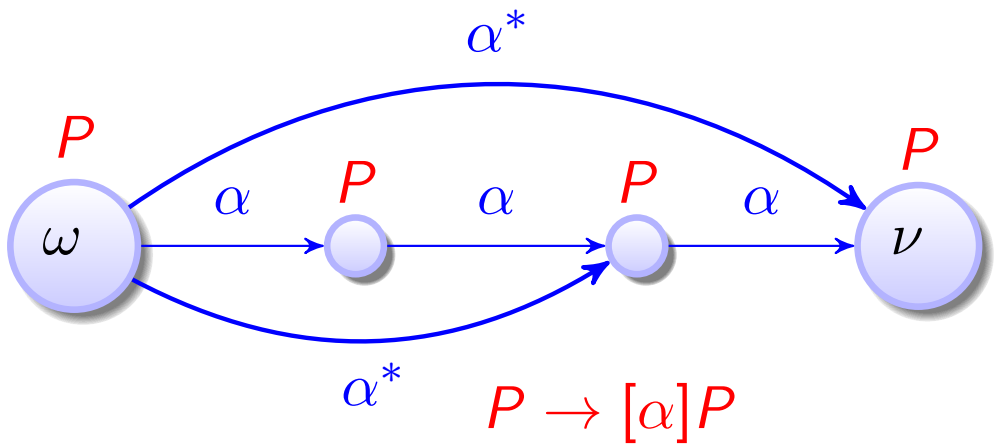
$$I \quad [\alpha^*]P \leftrightarrow P \wedge [\alpha^*](P \rightarrow [\alpha]P)$$



Induction Axiom

Lemma (I is sound)

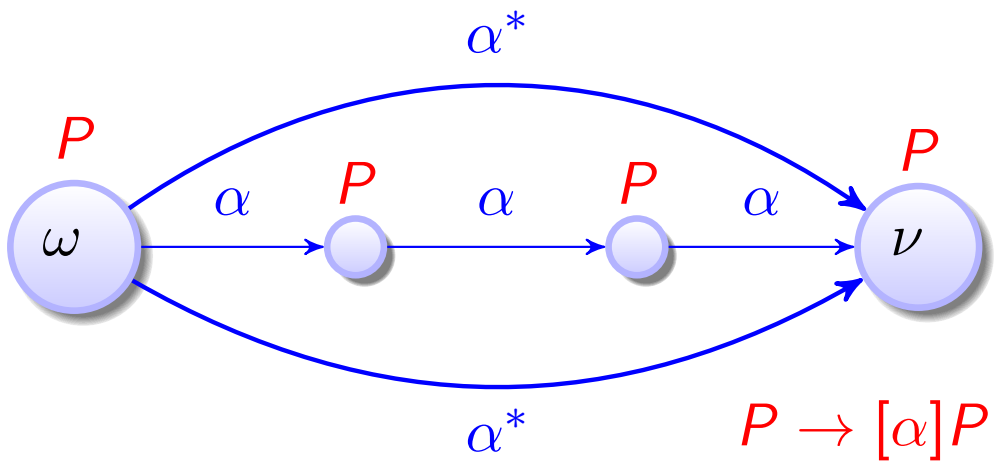
$$I \quad [\alpha^*]P \leftrightarrow P \wedge [\alpha^*](P \rightarrow [\alpha]P)$$



Induction Axiom

Lemma (I is sound)

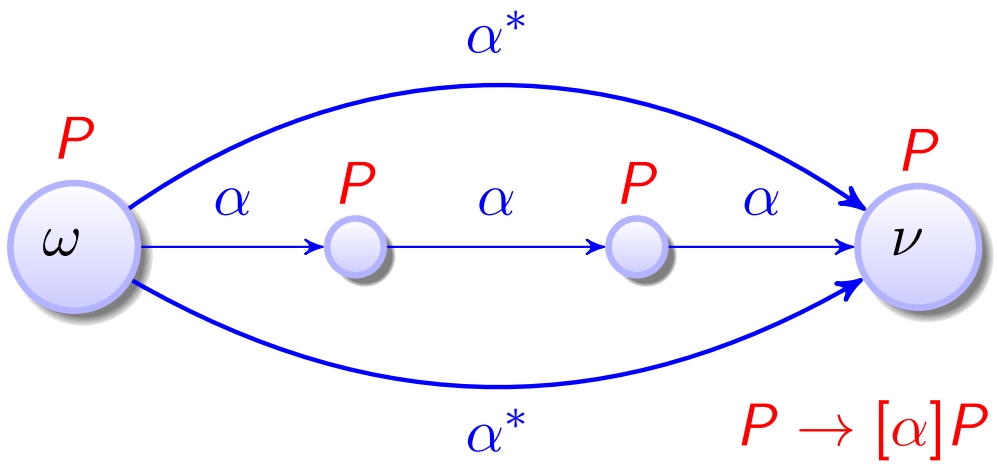
$$I \quad [\alpha^*]P \leftrightarrow P \wedge [\alpha^*](P \rightarrow [\alpha]P)$$



Induction Axiom

Lemma (I is sound)

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



Problem: Inductive proof for $[\alpha^*]P$ needs proof of $[\alpha^*](P \rightarrow [\alpha]P)$

Induction Rule for Loops

Generalize induction step $[\alpha^*](P \to [\alpha]P)$ by Gödel

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

Lemma (Loop induction rule ind is sound)

$$\mathit{ind}\ \frac{P \vdash [\alpha]P}{P \vdash [\alpha^*]P}$$

Induction Rule for Loops

Generalize induction step $[\alpha^*](P \to [\alpha]P)$ by Gödel

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

Lemma (Loop induction rule ind is sound)

$$\mathit{ind}\ \frac{P \vdash [\alpha]P}{P \vdash [\alpha^*]P}$$

Proof (Derived rule).

$$\cfrac{\cfrac{\cfrac{}{P \vdash P}\,\text{id}(*) \qquad \cfrac{\cfrac{P \vdash [\alpha]P}{\vdash P \to [\alpha]P}\,\to\text{R}}{P \vdash [\alpha^*](P \to [\alpha]P)}\,\text{G}}{P \vdash P \wedge [\alpha^*](P \to [\alpha]P)}\,\wedge\text{R}}{P \vdash [\alpha^*]P}\,\text{I}$$

Induction Rule for Loops

Generalize induction step $[\alpha^*](P \to [\alpha]P)$ by Gödel $\quad \mathsf{G}\ \dfrac{P}{[\alpha]P}$

Lemma (Loop induction rule ind is sound)

$$\mathit{ind}\ \frac{P \vdash [\alpha]P}{P \vdash [\alpha^*]P}$$

Proof (Derived rule).

$$\mathsf{I}\ \frac{\mathsf{id}\dfrac{*}{P \vdash P} \quad \wedge\mathsf{R}\dfrac{\mathsf{G}\dfrac{\to\mathsf{R}\dfrac{P \vdash [\alpha]P}{\vdash P \to [\alpha]P}}{P \vdash [\alpha^*](P \to [\alpha]P)}}{P \vdash P \wedge [\alpha^*](P \to [\alpha]P)}}{P \vdash [\alpha^*]P}$$

□

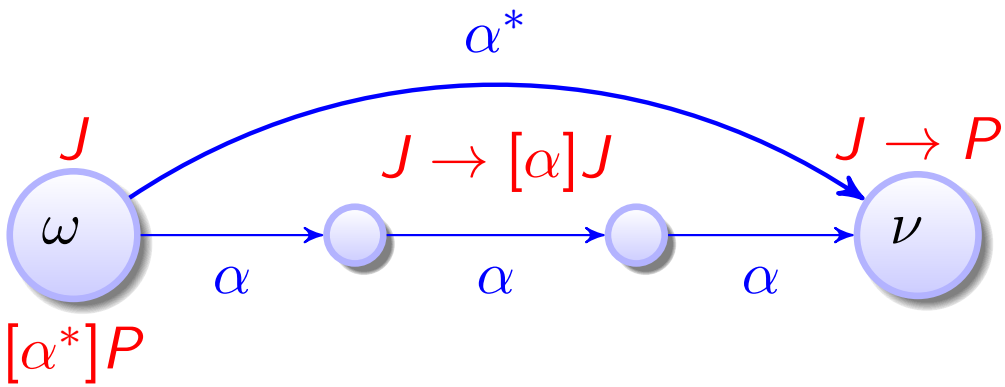
Problem: Rule ind is no equivalence. Its use of G may lose information: $[\alpha^*](P \to [\alpha]P)$ true but $P \vdash [\alpha]P$ is not valid.

Loop Invariants

Generalize postcondition to strong loop invariant J by $\mathrm{M}[\cdot]$ $\dfrac{P \to Q}{[\alpha]P \to [\alpha]Q}$

Lemma (Loop invariant rule loop is sound)

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



Loop Invariants

Generalize postcondition to strong loop invariant J by $\mathrm{M}[\cdot]$ $\dfrac{P \to Q}{[\alpha]P \to [\alpha]Q}$

Lemma (Loop invariant rule loop is sound)

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

Proof (Derived rule).

$$\cut\frac{\dfrac{\dfrac{J \vdash [\alpha]J}{\mathrm{ind}\dfrac{J \vdash [\alpha^*]J}{\to\mathrm{R}\dfrac{}{\Gamma \vdash J \to [\alpha^*]J, \Delta}}} \qquad \to\mathrm{L}\dfrac{\Gamma \vdash J, \Delta \qquad \mathrm{M}[\cdot]\dfrac{J \vdash P}{[\alpha^*]J \vdash [\alpha^*]P}}{\Gamma, J \to [\alpha^*]J \vdash [\alpha^*]P, \Delta}}{\Gamma \vdash [\alpha^*]P, \Delta}$$

Loop Invariants

Generalize postcondition to strong loop invariant J by $\mathrm{M}[\cdot]$ $\dfrac{P \to Q}{[\alpha]P \to [\alpha]Q}$

Lemma (Loop invariant rule loop is sound)

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

Proof (Derived rule).

$$\cfrac{\cfrac{\cfrac{J \vdash [\alpha]J}{\mathrm{ind}\ \cfrac{J \vdash [\alpha^*]J}{\to\mathrm{R}\ \Gamma \vdash J \to [\alpha^*]J, \Delta}} \qquad \cfrac{\Gamma \vdash J, \Delta \qquad \mathrm{M}[\cdot]\ \cfrac{J \vdash P}{[\alpha^*]J \vdash [\alpha^*]P}}{\to\mathrm{L}\ \Gamma, J \to [\alpha^*]J \vdash [\alpha^*]P, \Delta}}{\mathrm{cut}\ \Gamma \vdash [\alpha^*]P, \Delta}$$

□

Problem: Finding invariant J can be a challenge.

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

A Simple Discrete Loop Example

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

$$\rightarrow\text{R}\ \frac{\text{loop}\ \dfrac{x{\geq}8 \land 5{\geq}y \land y{\geq}0 \vdash J \quad J \vdash [x := x + y;\ y := x - 2 \cdot y]J \quad J \vdash x \geq 0}{x{\geq}8 \land 5{\geq}y \land y{\geq}0 \vdash [(x := x + y;\ y := x - 2 \cdot y)^*]\, x \geq 0}}{\vdash x{\geq}8 \land 5{\geq}y \land y{\geq}0 \rightarrow [(x := x + y;\ y := x - 2 \cdot y)^*]\, x \geq 0}$$

1. $J \equiv x \geq 0$

A Simple Discrete Loop Example

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

$$\rightarrow\text{R}\ \frac{\text{loop}\ \dfrac{x{\geq}8 \land 5{\geq}y \land y{\geq}0 \vdash J \quad J \vdash [x := x + y;\ y := x - 2 \cdot y]J \quad J \vdash x \geq 0}{x{\geq}8 \land 5{\geq}y \land y{\geq}0 \vdash [(x := x + y;\ y := x - 2 \cdot y)^*]\, x \geq 0}}{\vdash x{\geq}8 \land 5{\geq}y \land y{\geq}0 \rightarrow [(x := x + y;\ y := x - 2 \cdot y)^*]\, x \geq 0}$$

1. $J \equiv x \geq 0$ stronger: Lacks info about y

A Simple Discrete Loop Example

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

$$\to\text{R}\ \frac{\text{loop}\ \dfrac{x{\geq}8 \land 5{\geq}y \land y{\geq}0 \vdash J \quad J \vdash [x := x + y;\ y := x - 2 \cdot y]J \quad J \vdash x \geq 0}{x{\geq}8 \land 5{\geq}y \land y{\geq}0 \vdash [(x := x + y;\ y := x - 2 \cdot y)^*]\, x \geq 0}}{\vdash x{\geq}8 \land 5{\geq}y \land y{\geq}0 \to [(x := x + y;\ y := x - 2 \cdot y)^*]\, x \geq 0}$$

1. $J \equiv x \geq 0$ — stronger: Lacks info about y
2. $J \equiv x \geq 8 \land 5 \geq y \land y \geq 0$

A Simple Discrete Loop Example

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

$$\rightarrow\text{R}\ \frac{\text{loop}\ \dfrac{x{\geq}8 \land 5{\geq}y \land y{\geq}0 \vdash J \quad J \vdash [x := x + y;\ y := x - 2 \cdot y]J \quad J \vdash x \geq 0}{x{\geq}8 \land 5{\geq}y \land y{\geq}0 \vdash [(x := x + y;\ y := x - 2 \cdot y)^*]\, x \geq 0}}{\vdash x{\geq}8 \land 5{\geq}y \land y{\geq}0 \rightarrow [(x := x + y;\ y := x - 2 \cdot y)^*]\, x \geq 0}$$

1. $J \equiv x \geq 0$ — stronger: Lacks info about y
2. $J \equiv x \geq 8 \land 5 \geq y \land y \geq 0$ — weaker: Changes immediately

A Simple Discrete Loop Example

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

$$\rightarrow\text{R}\ \frac{\text{loop}\ \dfrac{x{\geq}8 \land 5{\geq}y \land y{\geq}0 \vdash J \quad J \vdash [x := x + y;\ y := x - 2 \cdot y]J \quad J \vdash x \geq 0}{x{\geq}8 \land 5{\geq}y \land y{\geq}0 \vdash [(x := x + y;\ y := x - 2 \cdot y)^*]\, x \geq 0}}{\vdash x{\geq}8 \land 5{\geq}y \land y{\geq}0 \rightarrow [(x := x + y;\ y := x - 2 \cdot y)^*]\, x \geq 0}$$

1. $J \equiv x \geq 0$ — stronger: Lacks info about y
2. $J \equiv x \geq 8 \land 5 \geq y \land y \geq 0$ — weaker: Changes immediately
3. $J \equiv x \geq 0 \land y \geq 0$

A Simple Discrete Loop Example

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

$$\rightarrow\text{R}\ \frac{\text{loop}\ \dfrac{x{\geq}8 \land 5{\geq}y \land y{\geq}0 \vdash J \quad J \vdash [x := x + y;\ y := x - 2 \cdot y]J \quad J \vdash x \geq 0}{x{\geq}8 \land 5{\geq}y \land y{\geq}0 \vdash [(x := x + y;\ y := x - 2 \cdot y)^*]\, x \geq 0}}{\vdash x{\geq}8 \land 5{\geq}y \land y{\geq}0 \rightarrow [(x := x + y;\ y := x - 2 \cdot y)^*]\, x \geq 0}$$

1. $J \equiv x \geq 0$ — stronger: Lacks info about y
2. $J \equiv x \geq 8 \land 5 \geq y \land y \geq 0$ — weaker: Changes immediately
3. $J \equiv x \geq 0 \land y \geq 0$ — no: y may become negative if $x < y$

A Simple Discrete Loop Example

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

$$\to\text{R}\ \frac{\text{loop}\ \dfrac{x{\geq}8 \land 5{\geq}y \land y{\geq}0 \vdash J \quad J \vdash [x := x + y;\ y := x - 2 \cdot y]J \quad J \vdash x \geq 0}{x{\geq}8 \land 5{\geq}y \land y{\geq}0 \vdash [(x := x + y;\ y := x - 2 \cdot y)^*]\, x \geq 0}}{\vdash x{\geq}8 \land 5{\geq}y \land y{\geq}0 \to [(x := x + y;\ y := x - 2 \cdot y)^*]\, x \geq 0}$$

1. $J \equiv x \geq 0$ — stronger: Lacks info about y
2. $J \equiv x \geq 8 \land 5 \geq y \land y \geq 0$ — weaker: Changes immediately
3. $J \equiv x \geq 0 \land y \geq 0$ — no: y may become negative if $x < y$
4. $J \equiv x \geq y \land y \geq 0$

A Simple Discrete Loop Example

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

$$\rightarrow\text{R}\ \frac{\text{loop}\ \dfrac{x{\geq}8 \land 5{\geq}y \land y{\geq}0 \vdash J \quad J \vdash [x := x + y;\ y := x - 2 \cdot y]J \quad J \vdash x \geq 0}{x{\geq}8 \land 5{\geq}y \land y{\geq}0 \vdash [(x := x + y;\ y := x - 2 \cdot y)^*]\, x \geq 0}}{\vdash x{\geq}8 \land 5{\geq}y \land y{\geq}0 \rightarrow [(x := x + y;\ y := x - 2 \cdot y)^*]\, x \geq 0}$$

1. $J \equiv x \geq 0$ — stronger: Lacks info about y
2. $J \equiv x \geq 8 \land 5 \geq y \land y \geq 0$ — weaker: Changes immediately
3. $J \equiv x \geq 0 \land y \geq 0$ — no: y may become negative if $x < y$
4. $J \equiv x \geq y \land y \geq 0$ — correct loop invariant

Add Context Γ, Δ to Premises?

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

Add Context Γ, Δ to Premises?

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

$$\lightning \frac{x = 0, x \leq 1 \vdash [x := x + 1]x \leq 1}{x = 0, x \leq 1 \vdash [(x := x + 1)^*]x \leq 1}$$

Add Context Γ, Δ to Premises?

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

$$\lightning \frac{x = 0, x \leq 1 \vdash [x := x + 1]x \leq 1}{x = 0, x \leq 1 \vdash [(x := x + 1)^*]x \leq 1}$$

$$\lightning \frac{x = 0 \vdash x \geq 0 \quad x \geq 0 \vdash [x := x + 1]x \geq 0 \quad x = 0, x \geq 0 \vdash x = 0}{x = 0 \vdash [(x := x + 1)^*]x = 0}$$

Add Context Γ, Δ to Premises?

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

$$\lightning \frac{x = 0, x \leq 1 \vdash [x := x + 1]x \leq 1}{x = 0, x \leq 1 \vdash [(x := x + 1)^*]x \leq 1}$$

$$\lightning \frac{x = 0 \vdash x \geq 0 \quad x \geq 0 \vdash [x := x + 1]x \geq 0 \quad x = 0, x \geq 0 \vdash x = 0}{x = 0 \vdash [(x := x + 1)^*]x = 0}$$

Unsound! Be careful where your assumptions go.

Outline

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

$$\text{loop}\ \frac{A \vdash j(x,v) \quad [;]\ \dfrac{}{j(x,v) \vdash [x''=;\,(?x=0;\, v:=-cv \cup ?x\neq 0]j(x,v)} \quad j(x,v) \vdash B(x,v)}{A \vdash [\left(x''=;\,(?x=0;\, v:=-cv \cup ?x\neq 0)\right)^*]B(x,v)}$$

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

$$\dfrac{A \vdash j(x,v) \quad [;]\dfrac{}{j(x,v) \vdash [x''=; (?x{=}0; v:=-cv \cup ?x{\neq}0]j(x,v)} \quad j(x,v) \vdash B(x,v)}{A \vdash [\left(x''=; (?x{=}0; v:=-cv \cup ?x{\neq}0)\right)^*]B(x,v)}loop$$

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

$A \vdash j(x,v)$

$j(x,v) \vdash [x''=](j(x,v))$

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

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

$j(x,v) \vdash B(x,v)$

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

1. $j(x,v) \equiv x \geq 0$
2. $j(x,v) \equiv 0 \leq x \wedge x \leq H$
3. $j(x,v) \equiv x = 0 \wedge v = 0$

weaker: fails postcondition if $x > H$

weak: fails ODE if $v \gg 0$

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

$0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0 \vdash 2gx{=}2gH{-}v^2 \wedge x{\geq}0$
$2gx{=}2gH{-}v^2 \wedge x{\geq}0 \vdash [\{x'{=}v, v'{=}{-}g \,\&\, x{\geq}0\}](2gx{=}2gH{-}v^2 \wedge x{\geq}0)$
$2gx{=}2gH{-}v^2 \wedge x{\geq}0, x{=}0 \vdash 2gx{=}2gH{-}(-cv)^2 \wedge x{\geq}0$
$2gx{=}2gH{-}v^2 \wedge x{\geq}0, x{\neq}0 \vdash 2gx{=}2gH{-}v^2 \wedge x{\geq}0$
$2gx{=}2gH{-}v^2 \wedge x{\geq}0 \vdash 0 \leq x \wedge x \leq H$

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

Proving Quantum the Acrophobic Bouncing Ball

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

Proving Quantum the Acrophobic Bouncing Ball

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

Proving Quantum the Acrophobic Bouncing Ball

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

Proving Quantum the Acrophobic Bouncing Ball

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

Proving Quantum the Acrophobic Bouncing Ball

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

$$\begin{array}{rl}
 & j(x,v), t\geq 0, H-\frac{g}{2}t^2\geq 0 \vdash j(H-\frac{g}{2}t^2,-gt) \\
\to R & \hline
 & j(x,v) \vdash t\geq 0 \to H-\frac{g}{2}t^2\geq 0 \to j(H-\frac{g}{2}t^2,-gt) \\
\forall R & \hline
 & j(x,v) \vdash \forall t\geq 0 \left(H-\frac{g}{2}t^2\geq 0 \to j(H-\frac{g}{2}t^2,-gt)\right) \\
[:=] & \hline
 & j(x,v) \vdash \forall t\geq 0 \left[x:=H-\frac{g}{2}t^2\right](x\geq 0 \to j(x,-gt)) \\
[:=] & \hline
 & j(x,v) \vdash \forall t\geq 0 \left[x:=H-\frac{g}{2}t^2\right][v:=-gt](x\geq 0 \to j(x,v)) \\
[;] & \hline
 & j(x,v) \vdash \forall t\geq 0 \left[x:=H-\frac{g}{2}t^2; v:=-gt\right](x\geq 0 \to j(x,v)) \\
['] & \hline
 & j(x,v) \vdash [x'=v, v'=-g \,\&\, x\geq 0]j(x,v)
\end{array}$$

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

$$
\dfrac{
\dfrac{
\dfrac{
\dfrac{
\dfrac{
\dfrac{
\dfrac{
\dfrac{}{2gx=2gH-v^2 \vdash 2g(H-\frac{g}{2}t^2)=2gH-(gt)^2}\,\mathbb{R}^{*}
\quad
\dfrac{}{H-\frac{g}{2}t^2\geq 0 \vdash H-\frac{g}{2}t^2\geq 0}
}{2gx=2gH-v^2 \wedge x\geq 0, H-\frac{g}{2}t^2\geq 0 \vdash 2g(H-\frac{g}{2}t^2)=2gH-(gt)^2 \wedge (H-\frac{g}{2}t^2)\geq 0}\,\wedge R
}{j(x,v), t\geq 0, H-\frac{g}{2}t^2\geq 0 \vdash j(H-\frac{g}{2}t^2,-gt)}\,\to R
}{j(x,v) \vdash t\geq 0 \to H-\frac{g}{2}t^2\geq 0 \to j(H-\frac{g}{2}t^2,-gt)}\,\forall R
}{j(x,v) \vdash \forall t\geq 0\,(H-\frac{g}{2}t^2\geq 0 \to j(H-\frac{g}{2}t^2,-gt))}\,[:=]
}{j(x,v) \vdash \forall t\geq 0\,[x:=H-\frac{g}{2}t^2](x\geq 0 \to j(x,-gt))}\,[:=]
}{j(x,v) \vdash \forall t\geq 0\,[x:=H-\frac{g}{2}t^2][v:=-gt](x\geq 0 \to j(x,v))}\,[;]
}{j(x,v) \vdash \forall t\geq 0\,[x:=H-\frac{g}{2}t^2; v:=-gt](x\geq 0 \to j(x,v))}\,[']
}{j(x,v) \vdash [x'=v, v'=-g \,\&\, x\geq 0]j(x,v)}
$$

Proving Quantum the Acrophobic Bouncing Ball

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{2gx=2gH-v^2 \vdash 2g(H-\frac{g}{2}t^2)=2gH-(gt)^2}\,\mathbb{R}(*) \quad \dfrac{}{H-\frac{g}{2}t^2\geq 0 \vdash H-\frac{g}{2}t^2\geq 0}\,\mathrm{id}(*)}{2gx=2gH-v^2\wedge x\geq 0, H-\frac{g}{2}t^2\geq 0 \vdash 2g(H-\frac{g}{2}t^2)=2gH-(gt)^2\wedge(H-\frac{g}{2}t^2)\geq 0}\,\wedge\mathrm{R}}{j(x,v),\, t\geq 0,\, H-\frac{g}{2}t^2\geq 0 \vdash j(H-\frac{g}{2}t^2,-gt)}}{j(x,v) \vdash t\geq 0 \to H-\frac{g}{2}t^2\geq 0 \to j(H-\frac{g}{2}t^2,-gt)}\,\to\mathrm{R}}{j(x,v) \vdash \forall t\geq 0\,(H-\frac{g}{2}t^2\geq 0 \to j(H-\frac{g}{2}t^2,-gt))}\,\forall\mathrm{R}}{j(x,v) \vdash \forall t\geq 0\,[x:=H-\frac{g}{2}t^2](x\geq 0 \to j(x,-gt))}\,[:=]}{j(x,v) \vdash \forall t\geq 0\,[x:=H-\frac{g}{2}t^2][v:=-gt](x\geq 0 \to j(x,v))}\,[:=]}{j(x,v) \vdash \forall t\geq 0\,[x:=H-\frac{g}{2}t^2;\, v:=-gt](x\geq 0 \to j(x,v))}\,[;]}{j(x,v) \vdash [x'=v,\, v'=-g\,\&\, x\geq 0]j(x,v)}\,[']
$$

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

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

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

- Is Quantum done with his safety proof?

Proving Quantum the Acrophobic Bouncing Ball

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

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

- Is Quantum done with his safety proof?
- Oh no! The solutions we sneaked into $[']$ only solve the ODE/IVP if $x = 0, v = 0$ which $j(x,v)$ can't guarantee!

Proving Quantum the Acrophobic Bouncing Ball

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

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

- Is Quantum done with his safety proof?
- Oh no! The solutions we sneaked into $[']$ only solve the ODE/IVP if $x=0, v=0$ which $j(x,v)$ can't guarantee!
- Never use solutions without proof! $\rightsquigarrow$ redo proof with true solution

Quantum Misplaced the Constants

$$\text{loop}\ \frac{}{A \vdash [\alpha^*]B(x,v)}$$

1. $j(x,v) \equiv 2gx{=}2gH - v^2 \land x{\geq}0$
2. $p \equiv c{=}1 \land g{>}0$
3. $J \equiv j(x,v) \land p$ as loop invariant

Quantum Misplaced the Constants

$$\text{loop}\frac{\mathbb{R}\dfrac{}{A \vdash j(x,v)\wedge p} \quad []\wedge\dfrac{}{j(x,v) \wedge p \vdash [\alpha](j(x,v) \wedge p)}}{A \vdash [\alpha^*]B(x,v)}$$

1. $j(x,v) \equiv 2gx{=}2gH{-}v^2 \wedge x{\geq}0$
2. $p \equiv c{=}1 \wedge g{>}0$
3. $J \equiv j(x,v) \wedge p$ as loop invariant

Quantum Misplaced the Constants

$$\text{loop}\,\frac{\mathbb{R}\,\overset{*}{\dfrac{}{A \vdash j(x,v)\wedge p}} \quad []\wedge\dfrac{}{j(x,v) \wedge p \vdash [\alpha](j(x,v) \wedge p)}}{A \vdash [\alpha^*]B(x,v)}$$

1. $j(x,v) \equiv 2gx{=}2gH{-}v^2 \wedge x{\geq}0$
2. $p \equiv c{=}1 \wedge g{>}0$
3. $J \equiv j(x,v) \wedge p$ as loop invariant

Quantum Misplaced the Constants

$$[]\wedge \quad [\alpha](P \wedge Q) \leftrightarrow [\alpha]P \wedge [\alpha]Q$$

$$\text{loop}\,\frac{\mathbb{R}\,\dfrac{*}{A \vdash j(x,v) \wedge p} \qquad []\wedge\,\dfrac{\wedge R\,\dfrac{}{j(x,v) \wedge p \vdash [\alpha]j(x,v) \wedge [\alpha]p}}{j(x,v) \wedge p \vdash [\alpha](j(x,v) \wedge p)}}{A \vdash [\alpha^*]B(x,v)}$$

1. $j(x,v) \equiv 2gx{=}2gH - v^2 \wedge x{\geq}0$
2. $p \equiv c{=}1 \wedge g{>}0$
3. $J \equiv j(x,v) \wedge p$ as loop invariant

Quantum Misplaced the Constants

$[]\wedge \quad [\alpha](P \wedge Q) \leftrightarrow [\alpha]P \wedge [\alpha]Q$

$$\text{loop}\,\dfrac{\mathbb{R}\,\dfrac{*}{A \vdash j(x,v)\wedge p} \quad []\wedge\,\dfrac{\wedge R\,\dfrac{j(x,v)\wedge p \vdash [\alpha]j(x,v) \quad \text{V}\,\overline{j(x,v) \wedge p \vdash [\alpha]p}}{j(x,v)\wedge p \vdash [\alpha]j(x,v) \wedge [\alpha]p}}{j(x,v) \wedge p \vdash [\alpha](j(x,v) \wedge p)} \quad \mathbb{R}\,\overline{j(x,v)\wedge p \vdash B(x,}}{A \vdash [\alpha^*]B(x,v)}$$

1. $j(x,v) \equiv 2gx{=}2gH{-}v^2 \wedge x{\geq}0$
2. $p \equiv c{=}1 \wedge g{>}0$
3. $J \equiv j(x,v) \wedge p$ as loop invariant

Quantum Misplaced the Constants

$[]\wedge \quad [\alpha](P \wedge Q) \leftrightarrow [\alpha]P \wedge [\alpha]Q$

$$\text{loop}\,\frac{\mathbb{R}\,\dfrac{*}{A \vdash j(x,v)\wedge p} \qquad []\wedge\,\dfrac{\wedge R\,\dfrac{\text{above}\quad \dfrac{}{j(x,v)\wedge p \vdash [\alpha]j(x,v)} \qquad \mathsf{V}\,\dfrac{}{j(x,v)\wedge p \vdash [\alpha]p}}{j(x,v)\wedge p \vdash [\alpha]j(x,v)\wedge[\alpha]p}}{j(x,v)\wedge p \vdash [\alpha](j(x,v)\wedge p)} \qquad \mathbb{R}\,\dfrac{}{j(x,v)\wedge p \vdash B(x,}}{A \vdash [\alpha^*]B(x,v)}$$

1. $j(x,v) \equiv 2gx{=}2gH{-}v^2 \wedge x{\geq}0$
2. $p \equiv c{=}1 \wedge g{>}0$
3. $J \equiv j(x,v) \wedge p$ as loop invariant

Quantum Misplaced the Constants

$$[]\wedge \quad [\alpha](P \wedge Q) \leftrightarrow [\alpha]P \wedge [\alpha]Q \qquad \mathsf{V} \quad p \rightarrow [\alpha]p \qquad (FV(p) \cap BV(\alpha) = \emptyset)$$

$$\text{loop}\dfrac{\mathbb{R}\dfrac{*}{A \vdash j(x,v) \wedge p} \quad []\wedge\dfrac{\wedge R\dfrac{\text{above}}{j(x,v) \wedge p \vdash [\alpha]j(x,v)} \quad \mathsf{V}\dfrac{*}{j(x,v) \wedge p \vdash [\alpha]p}}{j(x,v) \wedge p \vdash [\alpha]j(x,v) \wedge [\alpha]p} \quad \mathbb{R}\dfrac{}{j(x,v) \wedge p \vdash [\alpha](j(x,v) \wedge p)} \quad \mathbb{R}\dfrac{}{j(x,v) \wedge p \vdash B(x,}}{A \vdash [\alpha^*]B(x,v)}$$

1. $j(x,v) \equiv 2gx{=}2gH - v^2 \wedge x{\geq}0$
2. $p \equiv c{=}1 \wedge g{>}0$
3. $J \equiv j(x,v) \wedge p$ as loop invariant

Quantum Misplaced the Constants

$$[]\wedge \quad [\alpha](P \wedge Q) \leftrightarrow [\alpha]P \wedge [\alpha]Q \qquad \mathsf{V} \quad p \rightarrow [\alpha]p \qquad (FV(p) \cap BV(\alpha) = \emptyset)$$

$$\text{loop}\dfrac{\mathbb{R}\dfrac{*}{A \vdash j(x,v) \wedge p} \quad []\wedge\dfrac{\wedge\mathsf{R}\dfrac{\text{above}}{j(x,v) \wedge p \vdash [\alpha]j(x,v)} \quad \mathsf{V}\dfrac{*}{j(x,v) \wedge p \vdash [\alpha]p}}{j(x,v) \wedge p \vdash [\alpha]j(x,v) \wedge [\alpha]p} \quad \mathbb{R}\dfrac{*}{j(x,v) \wedge p \vdash [\alpha](j(x,v) \wedge p)} \quad \mathbb{R}\dfrac{*}{j(x,v) \wedge p \vdash B(x,}}{A \vdash [\alpha^*]B(x,v)}$$

1. $j(x,v) \equiv 2gx{=}2gH - v^2 \wedge x{\geq}0$
2. $p \equiv c{=}1 \wedge g{>}0$
3. $J \equiv j(x,v) \wedge p$ as loop invariant

Quantum the Provably Safe Bouncing Ball

Proposition (Quantum can bounce around safely)

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

$$@\text{requires}(0 \leq x \wedge x = H \wedge v = 0)$$
$$@\text{requires}(g > 0 \wedge c = 1)$$
$$@\text{ensures}(0 \leq x \wedge x \leq H)$$
$$\{\{x' = v, v' = -g \,\&\, x \geq 0\};$$
$$(?x = 0; v{:=}-cv \cup ?x \neq 0))\}^* @\text{invariant}(2gx = 2gH - v^2 \wedge x \geq 0)$$

Invariant Contracts

Invariants play a crucial role in CPS design. Capture them if you can. Use @invariant contracts in your hybrid programs.

Note: constants $c = 1 \wedge g > 0$ that never change are usually elided

Outline

Invariants

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

Invariants are a fundamental force of CS

Variants are another fundamental force of CS

Outline

Summary

$$\text{I}\quad [\alpha^*]P \leftrightarrow P \wedge [\alpha^*](P \rightarrow [\alpha]P)$$

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

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

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

$$\text{MR}\quad \frac{\Gamma \vdash [\alpha]Q, \Delta \qquad Q \vdash P}{\Gamma \vdash [\alpha]P, \Delta}$$

$$[]\wedge\quad [\alpha](P \wedge Q) \leftrightarrow [\alpha]P \wedge [\alpha]Q$$

$$\text{V}\quad p \rightarrow [\alpha]p \quad (FV(p) \cap BV(\alpha) = \emptyset)$$

Outline

Iteration Axiom

compositional semantics $\Rightarrow$ compositional rules!

Loops of Proofs: Iterations

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

$$\frac{}{A \vdash [\alpha^*]B}$$

Loops of Proofs: Iterations

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

$$[^*]\frac{\dfrac{}{A \vdash B \wedge [\alpha][\alpha^*]B}}{A \vdash [\alpha^*]B}$$

Loops of Proofs: Iterations

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

$$\dfrac{\dfrac{\dfrac{}{A \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)}}{A \vdash B \wedge [\alpha][\alpha^*]B}[^*]}{A \vdash [\alpha^*]B}[^*]$$

Loops of Proofs: Iterations

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

$$\dfrac{\dfrac{\dfrac{}{A \vdash B \wedge [\alpha]\big(B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)\big)}}{A \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)}[^*]}{A \vdash B \wedge [\alpha][\alpha^*]B}[^*]}{A \vdash [\alpha^*]B}[^*]$$

Loops of Proofs: Iterations & Splitting the Box

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

$$[]\wedge\ [\alpha](P \wedge Q) \leftrightarrow [\alpha]P \wedge [\alpha]Q$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A \vdash B \wedge [\alpha]B \wedge [\alpha][\alpha](B \wedge [\alpha][\alpha^*]B)}}{A \vdash B \wedge [\alpha]\big(B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)\big)}\,[]\wedge}{A \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)}\,[^*]}{A \vdash B \wedge [\alpha][\alpha^*]B}\,[^*]}{A \vdash [\alpha^*]B}\,[^*]$$

Loops of Proofs: Iterations & Splitting the Box

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

$$[]\wedge\ [\alpha](P \wedge Q) \leftrightarrow [\alpha]P \wedge [\alpha]Q$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A \vdash B \wedge [\alpha]B \wedge [\alpha]([\alpha]B \wedge [\alpha][\alpha][\alpha^*]B)}}{A \vdash B \wedge [\alpha]B \wedge [\alpha][\alpha](B \wedge [\alpha][\alpha^*]B)}\,[]\wedge}{A \vdash B \wedge [\alpha]\big(B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)\big)}\,[]\wedge}{A \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)}\,[^*]}{A \vdash B \wedge [\alpha][\alpha^*]B}\,[^*]}{A \vdash [\alpha^*]B}\,[^*]$$

Loops of Proofs: Iterations & Splitting the Box

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

$$[]\wedge\ [\alpha](P \wedge Q) \leftrightarrow [\alpha]P \wedge [\alpha]Q$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A \vdash B \wedge [\alpha]B \wedge [\alpha][\alpha]B \wedge [\alpha][\alpha][\alpha][\alpha^*]B}}{A \vdash B \wedge [\alpha]B \wedge [\alpha]([\alpha]B \wedge [\alpha][\alpha][\alpha^*]B)}\,[]\wedge}{A \vdash B \wedge [\alpha]B \wedge [\alpha][\alpha](B \wedge [\alpha][\alpha^*]B)}\,[]\wedge}{A \vdash B \wedge [\alpha]\big(B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)\big)}\,[]\wedge}{A \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)}\,[^*]}{A \vdash B \wedge [\alpha][\alpha^*]B}\,[^*]}{A \vdash [\alpha^*]B}\,[^*]$$

Loops of Proofs: Iterations & Splitting the Box

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

$$[]\wedge\ [\alpha](P \wedge Q) \leftrightarrow [\alpha]P \wedge [\alpha]Q$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{A \vdash B \quad A \vdash [\alpha]B \quad A \vdash [\alpha][\alpha]B \quad A \vdash [\alpha][\alpha][\alpha][\alpha^*]B}{A \vdash B \wedge [\alpha]B \wedge [\alpha][\alpha]B \wedge [\alpha][\alpha][\alpha][\alpha^*]B}\wedge R}{A \vdash B \wedge [\alpha]B \wedge [\alpha]([\alpha]B \wedge [\alpha][\alpha][\alpha^*]B)}[]\wedge}{A \vdash B \wedge [\alpha]B \wedge [\alpha][\alpha](B \wedge [\alpha][\alpha^*]B)}[]\wedge}{A \vdash B \wedge [\alpha]\big(B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)\big)}[]\wedge}{A \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)}[^*]}{A \vdash B \wedge [\alpha][\alpha^*]B}[^*]}{A \vdash [\alpha^*]B}[^*]$$

Loops of Proofs: Iterations & Splitting the Box

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

$$[]\wedge\ [\alpha](P \wedge Q) \leftrightarrow [\alpha]P \wedge [\alpha]Q$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{A \vdash B \quad A \vdash [\alpha]B \quad A \vdash [\alpha][\alpha]B \quad A \vdash [\alpha][\alpha][\alpha][\alpha^*]B}{A \vdash B \wedge [\alpha]B \wedge [\alpha][\alpha]B \wedge [\alpha][\alpha][\alpha][\alpha^*]B}\wedge R}{A \vdash B \wedge [\alpha]B \wedge [\alpha]([\alpha]B \wedge [\alpha][\alpha][\alpha^*]B)}[]\wedge}{A \vdash B \wedge [\alpha]B \wedge [\alpha][\alpha](B \wedge [\alpha][\alpha^*]B)}[]\wedge}{A \vdash B \wedge [\alpha]\big(B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)\big)}[]\wedge}{A \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)}[^*]}{A \vdash B \wedge [\alpha][\alpha^*]B}[^*]}{A \vdash [\alpha^*]B}[^*]$$

1. Simple approach . . . if we don't mind unrolling until the end of time
2. Useful for finding counterexamples

Loops of Proofs: Iterations & Generalizations

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

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \vdash B \wedge [\alpha]\big(B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)\big)}}{A \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)}[^*]}{A \vdash B \wedge [\alpha][\alpha^*]B}[^*]}{A \vdash [\alpha^*]B}[^*]$$

Loops of Proofs: Iterations & Generalizations

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

$$\text{MR}\ \frac{\Gamma \vdash [\alpha]Q, \Delta \qquad Q \vdash P}{\Gamma \vdash [\alpha]P, \Delta}$$

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{A \vdash B}{A \vdash [\alpha]\big(B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)\big)}}{A \vdash B \wedge [\alpha]\big(B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)\big)}\wedge R}{A \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)}[^*]}{A \vdash B \wedge [\alpha][\alpha^*]B}[^*]}{A \vdash [\alpha^*]B}[^*]$$

Loops of Proofs: Iterations & Generalizations

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

$$\text{MR}\ \frac{\Gamma \vdash [\alpha]Q, \Delta \qquad Q \vdash P}{\Gamma \vdash [\alpha]P, \Delta}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{A \vdash [\alpha]J_1 \qquad J_1 \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)}{A \vdash B}\,\text{MR}}{A \vdash [\alpha]\big(B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)\big)}\,\wedge\text{R}}{A \vdash B \wedge [\alpha]\big(B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)\big)}\,[^*]}{A \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)}\,[^*]}{A \vdash B \wedge [\alpha][\alpha^*]B}\,[^*]}{A \vdash [\alpha^*]B}$$

Loops of Proofs: Iterations & Generalizations

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

$$\text{MR}\ \frac{\Gamma \vdash [\alpha]Q, \Delta \qquad Q \vdash P}{\Gamma \vdash [\alpha]P, \Delta}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A \vdash B}\,\text{MR} \quad \dfrac{\dfrac{J_1 \vdash B}{J_1 \vdash [\alpha](B \wedge [\alpha][\alpha^*]B)}}{A \vdash [\alpha]J_1}\,\wedge\text{R}}{A \vdash [\alpha]\big(B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)\big)}\,\text{MR}}{A \vdash B \wedge [\alpha]\big(B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)\big)}\,\wedge\text{R}}{A \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)}\,[*]}{A \vdash B \wedge [\alpha][\alpha^*]B}\,[*]}{A \vdash [\alpha^*]B}\,[*]$$

Loops of Proofs: Iterations & Generalizations

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

$$\text{MR}\ \frac{\Gamma \vdash [\alpha]Q, \Delta \qquad Q \vdash P}{\Gamma \vdash [\alpha]P, \Delta}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{J_1 \vdash [\alpha]J_2}}{J_2 \vdash B \wedge [\alpha][\alpha^*]B}}{J_1 \vdash B}\text{MR}}{J_1 \vdash [\alpha](B \wedge [\alpha][\alpha^*]B)}}{A \vdash [\alpha]J_1}\wedge\text{R}}{J_1 \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)}}{A \vdash B}\text{MR}}{A \vdash [\alpha]\big(B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)\big)}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{A \vdash B \wedge [\alpha]\big(B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)\big)}{A \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)}[*]}{A \vdash B \wedge [\alpha][\alpha^*]B}[*]}{A \vdash [\alpha^*]B}[*]}{}\wedge\text{R}$$

Loops of Proofs: Iterations & Generalizations

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

$$\text{MR}\ \frac{\Gamma \vdash [\alpha]Q, \Delta \qquad Q \vdash P}{\Gamma \vdash [\alpha]P, \Delta}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A \vdash B}\,\text{MR}}{A \vdash [\alpha]J_1}\,\wedge\text{R} \quad \dfrac{}{J_1 \vdash B}\,\text{MR}}{J_1 \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)}\,\wedge\text{R} \quad \dfrac{}{J_1 \vdash [\alpha]J_2}\,\wedge\text{R} \quad \dfrac{}{J_2 \vdash B}}{J_1 \vdash [\alpha](B \wedge [\alpha][\alpha^*]B)}}{J_2 \vdash B \wedge [\alpha][\alpha^*]B}}{A \vdash [\alpha]\big(B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)\big)}\,\text{MR} \quad \dfrac{}{J_2 \vdash [\alpha][\alpha^*]B}}{A \vdash B \wedge [\alpha]\big(B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)\big)}\,\wedge\text{R}}{A \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)}\,[^*]}{A \vdash B \wedge [\alpha][\alpha^*]B}\,[^*]}{A \vdash [\alpha^*]B}\,[^*]$$

Loops of Proofs: Iterations & Generalizations

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

$$\text{MR}\ \frac{\Gamma \vdash [\alpha]Q, \Delta \qquad Q \vdash P}{\Gamma \vdash [\alpha]P, \Delta}$$

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{}{A \vdash B}\,\text{MR}}{A \vdash [\alpha]J_1}\,\wedge\text{R} \qquad \cfrac{}{J_1 \vdash B}\,\text{MR}}{J_1 \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)}}{A \vdash [\alpha]\big(B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)\big)}\,\text{MR} \qquad \cfrac{}{J_1 \vdash [\alpha]J_2}\,\wedge\text{R} \qquad \cfrac{}{J_2 \vdash B} \qquad \cfrac{}{J_2 \vdash [\alpha]J_3} \quad \ldots}{A \vdash B \wedge [\alpha]\big(B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)\big)}\,\wedge\text{R} \qquad \cfrac{}{J_2 \vdash [\alpha][\alpha^*]B}}{A \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)}\,[*] \qquad \cfrac{}{J_2 \vdash B \wedge [\alpha][\alpha^*]B}}{A \vdash B \wedge [\alpha][\alpha^*]B}\,[*] \qquad \cfrac{}{J_1 \vdash [\alpha](B \wedge [\alpha][\alpha^*]B)}}{A \vdash [\alpha^*]B}\,[*]$$

Loops of Proofs: Common Generalizations

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

$$\text{MR}\ \frac{\Gamma \vdash [\alpha]Q, \Delta \qquad Q \vdash P}{\Gamma \vdash [\alpha]P, \Delta}$$

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{}{A \vdash B}\,\text{MR}}{A \vdash [\alpha]\big(B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)\big)}\,\wedge\text{R}}{A \vdash B \wedge [\alpha]\big(B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)\big)}\,[*]}{A \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)}\,[*]}{A \vdash B \wedge [\alpha][\alpha^*]B}\,[*]}{A \vdash [\alpha^*]B}$$

$$\cfrac{\cfrac{\cfrac{\cfrac{}{J \vdash B}\quad \cfrac{J \vdash [\alpha]J \qquad \ldots}{J \vdash [\alpha][\alpha^*]B}}{J \vdash B \wedge [\alpha][\alpha^*]B}\,\wedge\text{R}}{J \vdash [\alpha](B \wedge [\alpha][\alpha^*]B)}\,\text{MR}}{J \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)}\,\wedge\text{R}$$

Loops of Proofs: Extracting a Proof Rule

$$\frac{J \vdash B}{A \vdash [\alpha^*]B}$$

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

$$\text{MR}\ \frac{\Gamma \vdash [\alpha]Q, \Delta \qquad Q \vdash P}{\Gamma \vdash [\alpha]P, \Delta}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A \vdash B}\,\text{MR}}{A \vdash [\alpha]J}\,\wedge\text{R} \quad \dfrac{}{J \vdash B}\,\text{MR}}{J \vdash B \wedge [\alpha]J}\,\wedge\text{R} \quad \dfrac{J \vdash [\alpha]J \quad \ldots}{J \vdash [\alpha][\alpha^*]B}}{J \vdash [\alpha](B \wedge [\alpha][\alpha^*]B)}}{J \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)}}{A \vdash [\alpha]\big(B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)\big)}}{A \vdash B \wedge [\alpha]\big(B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)\big)}\,\wedge\text{R}}{A \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)}\,[^*]}{A \vdash B \wedge [\alpha][\alpha^*]B}\,[^*]}{A \vdash [\alpha^*]B}\,[^*]$$

Loops of Proofs: Extracting a Proof Rule

$$\frac{J \vdash [\alpha]J \qquad J \vdash B}{A \vdash [\alpha^*]B}$$

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

$$\text{MR}\ \frac{\Gamma \vdash [\alpha]Q, \Delta \qquad Q \vdash P}{\Gamma \vdash [\alpha]P, \Delta}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A \vdash B}\,\text{MR}}{A \vdash [\alpha]J}\,\wedge\text{R} \quad \dfrac{\dfrac{}{J \vdash B}\,\text{MR}}{J \vdash [\alpha]J}\,\wedge\text{R}}{A \vdash B \wedge [\alpha]J}\,\text{MR} \quad \dfrac{J \vdash B \qquad \dfrac{J \vdash [\alpha]J \qquad \ldots}{J \vdash [\alpha][\alpha^*]B}}{J \vdash B \wedge [\alpha][\alpha^*]B}\,\wedge\text{R}}{A \vdash [\alpha](B \wedge [\alpha][\alpha^*]B)}\,\text{MR}}{J \vdash [\alpha](B \wedge [\alpha][\alpha^*]B)}}{A \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)}\,\wedge\text{R}}{A \vdash [\alpha](B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B))}}{A \vdash B \wedge [\alpha](B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B))}}{A \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)}\,[^*]}{A \vdash B \wedge [\alpha][\alpha^*]B}\,[^*]}{A \vdash [\alpha^*]B}\,[^*]$$

Loops of Proofs: Extracting a Proof Rule

$$\frac{A \vdash J \qquad J \vdash [\alpha]J \qquad J \vdash B}{A \vdash [\alpha^*]B}$$

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

$$\text{MR}\ \frac{\Gamma \vdash [\alpha]Q, \Delta \qquad Q \vdash P}{\Gamma \vdash [\alpha]P, \Delta}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A \vdash J}\quad \dfrac{\dfrac{}{J \vdash [\alpha]J}\quad \dfrac{\dfrac{}{J \vdash B}\quad \dfrac{\dfrac{}{J \vdash [\alpha]J}\quad \dots}{J \vdash [\alpha][\alpha^*]B}}{J \vdash B \wedge [\alpha][\alpha^*]B}\wedge\text{R}}{J \vdash [\alpha](B \wedge [\alpha][\alpha^*]B)}\text{MR}}{J \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)}\wedge\text{R}}{A \vdash [\alpha](B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B))}\text{MR}}{A \vdash B \wedge [\alpha](B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B))}\wedge\text{R}}{A \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)}[^*]}{A \vdash B \wedge [\alpha][\alpha^*]B}[^*]}{A \vdash [\alpha^*]B}[^*]$$

Loops of Proofs: Loop Invariants

$$\text{loop}\ \frac{A \vdash J \quad J \vdash [\alpha]J \quad J \vdash B}{A \vdash [\alpha^*]B}$$

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

$$\text{MR}\ \frac{\Gamma \vdash [\alpha]Q, \Delta \quad Q \vdash P}{\Gamma \vdash [\alpha]P, \Delta}$$

Invariant J generalized intermediate condition

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{J \vdash B} \quad \dfrac{}{J \vdash [\alpha]J} \quad \dfrac{}{\ldots}}{J \vdash [\alpha][\alpha^*]B}\,\wedge R}{J \vdash B \wedge [\alpha][\alpha^*]B}}{J \vdash [\alpha](B \wedge [\alpha][\alpha^*]B)}\,MR}{J \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)}\,\wedge R}{A \vdash [\alpha](B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B))}\,MR}{A \vdash B \wedge [\alpha](B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B))}\,\wedge R}{A \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)}\,[^*]}{A \vdash B \wedge [\alpha][\alpha^*]B}\,[^*]}{A \vdash [\alpha^*]B}\,[^*]$$


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


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