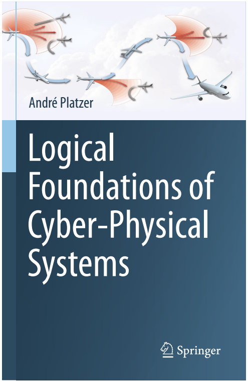
07: Control Loops & Invariants

Logical Foundations of Cyber-Physical Systems



Stefan Mitsch

Carnegie Mellon University
Computer Science Department

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

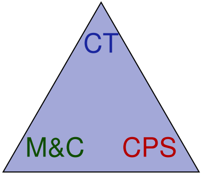
Outline

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

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

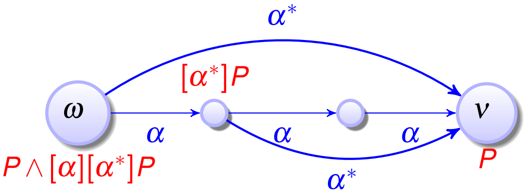
semantics of control loops
operational effects of control

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

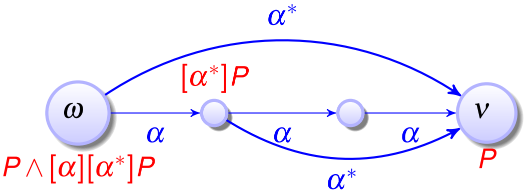
Iteration Axiom

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



Iteration Axiom

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

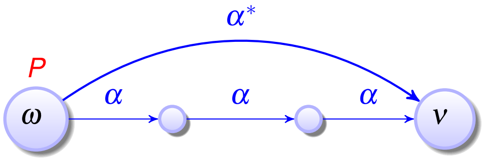


Problem: Proof for $[\alpha^*]P$ needs proof of $[\alpha][\alpha^*]P$

Induction Axiom

Lemma ( )

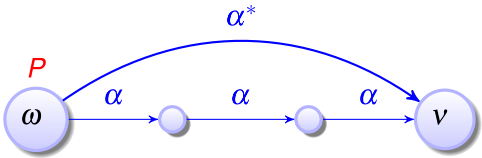
I $[\alpha^*]P \leftrightarrow P \land$



Induction Axiom

Lemma ( )

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

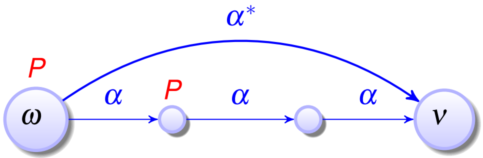


$P \rightarrow [\alpha]P$

Induction Axiom

Lemma ( )

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

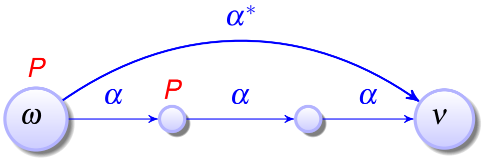


$P \rightarrow [\alpha]P$

Induction Axiom

Lemma (I is sound)

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

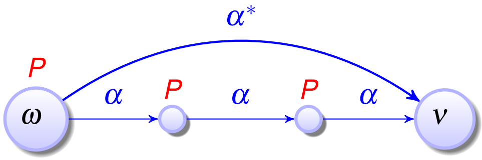


$P \rightarrow [\alpha]P \quad P \rightarrow [\alpha]P$

Induction Axiom

Lemma (I is sound)

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

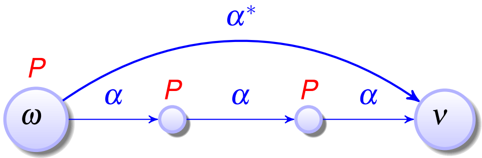


$P \rightarrow [\alpha]P \quad P \rightarrow [\alpha]P$

Induction Axiom

Lemma (I is sound)

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

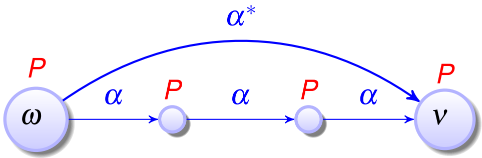


$P \to [\alpha]P \quad P \to [\alpha]P \quad P \to [\alpha]P$

Induction Axiom

Lemma (I is sound)

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

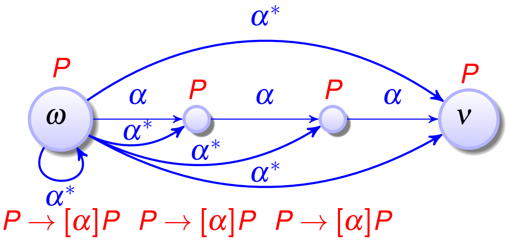


$P \rightarrow [\alpha]P$ $P \rightarrow [\alpha]P$ $P \rightarrow [\alpha]P$

Induction Axiom

Lemma (I is sound)

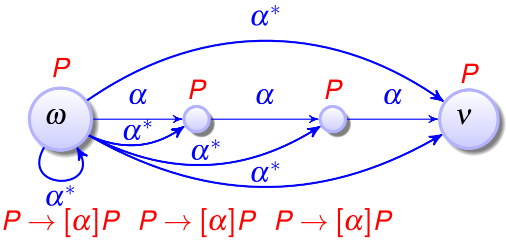
$$\text{I} \quad [\alpha^*]P \leftrightarrow P \land [\alpha^*](P \rightarrow [\alpha]P)$$



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 $[\alpha^*](P \rightarrow [\alpha]P)$

from $[\alpha^*]P \leftrightarrow P \land [\alpha^*](P \rightarrow [\alpha]P)$ by Gödel

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

Lemma (Loop induction rule ind is sound)

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

Induction Rule for Loops

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

from $[\alpha^*]P \leftrightarrow P \land [\alpha^*](P \rightarrow [\alpha]P)$ by Gödel $\quad \text{G} \ \dfrac{P}{[\alpha]P}$

Lemma (Loop induction rule ind is sound)

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

Proof (Derived rule).

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

□

Induction Rule for Loops

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

from $[\alpha^*]P \leftrightarrow P \land [\alpha^*](P \to [\alpha]P)$ by Gödel

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

Lemma (Loop induction rule ind is sound)

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

Proof (Derived rule).

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

□

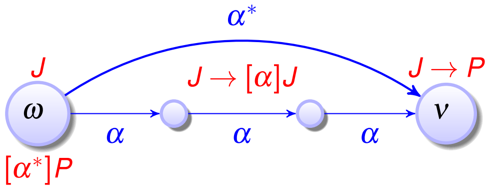
Problem: Rule ind is no equivalence. Its use of G may lose information: $[\alpha^*](P \to [\alpha]P)$ true but $P \vdash [\alpha]P$ is not valid.

Loop Invariants

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

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

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

Lemma (Loop invariant rule loop is sound)

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

Proof (Derived rule).

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

□

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

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

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

1. $J \equiv x \geq 0$

A Simple Discrete Loop Example

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

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

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

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

A Simple Discrete Loop Example

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

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

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

A Simple Discrete Loop Example

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

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

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

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

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

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 $x < y$

A Simple Discrete Loop Example

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

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

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

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

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

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

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. $J \equiv x \geq 0 \land y \geq 0$ — 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?

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

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

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

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 assumptions go,
or 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 Bouncing Ball

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

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

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

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

Proving Quantum the Bouncing Ball

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

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

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

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

Proving Quantum the Bouncing Ball

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

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

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

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

Proving Quantum the Bouncing Ball

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

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

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

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

Proving Quantum the Bouncing Ball

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

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

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

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

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

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

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

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

Proving Quantum the Bouncing Ball

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

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

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

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

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

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

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

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

Proving Quantum the Bouncing Ball

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

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

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

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

Proving Quantum the Bouncing Ball

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

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

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

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

Proving Quantum the Bouncing Ball

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

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

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

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

Proving Quantum the Bouncing Ball

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

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

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

$$[?]\ \dfrac{j(x,v),\, x\neq 0 \vdash j(x,v)}{j(x,v) \vdash [?x\neq 0]j(x,v)}$$

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

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

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

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

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

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

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

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

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

Proving Quantum the Bouncing Ball

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

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

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

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

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

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

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

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

Proving Quantum the Bouncing Ball

$A \vdash j(x,v)$

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

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

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

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

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

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

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

Proving Quantum the Bouncing Ball

$A \vdash j(x,v)$

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

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

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

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

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

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

Proving Quantum the Bouncing Ball

$A \vdash j(x,v)$

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

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

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

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

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

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

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

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

Proving Quantum the Bouncing Ball

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

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

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

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

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

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

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

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

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

Proving Quantum the Bouncing Ball

$A \vdash j(x,v)$

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

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

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

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

1. $j(x,v) \equiv 0 \leq x \wedge x \leq H$ — weak: fails ODE if $v \gg 0$
2. $j(x,v) \equiv 2gx = 2gH - v^2 \wedge x \geq 0$ — works: implicitly links v and x

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

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

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

Proving Quantum the Bouncing Ball

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

Proving Quantum the Bouncing Ball

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

Proving Quantum the Bouncing Ball

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

Proving Quantum the Bouncing Ball

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

Proving Quantum the Bouncing Ball

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

Proving Quantum the Bouncing Ball

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

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

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

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

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

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

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

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

Proving Quantum the Bouncing Ball

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

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

Proving Quantum the Bouncing Ball

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

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

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

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

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

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

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

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

Proving Quantum the Bouncing Ball

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

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

Proving Quantum the Bouncing Ball

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

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

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

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

- Wait, was this actually a safety proof for Quantum?

Proving Quantum the Bouncing Ball

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

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

- Wait, was this actually a safety proof for Quantum?
- Oh no! The solutions we sneaked into $[']$ only solve the ODE/IVP if $x = H, v = 0$ which assumption $j(x,v)$ can't guarantee!

Proving Quantum the Bouncing Ball

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

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

- Wait, was this actually a safety proof for Quantum?
- 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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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)

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

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

Invariant Contracts

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

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

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

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

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

Loops of Proofs: Iterations

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

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

Loops of Proofs: Iterations

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

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

Loops of Proofs: Iterations

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

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

Loops of Proofs: Iterations & Splitting the Box

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

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

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

Loops of Proofs: Iterations & Splitting the Box

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

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

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

Loops of Proofs: Iterations & Splitting the Box

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

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

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

Loops of Proofs: Iterations & Splitting the Box

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

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

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

Loops of Proofs: Iterations & Splitting the Box

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

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

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

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

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

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

Loops of Proofs: Iterations & Generalizations

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

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

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

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

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

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

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

Loops of Proofs: Iterations & Generalizations

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

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

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

Loops of Proofs: Iterations & Generalizations

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

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

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

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

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

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

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

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

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

$$\text{MR}\ \frac{J_2 \vdash [\alpha][\alpha^*]B}{}$$

$$\wedge\text{R}\ \frac{J_2 \vdash B \qquad J_2 \vdash [\alpha][\alpha^*]B}{J_2 \vdash B \wedge [\alpha][\alpha^*]B}$$

$$\text{MR}\ \frac{J_1 \vdash [\alpha]J_2 \qquad J_2 \vdash B \wedge [\alpha][\alpha^*]B}{J_1 \vdash [\alpha](B \wedge [\alpha][\alpha^*]B)}$$

$$\wedge\text{R}\ \frac{J_1 \vdash B \qquad J_1 \vdash [\alpha](B \wedge [\alpha][\alpha^*]B)}{J_1 \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)}$$

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

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

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

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

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

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

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

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

Loops of Proofs: Common Generalizations

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

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

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

Loops of Proofs: Extracting a Proof Rule

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

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

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

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

Loops of Proofs: Extracting a Proof Rule

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

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

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

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

Loops of Proofs: Extracting a Proof Rule

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

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

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

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

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

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

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.