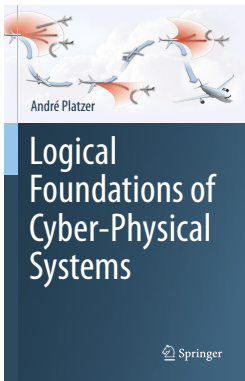
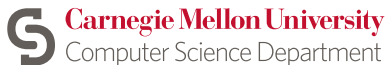


# 07: Control Loops & Invariants

## Logical Foundations of Cyber-Physical Systems



André Platzer





- 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



## 1 Learning Objectives

## 2 Induction for Loops

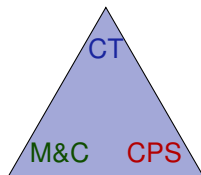
- Iteration Axiom
- Induction Axiom
- Induction Rule for Loops
- Loop Invariants
- Simple Example
- Contextual Soundness Requirements

## 3 Operationalize Invariant Construction

- Bouncing Ball
- Rescuing Misplaced Constants
- Safe Quantum

## 4 Summary

- 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



## 1 Learning Objectives

## 2 Induction for Loops

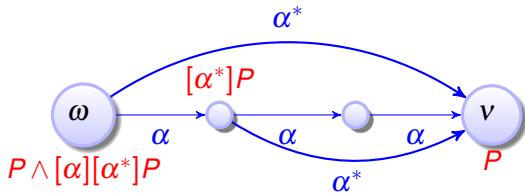
- Iteration Axiom
- Induction Axiom
- Induction Rule for Loops
- Loop Invariants
- Simple Example
- Contextual Soundness Requirements

## 3 Operationalize Invariant Construction

- Bouncing Ball
- Rescuing Misplaced Constants
- Safe Quantum

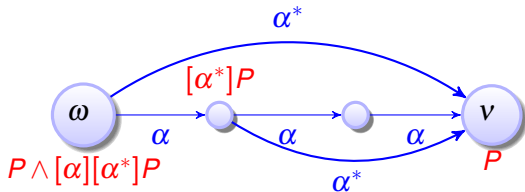
## 4 Summary

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





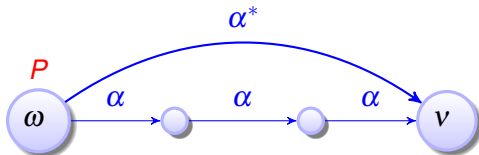
$$[*] [\alpha^*]P \leftrightarrow P \wedge [\alpha][\alpha^*]P$$



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

Lemma ( )

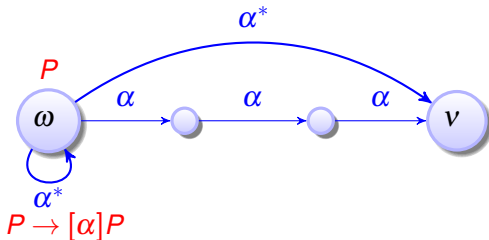
$$\vdash [\alpha^*]P \leftrightarrow P \wedge$$





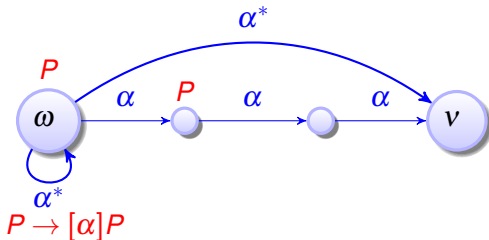
Lemma ( )

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



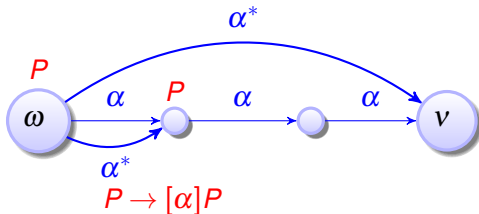
Lemma ( )

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



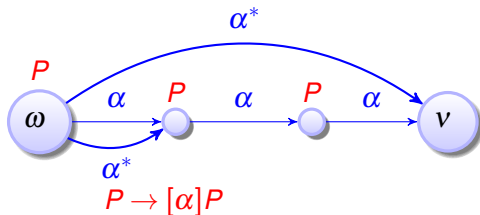
## Lemma (I is sound)

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



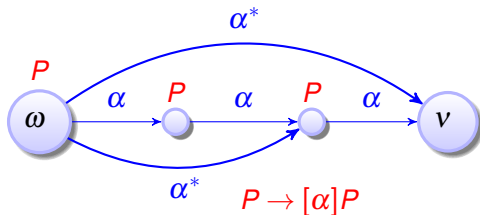
## Lemma (I is sound)

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



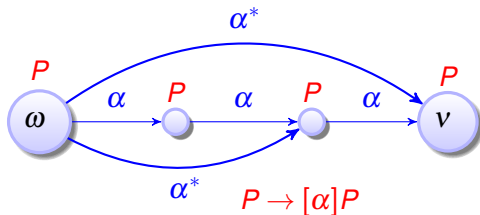
## Lemma (I is sound)

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



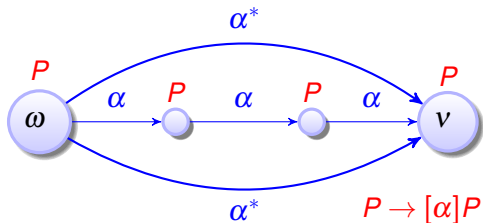
Lemma (I is sound)

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



Lemma (I is sound)

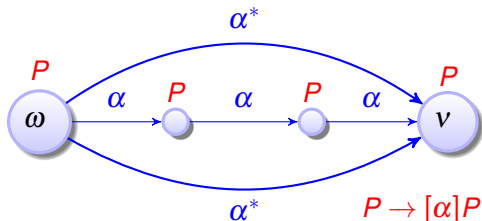
$$\vdash [\alpha^*]P \leftrightarrow P \wedge [\alpha^*](P \rightarrow [\alpha]P)$$





Lemma (I is sound)

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



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



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

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

Lemma (Loop induction rule *ind* is sound)

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

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

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

Lemma (Loop induction rule ind is sound)

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

Proof (Derived rule).

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

□

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

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

Lemma (Loop induction rule ind is sound)

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

Proof (Derived rule).

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

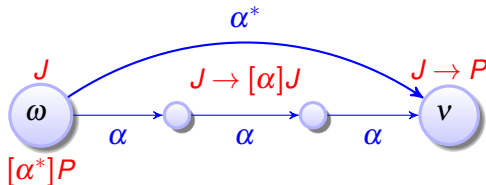
Problem: Rule ind is no equivalence. Its use of G may lose information:  $[\alpha^*](P \rightarrow [\alpha]P)$  true but  $P \vdash [\alpha]P$  is not valid. □

Generalize postcondition to strong loop invariant  $J$  by

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

Lemma (Loop invariant rule loop is sound)

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



Generalize postcondition to strong loop invariant  $J$  by

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

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).

$$\text{cut} \frac{\begin{array}{c} \text{ind} \frac{J \vdash [\alpha]J}{J \vdash [\alpha^*]J} \\ \rightarrow R \frac{J \vdash [\alpha^*]J}{\Gamma \vdash J \rightarrow [\alpha^*]J, \Delta} \end{array} \quad \begin{array}{c} \frac{J \vdash P}{M[\cdot] \frac{J \vdash P}{[\alpha^*]J \vdash [\alpha^*]P}} \\ \rightarrow L \frac{\Gamma \vdash J, \Delta \quad M[\cdot] \frac{J \vdash P}{[\alpha^*]J \vdash [\alpha^*]P}}{\Gamma, J \rightarrow [\alpha^*]J \vdash [\alpha^*]P, \Delta} \end{array}}{\Gamma \vdash [\alpha^*]P, \Delta}$$

□

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

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).

$$\text{cut} \frac{\begin{array}{c} \text{ind} \frac{J \vdash [\alpha]J}{J \vdash [\alpha^*]J} \\ \rightarrow R \frac{J \vdash [\alpha^*]J}{\Gamma \vdash J \rightarrow [\alpha^*]J, \Delta} \end{array} \quad \begin{array}{c} \frac{J \vdash P}{M[\cdot] \frac{J \vdash P}{[\alpha^*]J \vdash [\alpha^*]P}} \\ \rightarrow L \frac{\Gamma \vdash J, \Delta \quad M[\cdot] \frac{J \vdash P}{[\alpha^*]J \vdash [\alpha^*]P}}{\Gamma, J \rightarrow [\alpha^*]J \vdash [\alpha^*]P, \Delta} \end{array}}{\Gamma \vdash [\alpha^*]P, \Delta}$$

Problem: Finding invariant  $J$  can be a challenge.

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



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

$$\begin{array}{c} \text{loop} \frac{x \geq 8 \wedge 5 \geq y \wedge y \geq 0 \vdash J \quad J \vdash [x := x + y; y := x - 2 \cdot y]J \quad J \vdash x \geq 0}{x \geq 8 \wedge 5 \geq y \wedge y \geq 0 \vdash [(x := x + y; y := x - 2 \cdot y)^*]x \geq 0} \\ \rightarrow R \frac{}{\vdash x \geq 8 \wedge 5 \geq y \wedge y \geq 0 \rightarrow [(x := x + y; y := x - 2 \cdot y)^*]x \geq 0} \end{array}$$

①  $J \equiv x \geq 0$

# A Simple Discrete Loop Example

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

$$\begin{array}{c} \text{loop} \frac{x \geq 8 \wedge 5 \geq y \wedge y \geq 0 \vdash J \quad J \vdash [x := x + y; y := x - 2 \cdot y]J \quad J \vdash x \geq 0}{x \geq 8 \wedge 5 \geq y \wedge y \geq 0 \vdash [(x := x + y; y := x - 2 \cdot y)^*]x \geq 0} \\ \rightarrow R \frac{}{\vdash x \geq 8 \wedge 5 \geq y \wedge y \geq 0 \rightarrow [(x := x + y; y := x - 2 \cdot y)^*]x \geq 0} \end{array}$$

①  $J \equiv x \geq 0$

stronger: Lacks info about  $y$





# A Simple Discrete Loop Example

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

$$\begin{array}{c} \text{loop} \frac{x \geq 8 \wedge 5 \geq y \wedge y \geq 0 \vdash J \quad J \vdash [x := x + y; y := x - 2 \cdot y]J \quad J \vdash x \geq 0}{x \geq 8 \wedge 5 \geq y \wedge y \geq 0 \vdash [(x := x + y; y := x - 2 \cdot y)^*]x \geq 0} \\ \rightarrow R \frac{}{\vdash x \geq 8 \wedge 5 \geq y \wedge y \geq 0 \rightarrow [(x := x + y; y := x - 2 \cdot y)^*]x \geq 0} \end{array}$$

①  $J \equiv x \geq 0$

stronger: Lacks info about  $y$

②  $J \equiv x \geq 8 \wedge 5 \geq y \wedge y \geq 0$



# A Simple Discrete Loop Example

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

$$\begin{array}{c} \text{loop} \frac{x \geq 8 \wedge 5 \geq y \wedge y \geq 0 \vdash J \quad J \vdash [x := x + y; y := x - 2 \cdot y]J \quad J \vdash x \geq 0}{x \geq 8 \wedge 5 \geq y \wedge y \geq 0 \vdash [(x := x + y; y := x - 2 \cdot y)^*]x \geq 0} \\ \rightarrow R \frac{}{\vdash x \geq 8 \wedge 5 \geq y \wedge y \geq 0 \rightarrow [(x := x + y; y := x - 2 \cdot y)^*]x \geq 0} \end{array}$$

①  $J \equiv x \geq 0$

stronger: Lacks info about  $y$

②  $J \equiv x \geq 8 \wedge 5 \geq y \wedge y \geq 0$

weaker: Changes immediately



# A Simple Discrete Loop Example

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

$$\begin{array}{c} \text{loop} \frac{x \geq 8 \wedge 5 \geq y \wedge y \geq 0 \vdash J \quad J \vdash [x := x + y; y := x - 2 \cdot y]J \quad J \vdash x \geq 0}{x \geq 8 \wedge 5 \geq y \wedge y \geq 0 \vdash [(x := x + y; y := x - 2 \cdot y)^*]x \geq 0} \\ \rightarrow R \frac{}{\vdash x \geq 8 \wedge 5 \geq y \wedge y \geq 0 \rightarrow [(x := x + y; y := x - 2 \cdot y)^*]x \geq 0} \end{array}$$

①  $J \equiv x \geq 0$

stronger: Lacks info about  $y$

②  $J \equiv x \geq 8 \wedge 5 \geq y \wedge y \geq 0$

weaker: Changes immediately

③  $J \equiv x \geq 0 \wedge y \geq 0$



# A Simple Discrete Loop Example

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

$$\begin{array}{c} \text{loop} \frac{x \geq 8 \wedge 5 \geq y \wedge y \geq 0 \vdash J \quad J \vdash [x := x + y; y := x - 2 \cdot y]J \quad J \vdash x \geq 0}{x \geq 8 \wedge 5 \geq y \wedge y \geq 0 \vdash [(x := x + y; y := x - 2 \cdot y)^*]x \geq 0} \\ \rightarrow R \frac{}{\vdash x \geq 8 \wedge 5 \geq y \wedge y \geq 0 \rightarrow [(x := x + y; y := x - 2 \cdot y)^*]x \geq 0} \end{array}$$

①  $J \equiv x \geq 0$

stronger: Lacks info about  $y$

②  $J \equiv x \geq 8 \wedge 5 \geq y \wedge y \geq 0$

weaker: Changes immediately

③  $J \equiv x \geq 0 \wedge y \geq 0$

no:  $y$  may become negative if  $x < 0$



# A Simple Discrete Loop Example

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

$$\begin{array}{c} \text{loop} \frac{x \geq 8 \wedge 5 \geq y \wedge y \geq 0 \vdash J \quad J \vdash [x := x + y; y := x - 2 \cdot y]J \quad J \vdash x \geq 0}{x \geq 8 \wedge 5 \geq y \wedge y \geq 0 \vdash [(x := x + y; y := x - 2 \cdot y)^*]x \geq 0} \\ \rightarrow R \frac{}{\vdash x \geq 8 \wedge 5 \geq y \wedge y \geq 0 \rightarrow [(x := x + y; y := x - 2 \cdot y)^*]x \geq 0} \end{array}$$

①  $J \equiv x \geq 0$

stronger: Lacks info about  $y$

②  $J \equiv x \geq 8 \wedge 5 \geq y \wedge y \geq 0$

weaker: Changes immediately

③  $J \equiv x \geq 0 \wedge y \geq 0$

no:  $y$  may become negative if  $x < y$

④  $J \equiv x \geq y \wedge y \geq 0$



# A Simple Discrete Loop Example

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

$$\begin{array}{c} \text{loop} \frac{x \geq 8 \wedge 5 \geq y \wedge y \geq 0 \vdash J \quad J \vdash [x := x + y; y := x - 2 \cdot y]J \quad J \vdash x \geq 0}{x \geq 8 \wedge 5 \geq y \wedge y \geq 0 \vdash [(x := x + y; y := x - 2 \cdot y)^*]x \geq 0} \\ \rightarrow R \frac{}{\vdash x \geq 8 \wedge 5 \geq y \wedge y \geq 0 \rightarrow [(x := x + y; y := x - 2 \cdot y)^*]x \geq 0} \end{array}$$

①  $J \equiv x \geq 0$

stronger: Lacks info about  $y$

②  $J \equiv x \geq 8 \wedge 5 \geq y \wedge y \geq 0$

weaker: Changes immediately

③  $J \equiv x \geq 0 \wedge y \geq 0$

no:  $y$  may become negative if  $x < y$

④  $J \equiv x \geq y \wedge y \geq 0$

correct loop invariant



# Forgot to Add Sequent Context $\Gamma, \Delta$ 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 $\Gamma, \Delta$ to Premises

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

$$\begin{array}{l} x = 0 \vdash x \leq 1 \quad x = 0, x \leq 1 \vdash [x := x + 1]x \leq 1 \quad x \leq 1 \vdash x \leq 1 \\ \hline x = 0, x \leq 1 \vdash [(x := x + 1)^*]x \leq 1 \end{array}$$





# Forgot to Add Sequent Context $\Gamma, \Delta$ to Premises

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

$$\begin{array}{l} \text{⚡} \\ \frac{x = 0 \vdash x \leq 1 \quad x = 0, x \leq 1 \vdash [x := x + 1]x \leq 1 \quad x \leq 1 \vdash x \leq 1}{x = 0, x \leq 1 \vdash [(x := x + 1)^*]x \leq 1} \end{array}$$

$$\begin{array}{l} \text{⚡} \\ \frac{x = 0 \vdash x \geq 0 \quad x \geq 0 \vdash [x := x + 1]x \geq 0 \quad x = 0, x \geq 0 \vdash x = 0}{x = 0 \vdash [(x := x + 1)^*]x = 0} \end{array}$$



# Forgot to Add Sequent Context $\Gamma, \Delta$ to Premises

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

$$\begin{array}{l} \downarrow \\ \frac{x = 0 \vdash x \leq 1 \quad x = 0, x \leq 1 \vdash [x := x + 1]x \leq 1 \quad x \leq 1 \vdash x \leq 1}{x = 0, x \leq 1 \vdash [(x := x + 1)^*]x \leq 1} \end{array}$$

$$\begin{array}{l} \downarrow \\ \frac{x = 0 \vdash x \geq 0 \quad x \geq 0 \vdash [x := x + 1]x \geq 0 \quad x = 0, x \geq 0 \vdash x = 0}{x = 0 \vdash [(x := x + 1)^*]x = 0} \end{array}$$

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



- 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



---

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

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

$$B_{(x,v)} \equiv 0 \leq x \wedge x \leq H$$

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



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

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

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

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



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

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

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

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



$$\begin{array}{c}
 \frac{}{j(x,v) \vdash [\text{grav}][?x=0; v:=-cv \cup ?x \neq 0]j(x,v)} \\
 \frac{}{j(x,v) \vdash [\text{grav}; (?x=0; v:=-cv \cup ?x \neq 0)]j(x,v)} \\
 \frac{A \vdash j(x,v) \quad \frac{j(x,v) \vdash [\text{grav}; (?x=0; v:=-cv \cup ?x \neq 0)]j(x,v) \quad j(x,v) \vdash B(x,v)}{j(x,v) \vdash [\text{grav}; (?x=0; v:=-cv \cup ?x \neq 0)]j(x,v)}}{A \vdash [(\text{grav}; (?x=0; v:=-cv \cup ?x \neq 0))^*]B(x,v)} \\
 \text{loop}
 \end{array}$$

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

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

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

$$\begin{array}{c}
 \text{MR} \frac{j(x,v) \vdash [\text{grav}]j(x,v)}{j(x,v) \vdash [?x=0; v:=-cv \cup ?x \neq 0]j(x,v)} \\
 \text{[;]} \frac{j(x,v) \vdash [\text{grav}][?x=0; v:=-cv \cup ?x \neq 0]j(x,v)}{j(x,v) \vdash [\text{grav}; (?x=0; v:=-cv \cup ?x \neq 0)]j(x,v)} \\
 \text{loop} \frac{A \vdash j(x,v) \quad \frac{j(x,v) \vdash [\text{grav}; (?x=0; v:=-cv \cup ?x \neq 0)]j(x,v)}{j(x,v) \vdash [\text{grav}; (?x=0; v:=-cv \cup ?x \neq 0)]j(x,v)} \quad j(x,v) \vdash B(x,v)}{A \vdash [(\text{grav}; (?x=0; v:=-cv \cup ?x \neq 0))^*]B(x,v)}
 \end{array}$$

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

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

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





$$\begin{array}{c}
 \text{MR} \frac{j(x,v) \vdash [\text{grav}]j(x,v) \quad [\cup] \frac{j(x,v) \vdash [?x=0; v:=-cv]j(x,v) \wedge [?x \neq 0]j(x,v)}{j(x,v) \vdash [?x=0; v:=-cv \cup ?x \neq 0]j(x,v)}}{j(x,v) \vdash [\text{grav}][?x=0; v:=-cv \cup ?x \neq 0]j(x,v)} \\
 \text{[;]} \frac{j(x,v) \vdash [\text{grav}][?x=0; v:=-cv \cup ?x \neq 0]j(x,v)}{j(x,v) \vdash [\text{grav}; (?x=0; v:=-cv \cup ?x \neq 0)]j(x,v)} \\
 \text{loop} \frac{A \vdash j(x,v) \quad \frac{j(x,v) \vdash [\text{grav}; (?x=0; v:=-cv \cup ?x \neq 0)]j(x,v)}{j(x,v) \vdash [\text{grav}; (?x=0; v:=-cv \cup ?x \neq 0)]j(x,v)} \quad j(x,v) \vdash B(x,v)}{A \vdash [(\text{grav}; (?x=0; v:=-cv \cup ?x \neq 0))^*]B(x,v)}
 \end{array}$$

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

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

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



$$\begin{array}{c}
 \text{MR} \frac{j(x,v) \vdash [\text{grav}]j(x,v) \quad \text{[}\cup\text{]} \frac{\text{[}\wedge\text{]} \frac{j(x,v) \vdash [?x=0; v:=-cv]j(x,v) \quad j(x,v) \vdash [?x \neq 0]j(x,v)}{j(x,v) \vdash [?x=0; v:=-cv]j(x,v) \wedge [?x \neq 0]j(x,v)}}{j(x,v) \vdash [?x=0; v:=-cv \cup ?x \neq 0]j(x,v)}}{j(x,v) \vdash [\text{grav}][?x=0; v:=-cv \cup ?x \neq 0]j(x,v)} \\
 \text{[;]} \frac{A \vdash j(x,v) \quad \frac{j(x,v) \vdash [\text{grav}; (?x=0; v:=-cv \cup ?x \neq 0)]j(x,v)}{j(x,v) \vdash [\text{grav}; (?x=0; v:=-cv \cup ?x \neq 0)]j(x,v)} \quad j(x,v) \vdash B(x,v)}{A \vdash ([\text{grav}; (?x=0; v:=-cv \cup ?x \neq 0)]^*)B(x,v)} \\
 \text{loop}
 \end{array}$$

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

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

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

$$\begin{array}{c}
 \text{MR} \frac{\text{AR} \frac{[\cdot] \frac{j(x,v) \vdash [\text{?}x=0][v:=-cv]j(x,v)}{j(x,v) \vdash [\text{?}x=0; v:=-cv]j(x,v)} \quad j(x,v) \vdash [\text{?}x \neq 0]j(x,v)}{j(x,v) \vdash [\text{?}x=0; v:=-cv]j(x,v) \wedge [\text{?}x \neq 0]j(x,v)}}{j(x,v) \vdash [\text{?}x=0; v:=-cv \cup \text{?}x \neq 0]j(x,v)}}{j(x,v) \vdash [\text{grav}][\text{?}x=0; v:=-cv \cup \text{?}x \neq 0]j(x,v)} \\
 \text{loop} \frac{A \vdash j(x,v) \quad \frac{j(x,v) \vdash [\text{grav}; (\text{?}x=0; v:=-cv \cup \text{?}x \neq 0)]j(x,v)}{j(x,v) \vdash [\text{grav}; (\text{?}x=0; v:=-cv \cup \text{?}x \neq 0)]j(x,v)} \quad j(x,v) \vdash B(x,v)}{A \vdash ([\text{grav}; (\text{?}x=0; v:=-cv \cup \text{?}x \neq 0)]^*)B(x,v)}
 \end{array}$$

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

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

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

$$\begin{array}{c}
\frac{\frac{\frac{[?], \rightarrow R \quad \overline{j(x,v), x=0 \vdash [v := -cv]j(x,v)}}{[?], \rightarrow R} \quad \frac{[?], \rightarrow R \quad \overline{j(x,v) \vdash [?x=0][v := -cv]j(x,v)}}{[?], \rightarrow R}}{[?], \rightarrow R} \quad \frac{[?], \rightarrow R \quad \overline{j(x,v) \vdash [?x \neq 0]j(x,v)}}{[?], \rightarrow R}}{[?], \rightarrow R} \\
\frac{\frac{\frac{j(x,v) \vdash [grav]j(x,v)}{[?], \rightarrow R} \quad \frac{[?], \rightarrow R \quad \overline{j(x,v) \vdash [?x=0; v := -cv]j(x,v) \wedge [?x \neq 0]j(x,v)}}{[?], \rightarrow R}}{[?], \rightarrow R}}{[?], \rightarrow R} \quad \frac{[?], \rightarrow R \quad \overline{j(x,v) \vdash [?x=0; v := -cv \cup ?x \neq 0]j(x,v)}}{[?], \rightarrow R}}{[?], \rightarrow R} \\
\frac{\frac{\frac{j(x,v) \vdash [grav][?x=0; v := -cv \cup ?x \neq 0]j(x,v)}{[?], \rightarrow R} \quad \frac{[?], \rightarrow R \quad \overline{j(x,v) \vdash [grav; (?x=0; v := -cv \cup ?x \neq 0)]j(x,v)}}{[?], \rightarrow R}}{[?], \rightarrow R} \quad \frac{[?], \rightarrow R \quad \overline{j(x,v) \vdash B(x,v)}}{[?], \rightarrow R}}{[?], \rightarrow R} \\
\frac{\frac{A \vdash j(x,v)}{[?], \rightarrow R} \quad \frac{[?], \rightarrow R \quad \overline{j(x,v) \vdash [grav; (?x=0; v := -cv \cup ?x \neq 0)]j(x,v)}}{[?], \rightarrow R} \quad \frac{[?], \rightarrow R \quad \overline{j(x,v) \vdash B(x,v)}}{[?], \rightarrow R}}{[?], \rightarrow R} \\
\text{loop} \quad \frac{\frac{A \vdash j(x,v)}{[?], \rightarrow R} \quad \frac{[?], \rightarrow R \quad \overline{j(x,v) \vdash [grav; (?x=0; v := -cv \cup ?x \neq 0)]j(x,v)}}{[?], \rightarrow R} \quad \frac{[?], \rightarrow R \quad \overline{j(x,v) \vdash B(x,v)}}{[?], \rightarrow R}}{[?], \rightarrow R} \\
A \vdash [(grav; (?x=0; v := -cv \cup ?x \neq 0))^*]B(x,v)
\end{array}$$

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

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

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

$$\begin{array}{c}
\text{MR} \frac{
\begin{array}{c}
\text{[:=]} \frac{j(x,v), x=0 \vdash j(x,-cv)}{j(x,v), x=0 \vdash [v:=-cv]j(x,v)} \\
\text{[?],} \rightarrow R \frac{j(x,v) \vdash [?x=0][v:=-cv]j(x,v)}{j(x,v) \vdash [?x=0; v:=-cv]j(x,v)} \\
\text{[;]} \frac{j(x,v) \vdash [?x=0; v:=-cv]j(x,v) \quad j(x,v) \vdash [?x \neq 0]j(x,v)}{j(x,v) \vdash [?x=0; v:=-cv]j(x,v) \wedge [?x \neq 0]j(x,v)} \\
\wedge R \frac{j(x,v) \vdash [?x=0; v:=-cv]j(x,v) \wedge [?x \neq 0]j(x,v)}{j(x,v) \vdash [?x=0; v:=-cv \cup ?x \neq 0]j(x,v)} \\
\text{[}\cup\text{]} \frac{j(x,v) \vdash [grav]j(x,v) \quad j(x,v) \vdash [?x=0; v:=-cv \cup ?x \neq 0]j(x,v)}{j(x,v) \vdash [grav][?x=0; v:=-cv \cup ?x \neq 0]j(x,v)} \\
\text{[;]} \frac{j(x,v) \vdash [grav; (?x=0; v:=-cv \cup ?x \neq 0)]j(x,v)}{j(x,v) \vdash [grav; (?x=0; v:=-cv \cup ?x \neq 0)]j(x,v)} \\
A \vdash j(x,v) \quad j(x,v) \vdash B(x,v) \\
\text{loop} \frac{A \vdash j(x,v) \quad j(x,v) \vdash [grav; (?x=0; v:=-cv \cup ?x \neq 0)]j(x,v) \quad j(x,v) \vdash B(x,v)}{A \vdash [(grav; (?x=0; v:=-cv \cup ?x \neq 0))^*]B(x,v)}
\end{array}
}{A \vdash [(grav; (?x=0; v:=-cv \cup ?x \neq 0))^*]B(x,v)}
\end{array}$$

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

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

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







# Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

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

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

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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

weak: fails ODE if  $v \gg 0$

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

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

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

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

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

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

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

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

$$\textcircled{1} \quad j(x, v) \equiv x \geq 0$$

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

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 Acrophobic Bouncing Ball

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

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

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

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

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

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

weaker: fails postcondition if  $x > H$

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

weak: fails ODE if  $v \gg 0$

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

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

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

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

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

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

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

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

$$\textcircled{1} \quad \mathbf{j}(x, v) \equiv x \geq 0$$

weaker: fails postcondition if  $x > H$

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

weak: fails ODE if  $v \gg 0$

$$\textcircled{3} \quad \mathbf{j}(x, v) \equiv x = 0 \wedge v = 0$$

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

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

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

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

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

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

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

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

$$\textcircled{1} \quad j(x, v) \equiv x \geq 0$$

weaker: fails postcondition if  $x > H$

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

weak: fails ODE if  $v \gg 0$

$$\textcircled{3} \quad j(x, v) \equiv x = 0 \wedge v = 0$$

strong: fails initial condition if  $x > 0$

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

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

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

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

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

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

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

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

$$\textcircled{1} \quad j(x, v) \equiv x \geq 0$$

weaker: fails postcondition if  $x > H$

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

weak: fails ODE if  $v \gg 0$

$$\textcircled{3} \quad j(x, v) \equiv x = 0 \wedge v = 0$$

strong: fails initial condition if  $x > 0$

$$\textcircled{4} \quad j(x, v) \equiv x = 0 \vee x = H \wedge v = 0$$

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

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

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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$\textcircled{1} j(x, v) \equiv x \geq 0$$

weaker: fails postcondition if  $x > H$

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

weak: fails ODE if  $v \gg 0$

$$\textcircled{3} j(x, v) \equiv x = 0 \wedge v = 0$$

strong: fails initial condition if  $x > 0$

$$\textcircled{4} j(x, v) \equiv x = 0 \vee x = H \wedge v = 0$$

no space for intermediate states

$$\textcircled{5} j(x, v) \equiv 2gx = 2gH - v^2 \wedge x \geq 0$$

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

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

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

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

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

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

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

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

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

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

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

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



# Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

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

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

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

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

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

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

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



# Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

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



# Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

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



# Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

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





# Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

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



# Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

①  $j(x, v) \equiv x \geq 0$  weaker: fails postcondition if  $x > H$

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

③  $j(x, v) \equiv x = 0 \wedge v = 0$  strong: fails initial condition if  $x > 0$

④  $j(x, v) \equiv x = 0 \vee x = H \wedge v = 0$  no space for intermediate states

⑤  $j(x, v) \equiv 2gx = 2gH - v^2 \wedge x \geq 0$  works: implicitly links  $v$  and  $x$



# Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

①  $j(x, v) \equiv x \geq 0$

weaker: fails postcondition if  $x > H$

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

weak: fails ODE if  $v \gg 0$

③  $j(x, v) \equiv x = 0 \wedge v = 0$

strong: fails initial condition if  $x > 0$

④  $j(x, v) \equiv x = 0 \vee x = H \wedge v = 0$

no space for intermediate states

⑤  $j(x, v) \equiv 2gx = 2gH - v^2 \wedge x \geq 0$

works: implicitly links  $v$  and  $x$



# Proving Quantum the Acrophobic Bouncing Ball

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

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



# Proving Quantum the Acrophobic Bouncing Ball

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

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

# A Proving Quantum the Acrophobic Bouncing Ball

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

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



[']

---

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



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





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



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



# Proving Quantum the Acrophobic Bouncing Ball

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



# Proving Quantum the Acrophobic Bouncing Ball

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



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

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

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

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

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

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

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

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



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

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

- Is Quantum done with his safety proof?

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

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

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

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

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

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

2  $p \equiv c=1 \wedge g > 0$

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

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



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

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

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

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

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





# Clumsy Quantum Misplaced the Constants

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

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

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

- 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

$$\Box \wedge [\alpha](P \wedge Q) \leftrightarrow [\alpha]P \wedge [\alpha]Q \qquad \forall p \rightarrow [\alpha]p \quad (FV(p) \cap BV(\alpha) = \emptyset)$$

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

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

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

## Proposition (Quantum can bounce around safely)

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

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

**requires** $(0 \leq x \wedge x = H \wedge v = 0)$

**requires** $(g > 0 \wedge 1 = c)$

**ensures** $(0 \leq x \wedge x \leq H)$

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

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

**Invariant Contracts**

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



- 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

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

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

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

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

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

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

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



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



compositional semantics  $\Rightarrow$  compositional rules!



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

---

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

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

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

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

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

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

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



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

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

$$\begin{array}{l}
 \hline
 A \vdash B \wedge [\alpha]B \wedge [\alpha][\alpha](B \wedge [\alpha][\alpha^*]B) \\
 \hline
 [] \wedge \frac{A \vdash B \wedge [\alpha](B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B))}{A \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)} \\
 \hline
 [*] \frac{A \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)}{A \vdash B \wedge [\alpha][\alpha^*]B} \\
 \hline
 [*] \frac{A \vdash B \wedge [\alpha][\alpha^*]B}{A \vdash [\alpha^*]B} \\
 \hline
 \end{array}$$



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

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

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



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

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

$$\begin{array}{c}
 \hline
 A \vdash B \wedge [\alpha]B \wedge [\alpha][\alpha]B \wedge [\alpha][\alpha][\alpha][\alpha^*]B \\
 \hline
 [] \wedge \frac{}{A \vdash B \wedge [\alpha]B \wedge [\alpha]([\alpha]B \wedge [\alpha][\alpha][\alpha^*]B)} \\
 \hline
 [] \wedge \frac{}{A \vdash B \wedge [\alpha]B \wedge [\alpha][\alpha](B \wedge [\alpha][\alpha^*]B)} \\
 \hline
 [] \wedge \frac{}{A \vdash B \wedge [\alpha](B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B))} \\
 \hline
 [*] \frac{}{A \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)} \\
 \hline
 [*] \frac{}{A \vdash B \wedge [\alpha][\alpha^*]B} \\
 \hline
 [*] \frac{}{A \vdash [\alpha^*]B}
 \end{array}$$



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

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

$$\begin{array}{l}
 \wedge R \frac{A \vdash B \quad A \vdash [\alpha]B \quad A \vdash [\alpha][\alpha]B \quad A \vdash [\alpha][\alpha][\alpha][\alpha^*]B}{A \vdash B \wedge [\alpha]B \wedge [\alpha][\alpha]B \wedge [\alpha][\alpha][\alpha][\alpha^*]B} \\
 [] \wedge \frac{A \vdash B \wedge [\alpha]B \wedge [\alpha][\alpha]B \wedge [\alpha][\alpha][\alpha][\alpha^*]B}{A \vdash B \wedge [\alpha]B \wedge [\alpha]([\alpha]B \wedge [\alpha][\alpha][\alpha^*]B)} \\
 [] \wedge \frac{A \vdash B \wedge [\alpha]B \wedge [\alpha][\alpha](B \wedge [\alpha][\alpha^*]B)}{A \vdash B \wedge [\alpha](B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B))} \\
 [] \wedge \frac{A \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)}{A \vdash B \wedge [\alpha][\alpha^*]B} \\
 [*] \frac{A \vdash B \wedge [\alpha][\alpha^*]B}{A \vdash [\alpha^*]B}
 \end{array}$$



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

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

$$\begin{array}{c}
 \frac{A \vdash B \quad A \vdash [\alpha]B \quad A \vdash [\alpha][\alpha]B \quad A \vdash [\alpha][\alpha][\alpha][\alpha^*]B}{\wedge R} \\
 \frac{A \vdash B \wedge [\alpha]B \wedge [\alpha][\alpha]B \wedge [\alpha][\alpha][\alpha][\alpha^*]B}{[] \wedge} \\
 \frac{A \vdash B \wedge [\alpha]B \wedge [\alpha]([\alpha]B \wedge [\alpha][\alpha][\alpha^*]B)}{[] \wedge} \\
 \frac{A \vdash B \wedge [\alpha]B \wedge [\alpha][\alpha](B \wedge [\alpha][\alpha^*]B)}{[] \wedge} \\
 \frac{A \vdash B \wedge [\alpha](B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B))}{[*]} \\
 \frac{A \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)}{[*]} \\
 \frac{A \vdash B \wedge [\alpha][\alpha^*]B}{[*]} \\
 \frac{A \vdash [\alpha^*]B}{[*]}
 \end{array}$$

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

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

$$\begin{array}{c}
 \hline
 A \vdash B \wedge [\alpha](B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)) \\
 \hline
 [*] \frac{}{A \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)} \\
 \hline
 [*] \frac{}{A \vdash B \wedge [\alpha][\alpha^*]B} \\
 \hline
 [*] \frac{}{A \vdash [\alpha^*]B}
 \end{array}$$



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

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

$$\begin{array}{c}
 A \vdash B \quad \text{-----} \\
 \wedge\text{R} \quad \frac{A \vdash [\alpha](B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B))}{A \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)} \\
 [*] \quad \text{-----} \\
 [*] \quad \frac{A \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)}{A \vdash B \wedge [\alpha][\alpha^*]B} \\
 [*] \quad \text{-----} \\
 A \vdash [\alpha^*]B
 \end{array}$$

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

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

$$\begin{array}{c}
 A \vdash [\alpha]J_1 \quad \frac{}{J_1 \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)} \\
 A \vdash B_{\text{MR}} \quad \frac{}{A \vdash [\alpha](B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B))} \\
 \wedge R \quad \frac{}{A \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)} \\
 [*] \quad \frac{}{A \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)} \\
 [*] \quad \frac{}{A \vdash B \wedge [\alpha][\alpha^*]B} \\
 [*] \quad \frac{}{A \vdash [\alpha^*]B}
 \end{array}$$

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

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

$$\begin{array}{c}
 J_1 \vdash B \quad \frac{}{J_1 \vdash [\alpha](B \wedge [\alpha][\alpha^*]B)} \\
 A \vdash [\alpha]J_1 \wedge R \frac{}{J_1 \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)} \\
 A \vdash B_{\text{MR}} \frac{}{A \vdash [\alpha](B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B))} \\
 \wedge R \frac{}{A \vdash B \wedge [\alpha](B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B))} \\
 [*] \frac{}{A \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)} \\
 [*] \frac{}{A \vdash B \wedge [\alpha][\alpha^*]B} \\
 [*] \frac{}{A \vdash [\alpha^*]B}
 \end{array}$$



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

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

$$\begin{array}{c}
 \begin{array}{c}
 J_1 \vdash [\alpha]J_2 \\
 \hline
 J_2 \vdash B \wedge [\alpha][\alpha^*]B \\
 \hline
 J_1 \vdash [\alpha](B \wedge [\alpha][\alpha^*]B) \\
 \hline
 J_1 \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B) \\
 \hline
 A \vdash [\alpha]J_1 \wedge R \\
 \hline
 A \vdash B \wedge [\alpha](B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)) \\
 \hline
 \wedge R \\
 \hline
 A \vdash B \wedge [\alpha](B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)) \\
 \hline
 [*] \\
 \hline
 A \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B) \\
 \hline
 [*] \\
 \hline
 A \vdash B \wedge [\alpha][\alpha^*]B \\
 \hline
 [*] \\
 \hline
 A \vdash [\alpha^*]B
 \end{array}
 \end{array}$$





# Loops of Proofs: Iterations & Generalizations

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

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

$$J_2 \vdash B \quad \frac{J_2 \vdash [\alpha]J_3 \quad \dots}{J_2 \vdash [\alpha][\alpha^*]B}$$

$$J_1 \vdash [\alpha]J_2 \quad \wedge\text{R} \frac{J_2 \vdash B \wedge [\alpha][\alpha^*]B}{J_2 \vdash B \wedge [\alpha][\alpha^*]B}$$

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

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

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

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

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

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

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





# Loops of Proofs: Common Generalizations

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

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

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

$$J \vdash [\alpha]J \quad \wedge\text{R} \frac{J \vdash B \quad J \vdash [\alpha][\alpha^*]B}{J \vdash B \wedge [\alpha][\alpha^*]B}$$

$$J \vdash B_{\text{MR}} \frac{J \vdash [\alpha]J \quad \wedge\text{R} \frac{J \vdash B \quad J \vdash [\alpha][\alpha^*]B}{J \vdash B \wedge [\alpha][\alpha^*]B}}{J \vdash [\alpha](B \wedge [\alpha][\alpha^*]B)}$$

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

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

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

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

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

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



# Loops of Proofs: Extracting a Proof Rule

$$\begin{array}{c}
 \frac{}{A \vdash [\alpha^*]B} \quad J \vdash B \quad [*] \quad [\alpha^*]P \leftrightarrow P \wedge [\alpha][\alpha^*]P \\
 \\
 \frac{}{A \vdash [\alpha]J} \quad J \vdash [\alpha]J \quad \wedge R \quad \frac{J \vdash [\alpha]J \quad \dots}{J \vdash [\alpha][\alpha^*]B} \\
 \\
 \frac{A \vdash [\alpha]J \quad J \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)}{A \vdash B} \quad J \vdash B \wedge [\alpha][\alpha^*]B \quad MR \quad \frac{\Gamma \vdash [\alpha]Q, \Delta \quad Q \vdash P}{\Gamma \vdash [\alpha]P, \Delta} \\
 \\
 \frac{A \vdash B \quad J \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)}{A \vdash [\alpha](B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B))} \quad \wedge R \\
 \\
 \frac{A \vdash [\alpha](B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B))}{A \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)} \quad [*] \\
 \\
 \frac{A \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)}{A \vdash B \wedge [\alpha][\alpha^*]B} \quad [*] \\
 \\
 \frac{A \vdash B \wedge [\alpha][\alpha^*]B}{A \vdash [\alpha^*]B} \quad [*]
 \end{array}$$



# Loops of Proofs: Extracting a Proof Rule

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

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

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

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

$$J \vdash B_{\text{MR}} \quad \frac{J \vdash [\alpha]J \quad \wedge\text{R} \quad J \vdash B \wedge [\alpha][\alpha^*]B}{J \vdash B \wedge [\alpha][\alpha^*]B}$$

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

$$A \vdash B_{\text{MR}} \quad \frac{J \vdash B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B)}{A \vdash [\alpha](B \wedge [\alpha](B \wedge [\alpha][\alpha^*]B))}$$

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

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

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

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



# Loops of Proofs: Extracting a Proof Rule

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

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

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

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

$$J \vdash [\alpha]J \quad \wedge R \quad \frac{J \vdash B \quad \text{MR} \quad \frac{J \vdash [\alpha]J \quad \dots}{J \vdash [\alpha][\alpha^*]B}}{J \vdash B \wedge [\alpha][\alpha^*]B}$$

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

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

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

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

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

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

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

# $\mathcal{A}$ Loops of Proofs: Loop Invariants

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

Invariant  $J$  generalized  
intermediate condition

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

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

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

$$J \vdash [\alpha]J \quad \wedge\text{R} \frac{J \vdash B \quad \text{MR} \frac{J \vdash [\alpha][\alpha^*]B}{J \vdash B \wedge [\alpha][\alpha^*]B}}{J \vdash B \wedge [\alpha][\alpha^*]B}$$

$$J \vdash B_{\text{MR}} \frac{J \vdash [\alpha]J \quad \wedge\text{R} \frac{J \vdash B \wedge [\alpha][\alpha^*]B}{J \vdash [\alpha](B \wedge [\alpha][\alpha^*]B)}}{J \vdash [\alpha](B \wedge [\alpha][\alpha^*]B)}$$

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

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

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

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

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

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



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.