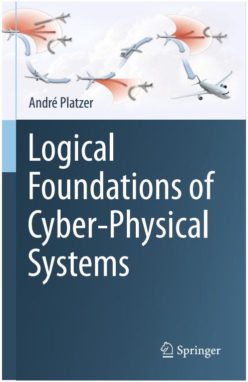
07: Control Loops & Invariants

Logical Foundations of Cyber-Physical Systems



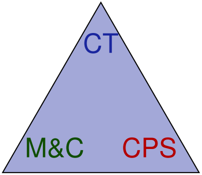
André Platzer

Carnegie Mellon University
Computer Science Department

Outline

Outline

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

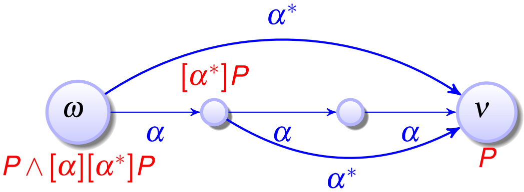


control loops
feedback mechanisms
dynamics of iteration

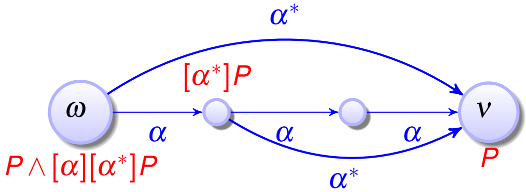
semantics of control loops
operational effects of control

Outline

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



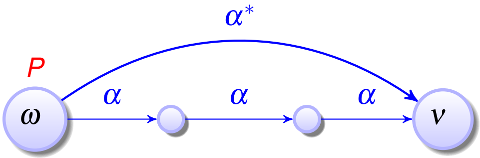
$[^*]$ $[\alpha^*]P \leftrightarrow P \land [\alpha][\alpha^*]P$



Problem: Proof for $[\alpha^*]P$ needs proof of $[\alpha][\alpha^*]P$

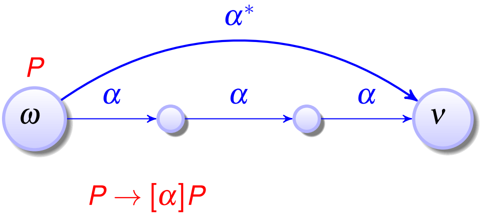
Lemma ( )

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



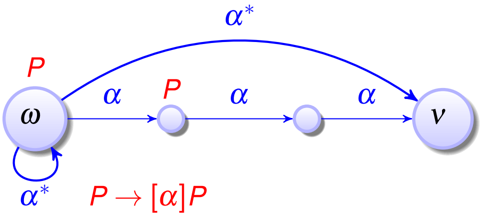
Lemma ( )

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



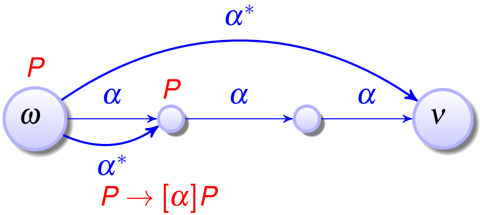
Lemma ( )

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



Lemma (I is sound)

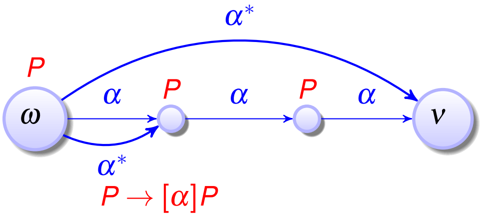
$$\text{I} \quad [\alpha^*]P \leftrightarrow P \land [\alpha^*](P \to [\alpha]P)$$



Induction Axiom

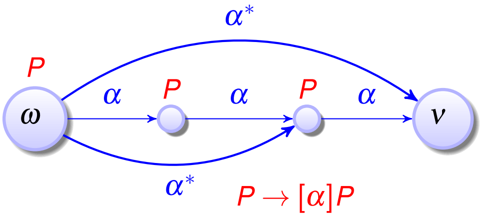
Lemma (I is sound)

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



Lemma (I is sound)

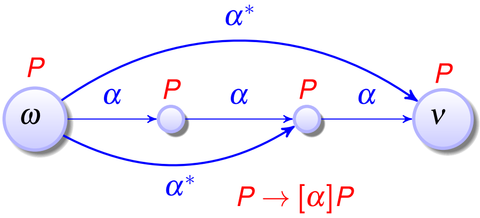
$$\text{I} \ [\alpha^*]P \leftrightarrow P \land [\alpha^*](P \rightarrow [\alpha]P)$$



Induction Axiom

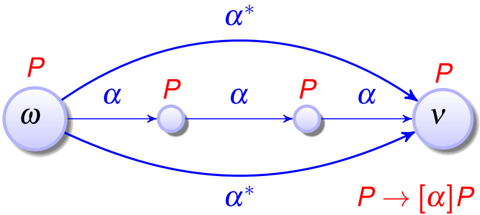
Lemma (I is sound)

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



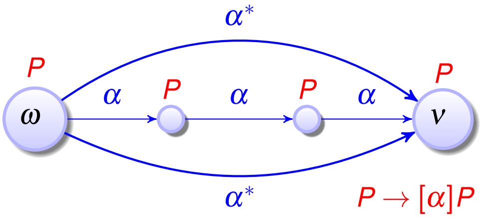
Lemma (I is sound)

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



Lemma (I is sound)

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



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

Induction Rule for Loops

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

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

Lemma (Loop induction rule ind is sound)

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

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).

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

□

Induction Rule for Loops

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

Lemma (Loop induction rule ind is sound)

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

Proof (Derived rule).

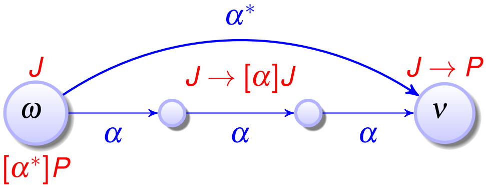
$$\text{I}\ \dfrac{\wedge\text{R}\ \dfrac{\text{id}\ \dfrac{*}{P \vdash P} \qquad \text{G}\ \dfrac{\rightarrow\text{R}\ \dfrac{P \vdash [\alpha]P}{\vdash P \rightarrow [\alpha]P}}{P \vdash [\alpha^*](P \rightarrow [\alpha]P)}}{P \vdash P \wedge [\alpha^*](P \rightarrow [\alpha]P)}}{P \vdash [\alpha^*]P}$$

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

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)

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



Loop Invariants

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

Lemma (Loop invariant rule loop is sound)

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

Proof (Derived rule).

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

□

Loop Invariants

Generalize postcondition to strong loop invariant J by

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

Lemma (Loop invariant rule loop is sound)

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

Proof (Derived rule).

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

□

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

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

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

1. $J \equiv x \geq 0$

A Simple Discrete Loop Example

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

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

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

A Simple Discrete Loop Example

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

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

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

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

A Simple Discrete Loop Example

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

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

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

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

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

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 $x < y$

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

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

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

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

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

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

Forgot to Add Sequent Context Γ, Δ to Premises

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

Forgot to Add Sequent Context Γ, Δ to Premises

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

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

Forgot to Add Sequent Context Γ, Δ to Premises

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

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

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

Forgot to Add Sequent Context Γ, Δ to Premises

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

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

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

Unsound! Be careful where your assumptions go,
or your CPS might go where it shouldn't.

Outline

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$
\text{loop}\;\dfrac{A \vdash j(x,v) \qquad \dfrac{\text{[;]}\;\dfrac{\text{MR}\;\dfrac{j(x,v) \vdash [\text{grav}]j(x,v) \qquad \text{[}\cup\text{]}\;\dfrac{\land\text{R}\;\dfrac{\text{[;]}\;\dfrac{\overline{j(x,v) \vdash [?x=0][v:=-cv]j(x,v)}}{j(x,v) \vdash [?x=0;\, v:=-cv]j(x,v)} \qquad \overline{j(x,v) \vdash [?x\neq0]j(x,v)}}{j(x,v) \vdash [?x=0;\, v:=-cv]j(x,v) \land [?x\neq0]j(x,v)}}{j(x,v) \vdash [?x=0;\, v:=-cv \cup ?x\neq0]j(x,v)}}{j(x,v) \vdash [\text{grav}][?x=0;\, v:=-cv \cup ?x\neq0]j(x,v)}}{j(x,v) \vdash [\text{grav};\, (?x=0;\, v:=-cv \cup ?x\neq0)]j(x,v)}}{j(x,v) \vdash [\text{grav};\, (?x=0;\, v:=-cv \cup ?x\neq0)]j(x,v)} \qquad j(x,v) \vdash B(x,v)}{A \vdash \big[\big(\text{grav};\, (?x=0;\, v:=-cv \cup ?x\neq0)\big)^*\big]B(x,v)}
$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

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

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

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

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

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

1. $j(x,v) \equiv x \geq 0$ — 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 $x > 0$

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

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

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

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

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

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

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

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

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

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

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

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

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

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

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

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

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

$$\forall R \quad \overline{\mathrm{j}(x,v) \vdash \forall t{\geq}0\,\big(H-\tfrac{g}{2}t^2{\geq}0 \rightarrow \mathrm{j}(H-\tfrac{g}{2}t^2,-gt)\big)}$$

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

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

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

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

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

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

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

$$\text{∧R}\;\dfrac{\text{ℝ}\;\dfrac{*}{2gx=2gH-v^2 \vdash 2g(H-\frac{g}{2}t^2)=2gH-(gt)^2} \qquad \dfrac{}{H-\frac{g}{2}t^2\geq 0 \vdash H-\frac{g}{2}t^2\geq 0}}{2gx=2gH-v^2\land x\geq 0,\, H-\frac{g}{2}t^2\geq 0 \vdash 2g(H-\frac{g}{2}t^2)=2gH-(gt)^2\land(H-\frac{g}{2}t^2)\geq 0}$$

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

- Is Quantum done with his safety proof?

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

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

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

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

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

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

Clumsy Quantum Misplaced the Constants

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

1. $j(x,v) \equiv 2gx = 2gH - v^2 \wedge x \geq 0$
2. $p \equiv c = 1 \wedge g > 0$

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

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

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

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

Clumsy Quantum Misplaced the Constants

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

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

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

Clumsy Quantum Misplaced the Constants

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

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

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

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

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

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

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

Proposition (Quantum can bounce around safely)

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

$$\textbf{requires}(0 \le x \land x = H \land v = 0)$$
$$\textbf{requires}(g > 0 \land 1 = c)$$
$$\textbf{ensures}(0 \le x \land x \le H)$$
$$\{\{x' = v, v' = -g \,\&\, x \ge 0\};$$
$$(?x = 0; v := -cv \cup ?x \ne 0))\}^* \textbf{@invariant}(2gx = 2gH - v^2 \land x \ge 0)$$

Invariant Contracts

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

Outline

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

Summary: Loops, Generalizations, Splittings

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

G $\dfrac{P}{[\alpha]P}$

M[·] $\dfrac{P \rightarrow Q}{[\alpha]P \rightarrow [\alpha]Q}$

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

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

[]∧ $[\alpha](P \land Q) \leftrightarrow [\alpha]P \land [\alpha]Q$

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

Outline

5. Appendix
   - Iteration Axiom
   - Iterations & Splitting the Box
   - Iteration & Generalizations

Iteration Axiom

compositional semantics $\Rightarrow$ compositional rules!

Loops of Proofs: Iterations

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

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

Loops of Proofs: Iterations

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

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

Loops of Proofs: Iterations

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

$$\dfrac{\dfrac{\dfrac{}{A \vdash B \land [\alpha](B \land [\alpha][\alpha^*]B)}}{A \vdash B \land [\alpha]{\color{red}[\alpha^*]B}}[^*]}{A \vdash [\alpha^*]B}[^*]$$

Loops of Proofs: Iterations

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

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

Loops of Proofs: Iterations & Splitting the Box

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

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

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

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

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

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

Loops of Proofs: Iterations & Splitting the Box

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

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

$$
\begin{array}{ll}
 & \overline{A \vdash B \land [\alpha]B \land [\alpha][\alpha]B \land [\alpha][\alpha][\alpha][\alpha^*]B} \\
[]\land & \overline{A \vdash B \land [\alpha]B \land \color{red}{[\alpha]([\alpha]B \land [\alpha][\alpha][\alpha^*]B)}} \\
[]\land & \overline{A \vdash B \land [\alpha]B \land [\alpha][\alpha](B \land [\alpha][\alpha^*]B)} \\
[]\land & \overline{A \vdash B \land [\alpha]\big(B \land [\alpha](B \land [\alpha][\alpha^*]B)\big)} \\
[^*] & \overline{A \vdash B \land [\alpha](B \land [\alpha][\alpha^*]B)} \\
[^*] & \overline{A \vdash B \land [\alpha][\alpha^*]B} \\
[^*] & A \vdash [\alpha^*]B
\end{array}
$$

Loops of Proofs: Iterations & Splitting the Box

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

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

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

Loops of Proofs: Iterations & Splitting the Box

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

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

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

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

Loops of Proofs: Iterations & Generalizations

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

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

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

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

$$\dfrac{\dfrac{\dfrac{\dfrac{A \vdash B \qquad \overline{A \vdash [\alpha]\big(B \land [\alpha](B \land [\alpha][\alpha^*]B)\big)}}{A \vdash B \land [\alpha]\big(B \land [\alpha](B \land [\alpha][\alpha^*]B)\big)}\land R}{A \vdash B \land [\alpha](B \land [\alpha][\alpha^*]B)}[^*]}{A \vdash B \land [\alpha][\alpha^*]B}[^*]}{A \vdash [\alpha^*]B}[^*]$$

Loops of Proofs: Iterations & Generalizations

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

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

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

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

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

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

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

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

$$
\text{[*]}\dfrac{\text{[*]}\dfrac{\text{[*]}\dfrac{\land\text{R}\dfrac{A \vdash B \qquad \text{MR}\dfrac{A \vdash [\alpha]{\color{green}J_1} \qquad \land\text{R}\dfrac{{\color{green}J_1} \vdash B \qquad \text{MR}\dfrac{{\color{green}J_1} \vdash [\alpha]{\color{green}J_2} \qquad \dfrac{}{{\color{green}J_2} \vdash B \land [\alpha][\alpha^*]B}}{{\color{green}J_1} \vdash {\color{red}[\alpha](B \land [\alpha][\alpha^*]B)}}}{{\color{green}J_1} \vdash B \land [\alpha](B \land [\alpha][\alpha^*]B)}}{A \vdash [\alpha]\big(B \land [\alpha](B \land [\alpha][\alpha^*]B)\big)}}{A \vdash B \land [\alpha]\big(B \land [\alpha](B \land [\alpha][\alpha^*]B)\big)}}{A \vdash B \land [\alpha](B \land [\alpha][\alpha^*]B)}}{A \vdash B \land [\alpha][\alpha^*]B}}{A \vdash [\alpha^*]B}
$$

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

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

$$J_2 \vdash B \qquad \overline{\qquad\qquad\qquad\qquad}$$

$$J_2 \vdash [\alpha][\alpha^*]B$$

$$J_1 \vdash [\alpha]J_2 \ \land\text{R}\ \overline{\qquad\qquad\qquad\qquad}$$

$$J_2 \vdash \color{red}{B \land [\alpha][\alpha^*]B}$$

$$J_1 \vdash B \ \text{MR}\ \overline{\qquad\qquad\qquad\qquad}$$

$$J_1 \vdash [\alpha](B \land [\alpha][\alpha^*]B)$$

$$A \vdash [\alpha]J_1 \ \land\text{R}\ \overline{\qquad\qquad\qquad\qquad}$$

$$J_1 \vdash B \land [\alpha](B \land [\alpha][\alpha^*]B)$$

$$A \vdash B \ \text{MR}\ \overline{\qquad\qquad\qquad\qquad}$$

$$A \vdash [\alpha]\big(B \land [\alpha](B \land [\alpha][\alpha^*]B)\big)$$

$$\land\text{R}\ \overline{\qquad\qquad\qquad\qquad}$$

$$A \vdash B \land [\alpha]\big(B \land [\alpha](B \land [\alpha][\alpha^*]B)\big)$$

$$[^*]\ \overline{\qquad\qquad\qquad\qquad}$$

$$A \vdash B \land [\alpha](B \land [\alpha][\alpha^*]B)$$

$$[^*]\ \overline{\qquad\qquad\qquad\qquad}$$

$$A \vdash B \land [\alpha][\alpha^*]B$$

$$[^*]\ \overline{\qquad\qquad\qquad\qquad}$$

$$A \vdash [\alpha^*]B$$

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

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

$$\dfrac{\dfrac{\dfrac{A \vdash B \quad \dfrac{A \vdash [\alpha]J_1 \quad \dfrac{J_1 \vdash B \quad \dfrac{J_1 \vdash [\alpha]J_2 \quad \dfrac{J_2 \vdash B \quad \dfrac{J_2 \vdash [\alpha]J_3 \quad \dots}{J_2 \vdash [\alpha][\alpha^*]B}}{J_2 \vdash B \land [\alpha][\alpha^*]B}\ \land\text{R}}{J_1 \vdash [\alpha](B \land [\alpha][\alpha^*]B)}\ \text{MR}}{J_1 \vdash B \land [\alpha](B \land [\alpha][\alpha^*]B)}\ \land\text{R}}{A \vdash [\alpha]\big(B \land [\alpha](B \land [\alpha][\alpha^*]B)\big)}\ \text{MR}}{A \vdash B \land [\alpha]\big(B \land [\alpha](B \land [\alpha][\alpha^*]B)\big)}\ \land\text{R}}{\dfrac{A \vdash B \land [\alpha](B \land [\alpha][\alpha^*]B)}{\dfrac{A \vdash B \land [\alpha][\alpha^*]B}{A \vdash [\alpha^*]B}\ [^*]}\ [^*]}\ [^*]$$

Loops of Proofs: Common Generalizations

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

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

$$
{\scriptstyle [*]}\dfrac{
{\scriptstyle [*]}\dfrac{
{\scriptstyle [*]}\dfrac{
{\scriptstyle \land R}\dfrac{
A \vdash B \qquad
{\scriptstyle \text{MR}}\dfrac{
A \vdash [\alpha]J \qquad
{\scriptstyle \land R}\dfrac{
J \vdash B \qquad
{\scriptstyle \text{MR}}\dfrac{
J \vdash [\alpha]J \qquad
{\scriptstyle \land R}\dfrac{
J \vdash B \qquad
\dfrac{J \vdash [\alpha]J \qquad \dots}{J \vdash [\alpha][\alpha^*]B}
}{J \vdash B \land [\alpha][\alpha^*]B}
}{J \vdash [\alpha](B \land [\alpha][\alpha^*]B)}
}{J \vdash B \land [\alpha](B \land [\alpha][\alpha^*]B)}
}{A \vdash [\alpha]\big(B \land [\alpha](B \land [\alpha][\alpha^*]B)\big)}
}{A \vdash B \land [\alpha]\big(B \land [\alpha](B \land [\alpha][\alpha^*]B)\big)}
}{A \vdash B \land [\alpha](B \land [\alpha][\alpha^*]B)}
}{A \vdash B \land [\alpha][\alpha^*]B}
}{A \vdash [\alpha^*]B}
$$

Loops of Proofs: Extracting a Proof Rule

$$\dfrac{\color{red}{J \vdash B}}{A \vdash [\alpha^*]B}$$

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

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

$$
[*]\dfrac{[*]\dfrac{[*]\dfrac{\land R\dfrac{A \vdash B \qquad \text{MR}\dfrac{A \vdash [\alpha]J \qquad \land R\dfrac{\color{red}{J \vdash B} \qquad \text{MR}\dfrac{J \vdash [\alpha]J \qquad \land R\dfrac{\color{red}{J \vdash B} \qquad \dfrac{J \vdash [\alpha]J \qquad \ldots}{J \vdash [\alpha][\alpha^*]B}}{J \vdash B \land [\alpha][\alpha^*]B}}{J \vdash [\alpha](B \land [\alpha][\alpha^*]B)}}{J \vdash B \land [\alpha](B \land [\alpha][\alpha^*]B)}}{A \vdash [\alpha]\big(B \land [\alpha](B \land [\alpha][\alpha^*]B)\big)}}{A \vdash B \land [\alpha]\big(B \land [\alpha](B \land [\alpha][\alpha^*]B)\big)}}{A \vdash B \land [\alpha](B \land [\alpha][\alpha^*]B)}}{A \vdash B \land [\alpha][\alpha^*]B}}{A \vdash [\alpha^*]B}
$$

Loops of Proofs: Extracting a Proof Rule

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

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

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

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

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

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

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

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

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

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

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

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

Invariant J generalized intermediate condition

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

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

André Platzer.
Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics.
Springer, Heidelberg, 2010.
URL: http://www.springer.com/978-3-642-14508-7,
doi:10.1007/978-3-642-14509-4.

André Platzer.
The complete proof theory of hybrid systems.
In *LICS*, pages 541–550, Los Alamitos, 2012. IEEE.
doi:10.1109/LICS.2012.64.