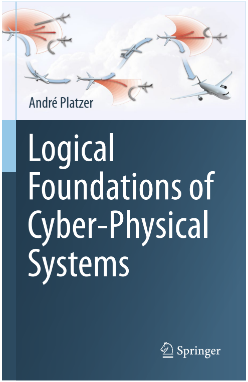
07: Control Loops & Invariants

Logical Foundations of Cyber-Physical Systems



André Platzer

Carnegie Mellon University
Computer Science Department

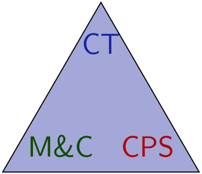
Outline

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

1. Learning Objectives

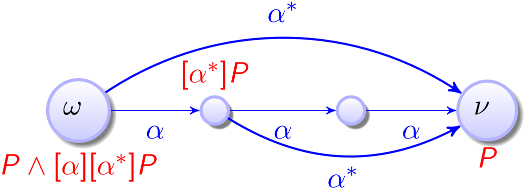
2. Induction for Loops
   - Iteration Axiom
   - Induction Axiom
   - Induction Rule for Loops
   - Loop Invariants
   - Simple Example
   - Contextual Soundness Requirements

3. Operationalize Invariant Construction
   - Bouncing Ball
   - Rescuing Misplaced Constants
   - Safe Quantum

4. Summary

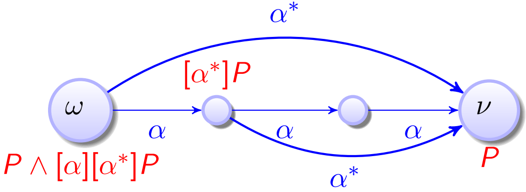
Iteration Axiom

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



Iteration Axiom

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

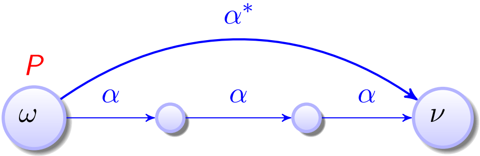


Problem: Proof for $[\alpha^*]P$ needs proof of $[\alpha][\alpha^*]P$

Induction Axiom

Lemma ( )

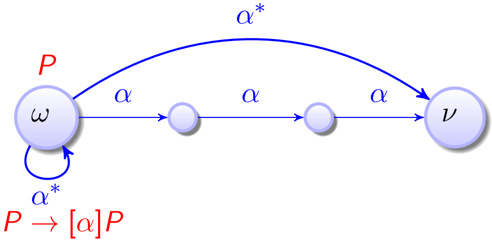
$$\mathrm{I}\quad [\alpha^*]P \leftrightarrow P \land$$



Induction Axiom

Lemma ( )

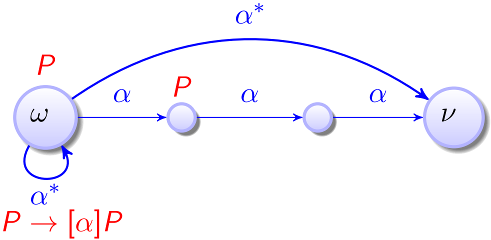
$$| \quad [\alpha^*]P \leftrightarrow P \land \qquad (P \rightarrow [\alpha]P)$$



Induction Axiom

Lemma ( )

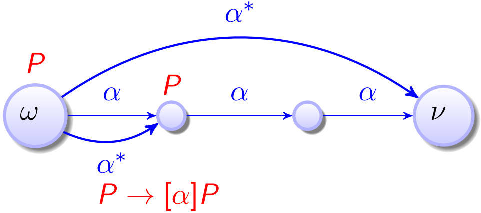
$$| \quad [\alpha^*]P \leftrightarrow P \land \qquad (P \to [\alpha]P)$$



Induction Axiom

Lemma (I is sound)

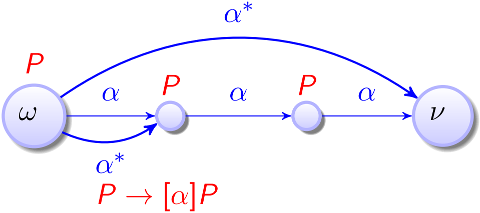
$$\text{I} \quad [\alpha^*]P \leftrightarrow P \land [\alpha^*](P \rightarrow [\alpha]P)$$



Induction Axiom

Lemma (I is sound)

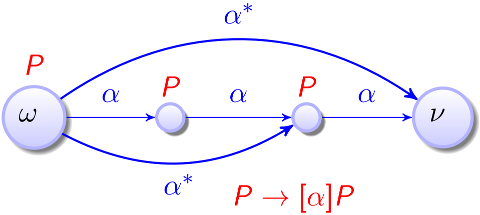
$$\text{I} \quad [\alpha^*]P \leftrightarrow P \land [\alpha^*](P \rightarrow [\alpha]P)$$



Induction Axiom

Lemma (I is sound)

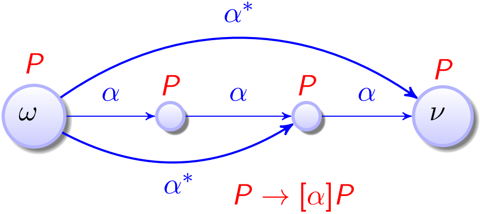
$$\text{I} \quad [\alpha^*]P \leftrightarrow P \land [\alpha^*](P \rightarrow [\alpha]P)$$



Induction Axiom

Lemma (I is sound)

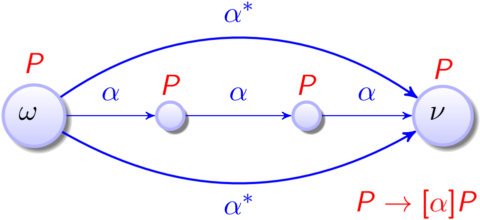
$$\text{I} \quad [\alpha^*]P \leftrightarrow P \wedge [\alpha^*](P \rightarrow [\alpha]P)$$



Induction Axiom

Lemma (I is sound)

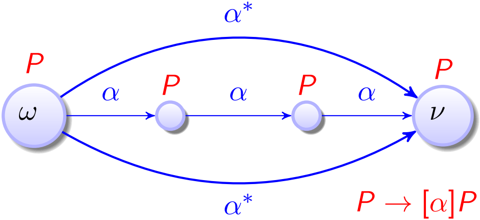
$$\text{I} \quad [\alpha^*]P \leftrightarrow P \land [\alpha^*](P \rightarrow [\alpha]P)$$



Induction Axiom

Lemma (I is sound)

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



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)

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

Induction Rule for Loops

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

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

Lemma (Loop induction rule ind is sound)

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

Proof (Derived rule).

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

□

Induction Rule for Loops

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

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

Lemma (Loop induction rule ind is sound)

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

Proof (Derived rule).

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

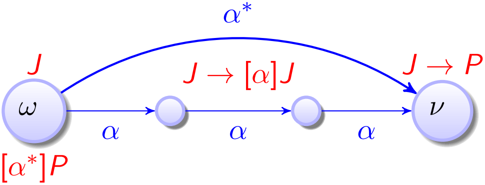
Problem: Rule ind is no equivalence. Its use of G may lose information: $\square$
$[\alpha^*](P \to [\alpha]P)$ true but $P \vdash [\alpha]P$ is not valid.

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)

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



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)

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

Proof (Derived rule).

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

□

Loop Invariants

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

Lemma (Loop invariant rule loop is sound)

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

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

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

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

1. $J \equiv x \geq 0$

A Simple Discrete Loop Example

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

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

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

A Simple Discrete Loop Example

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

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

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

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

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

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

A Simple Discrete Loop Example

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

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

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

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

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

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

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

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

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

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

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

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 $J \equiv x \geq y \land y \geq 0$ correct loop invariant

Forgot to Add Sequent Context Γ, Δ to Premises

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

Forgot to Add Sequent Context Γ, Δ to Premises

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

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

Forgot to Add Sequent Context Γ, Δ to Premises

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

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

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

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

1. Learning Objectives
2. Induction for Loops
   - Iteration Axiom
   - Induction Axiom
   - Induction Rule for Loops
   - Loop Invariants
   - Simple Example
   - Contextual Soundness Requirements
3. Operationalize Invariant Construction
   - Bouncing Ball
   - Rescuing Misplaced Constants
   - Safe Quantum
4. Summary

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

$$\begin{aligned} A &\equiv 0 \le x \land x = H \land v = 0 \land g > 0 \land 1 \ge c \ge 0 \\ B(x,v) &\equiv 0 \le x \land x \le H \\ \mathrm{grav} &\equiv \{x' = v, v' = -g \,\&\, x \ge 0\} \end{aligned}$$

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

② $\mathrm{j}(x,v) \equiv 0 \leq x \wedge x \leq H$

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

$\mathrm{j}(x,v) \vdash [\{x'=v, v'=-g \,\&\, x\geq0\}](\mathrm{j}(x,v))$

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

$\mathrm{j}(x,v), x\neq0 \vdash \mathrm{j}(x,v)$

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

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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 $v \gg 0$

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

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. $\mathrm{j}(x,v) \equiv x = 0 \land v = 0$

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

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 $x > 0$

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

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

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

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. $\mathrm{j}(x,v) \equiv x = 0 \lor x = H \land v = 0$

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

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. $j(x,v) \equiv x = 0 \lor x = H \land v = 0$ no space for intermediate states

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

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. $j(x,v) \equiv x = 0 \lor x = H \land v = 0$ no space for intermediate states
5. $j(x,v) \equiv 2gx=2gH-v^2 \land x\geq 0$

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

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

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

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
5. $\mathrm{j}(x,v) \equiv 2gx=2gH-v^2 \land x\geq 0$ works: implicitly links v and x

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

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

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

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 $c = 1 \ldots$

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

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

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

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 $c = 1 \ldots$

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

✓ $2gx{=}2gH{-}v^2 \land x{\geq}0, x{=}0 \vdash 2gx{=}2gH{-}(-cv)^2 \land x{\geq}0$ 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. $\mathrm{j}(x,v) \equiv x \geq 0$ 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. $\mathrm{j}(x,v) \equiv 2gx{=}2gH{-}v^2 \land x{\geq}0$ works: implicitly links v and x

Proving Quantum the Acrophobic Bouncing Ball

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

Proving Quantum the Acrophobic Bouncing Ball

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

Proving Quantum the Acrophobic Bouncing Ball

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

Proving Quantum the Acrophobic Bouncing Ball

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

Proving Quantum the Acrophobic Bouncing Ball

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

Proving Quantum the Acrophobic Bouncing Ball

$$j(x,v) \equiv 2gx=2gH-v^2 \land x\geq0$$

$$\begin{array}{ll}
\cline{2-2}
 & 2gx=2gH-v^2\land x\geq0,\ H-\frac{g}{2}t^2\geq0 \vdash 2g(H-\frac{g}{2}t^2)=2gH-(gt)^2\land(H-\frac{g}{2}t^2)\geq0 \\
 & j(x,v),\ t\geq0,\ H-\frac{g}{2}t^2\geq0 \vdash j(H-\frac{g}{2}t^2,-gt) \\
\cline{2-2}
\rightarrow\mathrm{R} & j(x,v) \vdash t\geq0 \rightarrow H-\frac{g}{2}t^2\geq0 \rightarrow j(H-\frac{g}{2}t^2,-gt) \\
\cline{2-2}
\forall\mathrm{R} & j(x,v) \vdash \forall t\geq0\, (H-\frac{g}{2}t^2\geq0 \rightarrow j(H-\frac{g}{2}t^2,-gt)) \\
\cline{2-2}
[:=] & j(x,v) \vdash \forall t\geq0\, [x:=H-\frac{g}{2}t^2](x\geq0 \rightarrow j(x,-gt)) \\
\cline{2-2}
[:=] & j(x,v) \vdash \forall t\geq0\, [x:=H-\frac{g}{2}t^2][v:=-gt](x\geq0 \rightarrow j(x,v)) \\
\cline{2-2}
[;] & j(x,v) \vdash \forall t\geq0\, [x:=H-\frac{g}{2}t^2;\ v:=-gt](x\geq0 \rightarrow j(x,v)) \\
\cline{2-2}
['] & j(x,v) \vdash [x'=v,\ v'=-g\ \&\ x\geq0]j(x,v)
\end{array}$$

Proving Quantum the Acrophobic Bouncing Ball

$$\land\mathrm{R}\,\dfrac{\dfrac{}{2gx=2gH-v^2 \vdash 2g(H-\frac{g}{2}t^2)=2gH-(gt)^2} \qquad \dfrac{}{H-\frac{g}{2}t^2\geq0 \vdash H-\frac{g}{2}t^2\geq0}}{2gx=2gH-v^2\land x\geq0,\ H-\frac{g}{2}t^2\geq0 \vdash \color{red}{2g(H-\frac{g}{2}t^2)=2gH-(gt)^2\land(H-\frac{g}{2}t^2)\geq0}}$$

$$[']\,\dfrac{[;]\,\dfrac{[:=]\,\dfrac{[:=]\,\dfrac{\forall\mathrm{R}\,\dfrac{\to\mathrm{R}\,\dfrac{\mathrm{j}(x,v),\ t\geq0,\ H-\frac{g}{2}t^2\geq0 \vdash \mathrm{j}(H-\frac{g}{2}t^2,-gt)}{\mathrm{j}(x,v) \vdash t\geq0 \to H-\frac{g}{2}t^2\geq0 \to \mathrm{j}(H-\frac{g}{2}t^2,-gt)}}{\mathrm{j}(x,v) \vdash \forall t\geq0\,(H-\frac{g}{2}t^2\geq0 \to \mathrm{j}(H-\frac{g}{2}t^2,-gt))}}{\mathrm{j}(x,v) \vdash \forall t\geq0\,[x:=H-\frac{g}{2}t^2](x\geq0 \to \mathrm{j}(x,-gt))}}{\mathrm{j}(x,v) \vdash \forall t\geq0\,[x:=H-\frac{g}{2}t^2][v:=-gt](x\geq0 \to \mathrm{j}(x,v))}}{\mathrm{j}(x,v) \vdash \forall t\geq0\,[x:=H-\frac{g}{2}t^2;\ v:=-gt](x\geq0 \to \mathrm{j}(x,v))}}{\mathrm{j}(x,v) \vdash [x'=v,\ v'=-g\ \&\ x\geq0]\mathrm{j}(x,v)}$$

Proving Quantum the Acrophobic Bouncing Ball

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

Proving Quantum the Acrophobic Bouncing Ball

$$\wedge\text{R}\,\cfrac{\mathbb{R}\,\dfrac{*}{2gx=2gH-v^2 \vdash 2g(H-\frac{g}{2}t^2)=2gH-(gt)^2} \qquad \text{id}\,\dfrac{*}{H-\frac{g}{2}t^2\geq0 \vdash H-\frac{g}{2}t^2\geq0}}{2gx=2gH-v^2\wedge x\geq0,\ H-\frac{g}{2}t^2\geq0 \vdash 2g(H-\frac{g}{2}t^2)=2gH-(gt)^2\wedge(H-\frac{g}{2}t^2)\geq0}$$

$$\begin{array}{rc}
 & \mathsf{j}(x,v),\ t\geq0,\ H-\frac{g}{2}t^2\geq0 \vdash \mathsf{j}(H-\frac{g}{2}t^2,-gt) \\ \hline
\to\text{R} & \mathsf{j}(x,v) \vdash t\geq0 \to H-\frac{g}{2}t^2\geq0 \to \mathsf{j}(H-\frac{g}{2}t^2,-gt) \\ \hline
\forall\text{R} & \mathsf{j}(x,v) \vdash \forall t\geq0\,(H-\frac{g}{2}t^2\geq0 \to \mathsf{j}(H-\frac{g}{2}t^2,-gt)) \\ \hline
[:=] & \mathsf{j}(x,v) \vdash \forall t\geq0\,[x:=H-\frac{g}{2}t^2](x\geq0 \to \mathsf{j}(x,-gt)) \\ \hline
[:=] & \mathsf{j}(x,v) \vdash \forall t\geq0\,[x:=H-\frac{g}{2}t^2][v:=-gt](x\geq0 \to \mathsf{j}(x,v)) \\ \hline
[;] & \mathsf{j}(x,v) \vdash \forall t\geq0\,[x:=H-\frac{g}{2}t^2;\ v:=-gt](x\geq0 \to \mathsf{j}(x,v)) \\ \hline
['] & \mathsf{j}(x,v) \vdash [x'=v,\ v'=-g\ \&\ x\geq0]\mathsf{j}(x,v)
\end{array}$$

- Is Quantum done with his safety proof?

Proving Quantum the Acrophobic Bouncing Ball

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

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

- 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 assumption $\mathrm{j}(x,v)$ can't guarantee!

Proving Quantum the Acrophobic Bouncing Ball

$$\wedge R\;\dfrac{\mathbb{R}\;\dfrac{*}{2gx=2gH-v^2 \vdash 2g(H-\frac{g}{2}t^2)=2gH-(gt)^2} \qquad \mathrm{id}\;\dfrac{*}{H-\frac{g}{2}t^2\geq0 \vdash H-\frac{g}{2}t^2\geq0}}{2gx=2gH-v^2\wedge x\geq0,\ H-\frac{g}{2}t^2\geq0 \vdash 2g(H-\frac{g}{2}t^2)=2gH-(gt)^2\wedge(H-\frac{g}{2}t^2)\geq0}$$

$$['']\;\dfrac{[;]\;\dfrac{[:=]\;\dfrac{[:=]\;\dfrac{\forall R\;\dfrac{\to R\;\dfrac{\mathrm{j}(x,v),\ t\geq0,\ H-\frac{g}{2}t^2\geq0 \vdash \mathrm{j}(H-\frac{g}{2}t^2,-gt)}{\mathrm{j}(x,v) \vdash t\geq0 \to H-\frac{g}{2}t^2\geq0 \to \mathrm{j}(H-\frac{g}{2}t^2,-gt)}}{\mathrm{j}(x,v) \vdash \forall t\geq0\,(H-\frac{g}{2}t^2\geq0 \to \mathrm{j}(H-\frac{g}{2}t^2,-gt))}}{\mathrm{j}(x,v) \vdash \forall t\geq0\,[x:=H-\frac{g}{2}t^2](x\geq0 \to \mathrm{j}(x,-gt))}}{\mathrm{j}(x,v) \vdash \forall t\geq0\,[x:=H-\frac{g}{2}t^2][v:=-gt](x\geq0 \to \mathrm{j}(x,v))}}{\mathrm{j}(x,v) \vdash \forall t\geq0\,[x:=H-\frac{g}{2}t^2;\, v:=-gt](x\geq0 \to \mathrm{j}(x,v))}}{\mathrm{j}(x,v) \vdash [x'=v,\, v'=-g\,\&\,x\geq0]\mathrm{j}(x,v)}$$

- Is Quantum done with his safety proof?
- Oh no! The solutions we sneaked into ['] only solve the ODE/IVP if $x = 0, v = 0$ 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. $\mathrm{j}(x,v) \equiv 2gx{=}2gH{-}v^2 \wedge x{\geq}0$
2. $p \equiv c{=}1 \wedge g{>}0$

Clumsy Quantum Misplaced the Constants

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

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

Clumsy Quantum Misplaced the Constants

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

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

Clumsy Quantum Misplaced the Constants

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

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

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

Clumsy Quantum Misplaced the Constants

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

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

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

Clumsy Quantum Misplaced the Constants

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

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

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

Quantum the Provably Safe Bouncing Ball

Proposition (Quantum can bounce around safely)

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

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

$$\textbf{requires}(0 \leq x \land x = H \land v = 0)$$

$$\textbf{requires}(g > 0 \land 1 = c)$$

$$\textbf{ensures}(0 \leq x \land x \leq H)$$

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

$$(?x = 0; v{:=}{-cv} \cup ?x \neq 0))\}^* \textbf{@invariant}(2gx = 2gH - v^2 \land x \geq 0)$$

Invariant Contracts

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

Outline

1. Learning Objectives
2. Induction for Loops
   - Iteration Axiom
   - Induction Axiom
   - Induction Rule for Loops
   - Loop Invariants
   - Simple Example
   - Contextual Soundness Requirements
3. Operationalize Invariant Construction
   - Bouncing Ball
   - Rescuing Misplaced Constants
   - Safe Quantum
4. Summary

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

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 ⇒ compositional rules!

Loops of Proofs: Iterations

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

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

Loops of Proofs: Iterations

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

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

Loops of Proofs: Iterations

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

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

Loops of Proofs: Iterations

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

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

Loops of Proofs: Iterations & Splitting the Box

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

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

$$\begin{array}{r|c}
 & \\ \hline
 & A \vdash B \land [\alpha]B \land [\alpha][\alpha](B \land [\alpha][\alpha^*]B) \\ \hline
[]\land & A \vdash B \land \color{red}{[\alpha]\big(B \land [\alpha](B \land [\alpha][\alpha^*]B)\big)} \\ \hline
[*] & A \vdash B \land [\alpha](B \land [\alpha][\alpha^*]B) \\ \hline
[*] & A \vdash B \land [\alpha][\alpha^*]B \\ \hline
[*] & A \vdash [\alpha^*]B
\end{array}$$

Loops of Proofs: Iterations & Splitting the Box

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

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

$$\begin{array}{rc}
\cline{2-2}
 & A \vdash B \land [\alpha]B \land [\alpha]([\alpha]B \land [\alpha][\alpha][\alpha^*]B) \\
\cline{2-2}
[]\land & A \vdash B \land [\alpha]B \land [\alpha][\alpha](B \land [\alpha][\alpha^*]B) \\
\cline{2-2}
[]\land & A \vdash B \land [\alpha]\big(B \land [\alpha](B \land [\alpha][\alpha^*]B)\big) \\
\cline{2-2}
[*] & A \vdash B \land [\alpha](B \land [\alpha][\alpha^*]B) \\
\cline{2-2}
[*] & A \vdash B \land [\alpha][\alpha^*]B \\
\cline{2-2}
[*] & A \vdash [\alpha^*]B
\end{array}$$

Loops of Proofs: Iterations & Splitting the Box

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

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

$$\begin{array}{rc}
\cline{2-2}
 & A \vdash B \land [\alpha]B \land [\alpha][\alpha]B \land [\alpha][\alpha][\alpha][\alpha^*]B \\
\cline{2-2}
[]\land & A \vdash B \land [\alpha]B \land {\color{red}[\alpha]([\alpha]B \land [\alpha][\alpha][\alpha^*]B)} \\
\cline{2-2}
[]\land & A \vdash B \land [\alpha]B \land [\alpha][\alpha](B \land [\alpha][\alpha^*]B) \\
\cline{2-2}
[]\land & A \vdash B \land [\alpha]\big(B \land [\alpha](B \land [\alpha][\alpha^*]B)\big) \\
\cline{2-2}
[*] & A \vdash B \land [\alpha](B \land [\alpha][\alpha^*]B) \\
\cline{2-2}
[*] & A \vdash B \land [\alpha][\alpha^*]B \\
\cline{2-2}
[*] & A \vdash [\alpha^*]B
\end{array}$$

Loops of Proofs: Iterations & Splitting the Box

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

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

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

Loops of Proofs: Iterations & Splitting the Box

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

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

$$\begin{array}{r|c}
 & A \vdash B \qquad A \vdash [\alpha]B \qquad A \vdash [\alpha][\alpha]B \qquad A \vdash [\alpha][\alpha][\alpha][\alpha^*]B \\ \cline{2-2}
\wedge\mathrm{R} & A \vdash B \wedge [\alpha]B \wedge [\alpha][\alpha]B \wedge [\alpha][\alpha][\alpha][\alpha^*]B \\ \cline{2-2}
[]\wedge & A \vdash B \wedge [\alpha]B \wedge [\alpha]([\alpha]B \wedge [\alpha][\alpha][\alpha^*]B) \\ \cline{2-2}
[]\wedge & A \vdash B \wedge [\alpha]B \wedge [\alpha][\alpha](B \wedge [\alpha][\alpha^*]B) \\ \cline{2-2}
[]\wedge & A \vdash B \wedge [\alpha]\big(B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)\big) \\ \cline{2-2}
[^*] & A \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B) \\ \cline{2-2}
[^*] & A \vdash B \wedge [\alpha][\alpha^*]B \\ \cline{2-2}
[^*] & A \vdash [\alpha^*]B
\end{array}$$

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

Loops of Proofs: Iterations & Generalizations

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

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

Loops of Proofs: Iterations & Generalizations

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

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

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

Loops of Proofs: Iterations & Generalizations

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

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

$$\scriptstyle[^*]\displaystyle\frac{\scriptstyle[^*]\displaystyle\frac{\scriptstyle[^*]\displaystyle\frac{\scriptstyle\wedge R\displaystyle\frac{A \vdash B \quad \scriptstyle\text{MR}\displaystyle\frac{A \vdash [\alpha]J_1 \qquad \displaystyle\frac{}{J_1 \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)}}{A \vdash [\alpha]\big(B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)\big)}}{A \vdash B \wedge [\alpha]\big(B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)\big)}}{A \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)}}{A \vdash B \wedge [\alpha][\alpha^*]B}}{A \vdash [\alpha^*]B}$$

Loops of Proofs: Iterations & Generalizations

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

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

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

Loops of Proofs: Iterations & Generalizations

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

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

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

Loops of Proofs: Iterations & Generalizations

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

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

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

Loops of Proofs: Iterations & Generalizations

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

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

$$[^*]\,\dfrac{[^*]\,\dfrac{[^*]\,\dfrac{\wedge\mathrm{R}\,\dfrac{A \vdash B \qquad \mathrm{MR}\,\dfrac{A \vdash [\alpha]J_1 \qquad \wedge\mathrm{R}\,\dfrac{J_1 \vdash B \qquad \mathrm{MR}\,\dfrac{J_1 \vdash [\alpha]J_2 \qquad \wedge\mathrm{R}\,\dfrac{J_2 \vdash B \qquad \dfrac{J_2 \vdash [\alpha]J_3 \qquad \dots}{J_2 \vdash [\alpha][\alpha^*]B}}{J_2 \vdash B \land [\alpha][\alpha^*]B}}{J_1 \vdash [\alpha](B \land [\alpha][\alpha^*]B)}}{J_1 \vdash B \land [\alpha](B \land [\alpha][\alpha^*]B)}}{A \vdash [\alpha]\big(B \land [\alpha](B \land [\alpha][\alpha^*]B)\big)}}{A \vdash B \land [\alpha]\big(B \land [\alpha](B \land [\alpha][\alpha^*]B)\big)}}{A \vdash B \land [\alpha](B \land [\alpha][\alpha^*]B)}}{A \vdash B \land [\alpha][\alpha^*]B}}{A \vdash [\alpha^*]B}$$

Loops of Proofs: Common Generalizations

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

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

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

Loops of Proofs: Extracting a Proof Rule

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

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

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

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

Loops of Proofs: Extracting a Proof Rule

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

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

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

$$[*]\,\dfrac{[*]\,\dfrac{[*]\,\dfrac{\land\mathrm{R}\,\dfrac{A \vdash B \quad \mathrm{MR}\,\dfrac{A \vdash [\alpha]J \quad \land\mathrm{R}\,\dfrac{J \vdash B \quad \mathrm{MR}\,\dfrac{\textcolor{red}{J \vdash [\alpha]J} \quad \land\mathrm{R}\,\dfrac{J \vdash B \quad \dfrac{\textcolor{red}{J \vdash [\alpha]J} \quad \dots}{J \vdash [\alpha][\alpha^*]B}}{J \vdash B \land [\alpha][\alpha^*]B}}{J \vdash [\alpha](B \land [\alpha][\alpha^*]B)}}{J \vdash B \land [\alpha](B \land [\alpha][\alpha^*]B)}}{A \vdash [\alpha]\big(B \land [\alpha](B \land [\alpha][\alpha^*]B)\big)}}{A \vdash B \land [\alpha]\big(B \land [\alpha](B \land [\alpha][\alpha^*]B)\big)}}{A \vdash B \land [\alpha](B \land [\alpha][\alpha^*]B)}}{A \vdash B \land [\alpha][\alpha^*]B}}{A \vdash [\alpha^*]B}$$

Loops of Proofs: Extracting a Proof Rule

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

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

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

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

Loops of Proofs: Loop Invariants

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

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

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

Invariant J generalized
intermediate condition

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

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

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

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