05: Dynamical Systems & Dynamic Axioms
15-424: Foundations of Cyber-Physical Systems

André Platzer

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

1. Learning Objectives
2. Approach
3. Reminder: Compositional Semantics
4. Bouncing Ball
5. Dynamic Axioms for Dynamical Systems
6. First Bouncing Ball Proof
Outline

1. Learning Objectives
2. Approach
3. Reminder: Compositional Semantics
4. Bouncing Ball
5. Dynamic Axioms for Dynamical Systems
6. First Bouncing Ball Proof
Learning Objectives
Dynamical Systems & Dynamic Axioms

- Cyber+physics interaction
- Relate discrete+continuous
- Rigorous reasoning about CPS
- dL as verification language
- Align semantics+reasoning operational CPS effects
**Logical Trinity**

**Syntax** defines the notation
What problems are we allowed to write down?

**Semantics** what carries meaning.
What real or mathematical objects does the syntax stand for?

**Axiomatics** internalizes semantic relations into universal syntactic transformations.
How does the semantics of $A$ relate to semantics of $A \land B$, syntactically? If $A$ is true, is $A \land B$ true, too? Conversely?

André Platzer (CMU)
Outline

1. Learning Objectives
2. Approach
3. Reminder: Compositional Semantics
4. Bouncing Ball
5. Dynamic Axioms for Dynamical Systems
6. First Bouncing Ball Proof
Logical guiding principle: Compositionality

1. Every CPS is modeled by a hybrid program (or game . . . )
2. All hybrid programs are combinations of simpler hybrid programs (by a program operator such as \( \cup \) and ; and \( * \))
3. All CPS can be analyzed if only we identify one suitable analysis technique for each operator.
Outline

1. Learning Objectives

2. Approach

3. Reminder: Compositional Semantics

4. Bouncing Ball

5. Dynamic Axioms for Dynamical Systems

6. First Bouncing Ball Proof
### Differential Dynamic Logic $d\mathcal{L}$: Semantics

#### Definition (Hybrid program semantics) \( ([\cdot] : \text{HP} \rightarrow \wp(S \times S)) \)

- \( [x := e] = \{ (\omega, \nu) : \nu = \omega \text{ except } [x] \nu = [e] \omega \} \)
- \( [? Q] = \{ (\omega, \omega) : \omega \in [Q] \} \)
- \( [x' = f(x)] = \{ (\varphi(0), \varphi(r)) : \varphi \models x' = f(x) \text{ for some duration } r \} \)
- \( [\alpha \cup \beta] = [\alpha] \cup [\beta] \)
- \( [\alpha; \beta] = [\alpha] \circ [\beta] \)
- \( [\alpha^*] = \bigcup_{n \in \mathbb{N}} [\alpha^n] \)

#### Definition ($d\mathcal{L}$ semantics) \( ([\cdot] : \text{Fml} \rightarrow \wp(S)) \)

- \( [\theta \geq \eta] = \{ \omega : [\theta] \omega \geq [\eta] \omega \} \)
- \( [\neg \phi] = ([\phi])^C \)
- \( [\phi \land \psi] = [\phi] \cap [\psi] \)
- \( [\langle \alpha \rangle \phi] = [\alpha] \circ [\phi] = \{ \omega : \nu \in [\phi] \text{ for some } \nu : (\omega, \nu) \in [\alpha] \} \)
- \( [[\alpha] \phi] = [\neg \langle \alpha \rangle \neg \phi] = \{ \omega : \nu \in [\phi] \text{ for all } \nu : (\omega, \nu) \in [\alpha] \} \)
- \( [\exists x \phi] = \{ \omega : \omega_x^r \in [\phi] \text{ for some } r \in \mathbb{R} \} \)
Differential Dynamic Logic $d\mathcal{L}$: Transition Semantics

\[\nu \text{ if } \nu(x) = \left[e\right]\omega \text{ and } \nu(z) = \omega(z) \text{ for } z \neq x\]

\[\omega' = f(x) \& Q\]

\[?Q\] if $\omega \in \left[Q\right]$
Differential Dynamic Logic $\mathcal{DL}$: Transition Semantics

\[ \omega \xrightarrow{\alpha} \nu_1 \quad \omega \xrightarrow{\alpha \cup \beta} \nu_2 \]

\[ \omega \quad \alpha ; \beta \quad \mu \quad \beta \quad \nu \]

\[ \omega \xrightarrow{\alpha} \omega_1 \xrightarrow{\alpha} \omega_2 \xrightarrow{\alpha} \nu \]

\[ x \]

\[ t \]

\[ \nu_1 \quad \nu_2 \]

\[ s \]

\[ \nu \]

\[ t \]

André Platzer (CMU)

FCPS / 05: Dynamical Systems & Dynamic Axioms
Differential Dynamic Logic $\mathcal{DL}$: Transition Semantics

\[
\begin{align*}
&\omega 
\xrightarrow{\alpha} \nu_1 \\
&\omega 
\xrightarrow{\beta} \nu_2 \\
&\nu_1 
\xrightarrow{\alpha \cup \beta} \nu_2 \\
&\omega 
\xrightarrow{\alpha} \mu 
\xrightarrow{\beta} \nu \\
&\nu 
\xrightarrow{\alpha ; \beta} \nu \\
&\omega 
\xrightarrow{\alpha} \omega_1 
\xrightarrow{\alpha} \omega_2 
\xrightarrow{\alpha} \nu
\end{align*}
\]
Differential Dynamic Logic \( d\mathcal{L} \): Transition Semantics

\[
\omega \xrightarrow{\alpha} \nu_1 \quad \nu_1 \xrightarrow{\beta} \nu_2 \\
\omega \xrightarrow{\alpha} \mu \xrightarrow{\beta} \nu \\
(\alpha ; \beta)^* \\
\omega \xrightarrow{\alpha} \omega_1 \xrightarrow{\alpha} \omega_2 \xrightarrow{\alpha} \nu
\]
Outline

1. Learning Objectives
2. Approach
3. Reminder: Compositional Semantics
4. Bouncing Ball
5. Dynamic Axioms for Dynamical Systems
6. First Bouncing Ball Proof
Example (Quantum the Bouncing Ball)

\[ 0 \leq x \land x = H \land v = 0 \land g > 0 \land 1 \geq c \geq 0 \rightarrow \]
\[ [(x' = v, v' = -g \land x \geq 0; (?x = 0; v := -cv \cup ?x \neq 0))^*] (0 \leq x \land x \leq H) \]
Conjecture: Quantum the Acrophobic Bouncing Ball

Example (Quantum the Bouncing Ball) (Single-hop)

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

Removing the repetition grotesquely changes the behavior to a single hop
Example (Quantum the Bouncing Ball) (Single-hop)

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

Removing the repetition grotesquely changes the behavior to a single hop
Developed on the board:

1. Intermediate condition proof rule $G[;]$ for sequential compositions
2. Dynamic axioms for dynamical systems
3. Example-driven sketch of single-hop bouncing ball proof

See lecture notes for details [1].
Outline

1. Learning Objectives
2. Approach
3. Reminder: Compositional Semantics
4. Bouncing Ball
5. Dynamic Axioms for Dynamical Systems
6. First Bouncing Ball Proof
compositional semantics ⇒ compositional rules!
\[\bigcup [\alpha \cup \beta]P \leftrightarrow [\alpha]P \land [\beta]P\]
Dynamic Axioms for Dynamical Systems

\[\bigcup\] \[[\alpha \cup \beta]P \leftrightarrow [\alpha]P \land [\beta]P\]

\[\;\] \[[\alpha; \beta]P \leftrightarrow [\alpha][\beta]P\]
Dynamic Axioms for Dynamical Systems

\[ \bigcup [\alpha \cup \beta]P \leftrightarrow [\alpha]P \land [\beta]P \]

\[ ; [\alpha; \beta]P \leftrightarrow [\alpha][\beta]P \]

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

1. Learning Objectives
2. Approach
3. Reminder: Compositional Semantics
4. Bouncing Ball
5. Dynamic Axioms for Dynamical Systems
6. First Bouncing Ball Proof
A Proof of a Short Single-hop Bouncing Ball

\[ \vdash [x'' = -g; (?x = 0; v := -cv \cup ?x \geq 0)] B(x, v) \]

\[ A \overset{\text{def}}{=} 0 \leq x \land x = H \land v = 0 \land g > 0 \land 1 \geq c \geq 0 \]

\[ B(x, v) \overset{\text{def}}{=} 0 \leq x \land x \leq H \]

\[ (x'' = -g) \overset{\text{def}}{=} (x' = v, v' = -g) \]
A Proof of a Short Single-hop Bouncing Ball

\[ A \vdash [x'' = -g][?x = 0; v := -cv \cup ?x \geq 0]B(x,v) \]

\[ A \vdash [x'' = -g; (?x = 0; v := -cv \cup ?x \geq 0)]B(x,v) \]

\[
A \overset{\text{def}}{=} 0 \leq x \land x = H \land v = 0 \land g > 0 \land 1 \geq c \geq 0
\]

\[
B(x,v) \overset{\text{def}}{=} 0 \leq x \land x \leq H
\]

\[
(x'' = -g) \overset{\text{def}}{=} (x' = v, v' = -g)
\]
A Proof of a Short Single-hop Bouncing Ball

\[
\begin{align*}
A &\vdash x'' = -g \left( ?x = 0; v := -cv \right) & B(x,v) \land \left[ ?x \geq 0 \right] B(x,v) \\
A &\vdash [x'' = -g] \left[ ?x = 0; v := -cv \cup ?x \geq 0 \right] B(x,v) \\
A &\vdash [x'' = -g; (?x = 0; v := -cv \cup ?x \geq 0)] B(x,v)
\end{align*}
\]

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

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

\[(x'' = -g) \equiv (x' = v, v' = -g)\]
A Proof of a Short Single-hop Bouncing Ball

\[ A \vdash [x'' = -g]([?x = 0][v := -cv]B(x,v) \land [?x \geq 0]B(x,v)) \]

\[ A \vdash [x'' = -g]([?x = 0; v := -cv]B(x,v) \land [?x \geq 0]B(x,v)) \]

\[ A \vdash [x'' = -g][?x = 0; v := -cv \cup ?x \geq 0]B(x,v) \]

\[ A \vdash [x'' = -g; (?x = 0; v := -cv \cup ?x \geq 0)]B(x,v) \]

\[ A \overset{\text{def}}{=} 0 \leq x \land x = H \land v = 0 \land g > 0 \land 1 \geq c \geq 0 \]

\[ B(x,v) \overset{\text{def}}{=} 0 \leq x \land x \leq H \]

\[ (x'' = -g) \overset{\text{def}}{=} (x' = v, v' = -g) \]
A Proof of a Short Single-hop Bouncing Ball

\[A \vdash [x'' = -g]((x = 0 \rightarrow [v := -cv]B(x,v)) \land (x \geq 0 \rightarrow B(x,v)))\]

\[\vdash [?x = 0][v := -cv]B(x,v) \land [?x \geq 0]B(x,v)\]

\[\vdash [?x = 0; v := -cv]B(x,v) \land [?x \geq 0]B(x,v)\]

\[\vdash [?x = 0; v := -cv \cup ?x \geq 0]B(x,v)\]

\[\vdash [x'' = -g; (?x = 0; v := -cv \cup ?x \geq 0)]B(x,v)\]

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

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

\[(x'' = -g) \equiv (x' = v, v' = -g)\]
A Proof of a Short Single-hop Bouncing Ball

\[ x'' = -g \]
\[ (x = 0 \rightarrow B(x, -cv)) \land (x \geq 0 \rightarrow B(x, v)) \]

\[ A \vdash \]

\[ x'' = -g \]
\[ (x = 0 \rightarrow [v := -cv] B(x, v)) \land (x \geq 0 \rightarrow B(x, v)) \]

\[ A \vdash \]

\[ x'' = -g \]
\[ (?x = 0) [v := -cv] B(x, v) \land (?x \geq 0) B(x, v) \]

\[ A \vdash \]

\[ x'' = -g \]
\[ (?x = 0; v := -cv) B(x, v) \land (?x \geq 0) B(x, v) \]

\[ A \vdash \]

\[ x'' = -g \]
\[ (?x = 0; v := -cv \cup ?x \geq 0) B(x, v) \]

\[ A \vdash \]

\[ [x'' = -g; (?x = 0; v := -cv \cup ?x \geq 0)] B(x, v) \]

\[ A \overset{\text{def}}{=} 0 \leq x \land x = H \land v = 0 \land g > 0 \land 1 \geq c \geq 0 \]

\[ B(x, v) \overset{\text{def}}{=} 0 \leq x \land x \leq H \]

\[ (x'' = -g) \overset{\text{def}}{=} (x' = v, v' = -g) \]
A Proof of a Short Single-hop Bouncing Ball

\[ \forall t \geq 0 \left[ x := H - \frac{g}{2} t^2; v := -gt \right] (x=0 \rightarrow B(x,-cv)) \wedge (x \geq 0 \rightarrow B(x,v)) \]

\[ A \vdash [x'' = -g] (x=0 \rightarrow B(x,-cv)) \wedge (x \geq 0 \rightarrow B(x,v)) \]

\[ A \vdash [x'' = -g] (x=0 \rightarrow [v := -cv] B(x,v)) \wedge (x \geq 0 \rightarrow B(x,v)) \]

\[ A \vdash [x'' = -g] ([?x = 0][v := -cv] B(x,v)) \wedge [?x \geq 0] B(x,v) \]

\[ A \vdash [x'' = -g] ([?x = 0; v := -cv] B(x,v)) \wedge [?x \geq 0] B(x,v) \]

\[ A \vdash [x'' = -g] [?x = 0; v := -cv \cup ?x \geq 0] B(x,v) \]

\[ A \vdash [x'' = -g; (?x = 0; v := -cv \cup ?x \geq 0)] B(x,v) \]

\[ A \overset{\text{def}}{=} 0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0 \]

\[ B(x,v) \overset{\text{def}}{=} 0 \leq x \wedge x \leq H \]

\[ (x'' = -g) \overset{\text{def}}{=} (x' = v, v' = -g) \]
A Proof of a Short Single-hop Bouncing Ball

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

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

\[ A \vdash [x'' = -g] ((x = 0 \rightarrow B(x, -cv)) \land (x \geq 0 \rightarrow B(x, v))) \]

\[ A \vdash [x'' = -g] (x = 0 \rightarrow [v := -cv] B(x, v)) \land (x \geq 0 \rightarrow B(x, v)) \]

\[ A \vdash [x'' = -g] ([?x = 0] [v := -cv] B(x, v) \land [?x \geq 0] B(x, v)) \]

\[ A \vdash [x'' = -g] ([?x = 0; v := -cv] B(x, v) \land [?x \geq 0] B(x, v)) \]

\[ A \vdash [x'' = -g] (?x = 0; v := -cv \cup ?x \geq 0] B(x, v) \]

\[ A \vdash [x'' = -g; (?x = 0; v := -cv \cup ?x \geq 0)] B(x, v) \]

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

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

\[ (x'' = -g) \equiv (x' = v, v' = -g) \]
A Proof of a Short Single-hop Bouncing Ball

\[ \begin{align*}
\vdash & \forall t \geq 0 \left[ x := H - \frac{g}{2} t^2 \right] \left( x = 0 \to B(x, -c(-gt)) \right) \land \left( x \geq 0 \to B(x, -gt) \right) \\
\vdash & \forall t \geq 0 \left[ x := H - \frac{g}{2} t^2 \right] \left[ v := -gt \right] \left( x = 0 \to B(x, -cv) \right) \land \left( x \geq 0 \to B(x, v) \right) \\
\vdash & \forall t \geq 0 \left[ x := H - \frac{g}{2} t^2 ; v := -gt \right] \left( x = 0 \to B(x, -cv) \right) \land \left( x \geq 0 \to B(x, v) \right) \\
\vdash & \left[ x'' = -g \right] \left( x = 0 \to B(x, -cv) \right) \land \left( x \geq 0 \to B(x, v) \right) \\
\vdash & \left[ x'' = -g \right] \left( x = 0 \to \left[ v := -cv \right] B(x, v) \right) \land \left( x \geq 0 \to B(x, v) \right) \\
\vdash & \left[ x'' = -g \right] \left[ ?x = 0 \right] \left[ v := -cv \right] B(x, v) \land \left[ ?x \geq 0 \right] B(x, v) \\
\vdash & \left[ x'' = -g \right] \left[ ?x = 0 ; v := -cv \right] B(x, v) \land \left[ ?x \geq 0 \right] B(x, v) \\
\vdash & \left[ x'' = -g \right] \left[ ?x = 0 ; v := -cv \cup ?x \geq 0 \right] B(x, v) \\
\vdash & \left[ x'' = -g ; ( ?x = 0 ; v := -cv \cup ?x \geq 0 ) \right] B(x, v) \\
A \defeq & 0 \leq x \land x = H \land v = 0 \land g > 0 \land 1 \geq c \geq 0 \\
B(x, v) \defeq & 0 \leq x \land x \leq H \\
\left( x'' = -g \right) \defeq & \left( x' = v, v' = -g \right)
\end{align*} \]
A Proof of a Short Single-hop Bouncing Ball

\[
A \vdash \forall t \geq 0 ((H - \frac{g}{2} t^2 = 0 \rightarrow B(H - \frac{g}{2} t^2, -c(-gt))) \land (H - \frac{g}{2} t^2 \geq 0 \rightarrow B(H - \frac{g}{2} t^2, -gt)))
\]

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

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

\[
A \vdash [x'' = -g]((x = 0 \rightarrow B(x, -cv)) \land (x \geq 0 \rightarrow B(x, v)))
\]

\[
A \vdash [x'' = -g]((x = 0 \rightarrow [v := -cv]B(x, v)) \land (x \geq 0 \rightarrow B(x, v)))
\]

\[
A \vdash [x'' = -g][?x = 0][v := -cv]B(x, v) \land [?x \geq 0]B(x, v)
\]

\[
A \vdash [x'' = -g][?x = 0; v := -cv]B(x, v) \land [?x \geq 0]B(x, v)
\]

\[
A \vdash [x'' = -g][?x = 0; v := -cv \cup ?x \geq 0]B(x, v)
\]

\[
A \vdash [x'' = -g; (?x = 0; v := -cv \cup ?x \geq 0)]B(x, v)
\]

\[
A \overset{\text{def}}{=} 0 \leq x \land x = H \land v = 0 \land g > 0 \land 1 \geq c \geq 0
\]

\[
B(x,v) \overset{\text{def}}{=} 0 \leq x \land x \leq H
\]

\[
(x'' = -g) \overset{\text{def}}{=} (x' = v, v' = -g)
\]
A Proof of a Short Single-hop Bouncing Ball

\[ A \vdash \forall t \geq 0 \left( \left( H - \frac{g}{2} t^2 = 0 \rightarrow B(H - \frac{g}{2} t^2, -c(-gt)) \right) \land \left( H - \frac{g}{2} t^2 \geq 0 \rightarrow B(H - \frac{g}{2} t^2, -gt) \right) \right) \]

\[ \left[=\right] \]
\[ A \vdash \forall t \geq 0 [x := H - \frac{g}{2} t^2] \left( (x = 0 \rightarrow B(x, -c(-gt))) \land (x \geq 0 \rightarrow B(x, -gt)) \right) \]

\[ \left[=\right] \]
\[ A \vdash \forall t \geq 0 [x := H - \frac{g}{2} t^2] [v := -gt] \left( (x = 0 \rightarrow B(x, -cv)) \land (x \geq 0 \rightarrow B(x, v)) \right) \]

\[ \left[=\right] \]
\[ A \vdash \forall t \geq 0 [x := H - \frac{g}{2} t^2; v := -gt] \left( (x = 0 \rightarrow B(x, -cv)) \land (x \geq 0 \rightarrow B(x, v)) \right) \]

\[ \left[=\right] \]
\[ A \vdash [x'' = -g] \left( (x = 0 \rightarrow B(x, -cv)) \land (x \geq 0 \rightarrow B(x, v)) \right) \]

\[ \left[=\right] \]
\[ A \vdash [x'' = -g] \left( (x = 0 \rightarrow [v := -cv] B(x, v)) \land (x \geq 0 \rightarrow B(x, v)) \right) \]

\[ \left[=\right] \]
\[ A \vdash [x'' = -g] \left( [?x = 0] [v := -cv] B(x, v) \land [?x \geq 0] B(x, v) \right) \]

\[ \left[=\right] \]
\[ A \vdash [x'' = -g] \left( [?x = 0; v := -cv] B(x, v) \land [?x \geq 0] B(x, v) \right) \]

\[ \left[=\right] \]
\[ A \vdash [x'' = -g] [?x = 0; v := -cv \cup ?x \geq 0] B(x, v) \]

\[ \left[=\right] \]
\[ A \vdash [x'' = -g; (?x = 0; v := -cv \cup ?x \geq 0)] B(x, v) \]

\[ A \overset{\text{def}}{=} 0 \leq x \land x = H \land v = 0 \land g > 0 \land 1 \geq c \geq 0 \]

\[ B(x, v) \overset{\text{def}}{=} 0 \leq x \land x \leq H \]

\[ (x'' = -g) \overset{\text{def}}{=} (x' = v, v' = -g) \]
Resolving abbreviations at the premise yields:

\[ 0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0 \rightarrow \]
\[ \forall t \geq 0 ((H - \frac{g}{2} t^2 = 0 \rightarrow 0 \leq H - \frac{g}{2} t^2 \wedge H - \frac{g}{2} t^2 \leq H) \]
\[ \wedge (H - \frac{g}{2} t^2 \geq 0 \rightarrow 0 \leq H - \frac{g}{2} t^2 \wedge H - \frac{g}{2} t^2 \leq H)) \]

which is provable by arithmetic (since \( g > 0 \) and \( t^2 \geq 0 \)).
A Proof of a Short Single-hop Bouncing Ball

Resolving abbreviations at the premise yields:

\[ 0 \leq x \land x = H \land v = 0 \land g > 0 \land 1 \geq c \geq 0 \rightarrow \]
\[ \forall t \geq 0 \left( \left( H - \frac{g}{2} t^2 = 0 \rightarrow 0 \leq H - \frac{g}{2} t^2 \land H - \frac{g}{2} t^2 \leq H \right) \right. \]
\[ \left. \land \left( H - \frac{g}{2} t^2 \geq 0 \rightarrow 0 \leq H - \frac{g}{2} t^2 \land H - \frac{g}{2} t^2 \leq H \right) \right) \]

which is provable by arithmetic (since \( g > 0 \) and \( t^2 \geq 0 \)).
Resolving abbreviations at the premise yields:

\[ 0 \leq x \land x = H \land v = 0 \land g > 0 \land 1 \geq c \geq 0 \rightarrow \]
\[ \forall t \geq 0 ((H - \frac{g}{2} t^2 = 0 \rightarrow 0 \leq H - \frac{g}{2} t^2 \land H - \frac{g}{2} t^2 \leq H) \]
\[ \land (H - \frac{g}{2} t^2 \geq 0 \rightarrow 0 \leq H - \frac{g}{2} t^2 \land H - \frac{g}{2} t^2 \leq H)) \]

which is provable by arithmetic (since \( g > 0 \) and \( t^2 \geq 0 \)).

---

**Exciting!**

We have just formally verified our very first CPS!
A Proof of a Short Single-hop Bouncing Ball

Resolving abbreviations at the premise yields:

\[ 0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0 \rightarrow \]

\[ \forall t \geq 0 \left( (H - \frac{g}{2} t^2 = 0 \rightarrow 0 \leq H - \frac{g}{2} t^2 \wedge H - \frac{g}{2} t^2 \leq H) \right. \]

\[ \wedge \left( H - \frac{g}{2} t^2 \geq 0 \rightarrow 0 \leq H - \frac{g}{2} t^2 \wedge H - \frac{g}{2} t^2 \leq H \right) \]

which is provable by arithmetic (since \( g > 0 \) and \( t^2 \geq 0 \)).

Exciting!

We have just formally verified our very first CPS!

Okay, alright, it was a grotesquely simplified single-hop bouncing ball. But the axioms of our proof technique were completely general and not specific to bouncing balls, so they should carry us forward to true CPS.
André Platzer.
Foundations of cyber-physical systems.

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