André Platzer

Carnegie Mellon University

Symposium on Principles of Programming Languages 2019 TutorialFest

http://keymaeraX.org/
1. CPS are Multi-Dynamical Systems
2. CPS Programs
   - Syntax
   - Semantics
   - Examples
3. Differential Dynamic Logic
   - Syntax
   - Semantics
   - Example: Car Control Design
4. Dynamic Axioms for Dynamical Systems
   - Axiomatics
   - Safe CPS Programming & Proving in KeYmaera X
5. Differential Invariants for Differential Equations
6. Applications
7. Verified Compilation of CPS Programs
8. Summary
Outline (Introduction to CPS)

1. CPS are Multi-Dynamical Systems

2. CPS Programs
   - Syntax
   - Semantics
   - Examples

3. Differential Dynamic Logic
   - Syntax
   - Semantics
   - Example: Car Control Design

4. Dynamic Axioms for Dynamical Systems
   - Axiomatics
   - Safe CPS Programming & Proving in KeYmaera X

5. Differential Invariants for Differential Equations

6. Applications

7. Verified Compilation of CPS Programs

8. Summary
Cyber-Physical Systems

CPSs combine cyber capabilities with physical capabilities to solve problems that neither part could solve alone.

Which control decisions are safe for aircraft collision avoidance?
CPSs Promise Transformative Impact!

Prospects: Safe & Efficient

- Driver assistance
- Autonomous cars
- Pilot decision support
- Autopilots / UAVs
- Train protection
- Robots near humans

Prerequisite: CPSs need to be safe

How do we make sure CPSs make the world a better place?
Can you trust a computer to control physics?

Depends on how it has been programmed

And on what will happen if it malfunctions

Safety guarantees require analytic foundations.

A common foundational core helps all application domains.

Foundations revolutionized digital computer science & our society.

Need even stronger foundations when software reaches out into our physical world.

CPSs deserve proofs as safety evidence!

André Platzer (CMU)
Programming Cyber-Physical Systems With Logic
Can you trust a computer to control physics?

1. Depends on how it has been programmed
2. And on what will happen if it malfunctions

Rationale

1. Safety guarantees require analytic foundations.
2. A common foundational core helps all application domains.
3. Foundations revolutionized digital computer science & our society.
4. Need even stronger foundations when software reaches out into our physical world.

CPSs deserve proofs as safety evidence!
CPSs are Multi-Dynamical Systems

CPS Dynamics
CPS are characterized by multiple facets of dynamical systems.

CPS Compositions
CPS combines multiple simple dynamical effects.

Descriptive simplification

Tame Parts
Exploiting compositionality tames CPS complexity.

Analytic simplification
Concept (Differential Dynamic Logic) (JAR’08, LICS’12)
CPS Analysis

Concept (Differential Dynamic Logic) (JAR’08, LICS’12)

\[ [\alpha] \varphi \Rightarrow \varphi \]

\[ x \neq m \]

\[ \neg x = m \land b > 0 \]

\[ \text{init} \rightarrow (\text{if } \text{SB}(x, m) \text{ then } a := -b \text{; } x' = v, v' = a) \]

\[ \text{post} \]

\[ a \]

\[ v \]

\[ x \]

\[ m \]

\[ t \]

\[ \text{André Platzer (CMU)} \]

Programming Cyber-Physical Systems With Logic
Concept (Differential Dynamic Logic) (JAR’08, LICS’12)

\[ [\alpha] \varphi \quad \varphi \]

\[ \Box x \neq m \quad x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]
CPS Analysis

Concept (Differential Dynamic Logic) (JAR’08, LICS’12)

\[ [\alpha] \varphi \rightarrow \varphi \]

\[ [\alpha] x \neq m \rightarrow x \neq m \]

\[ \begin{align*}
  &a \quad 0.5 \\
  &0.0 \\
  &-0.5 \\
  &-1.0 \\
  &-1.5 \\
  &-2.0 \\
  &-2.5 \\
  &\ \\
  &\text{2} \quad \text{3} \quad \text{4} \quad \text{5} \quad \text{6} \quad \text{7} \quad \text{t}
\end{align*} \]

\[ \begin{align*}
  &v \quad 6 \\
  &4 \\
  &2 \\
  &0 \\
  &-2 \\
  &\ \\
  &\text{1} \quad \text{2} \quad \text{3} \quad \text{4} \quad \text{5} \quad \text{6} \quad \text{7} \quad \text{t}
\end{align*} \]

\[ \begin{align*}
  &x \quad 10 \\
  &8 \\
  &6 \\
  &4 \\
  &2 \\
  &0 \\
  &-2 \\
  &\ \\
  &\text{1} \quad \text{2} \quad \text{3} \quad \text{4} \quad \text{5} \quad \text{6} \quad \text{7} \quad \text{t}
\end{align*} \]
Concept (Differential Dynamic Logic)

\[ [\alpha] \varphi \] \rightarrow \varphi

\[ x \neq m \]

\[ [\alpha] x \neq m \]

\[ x' = v, v' = a \]

\[ ODE \]

\[ a \]

\[ v \]

\[ x \]

\[ m \]
CPS Analysis

Concept (Differential Dynamic Logic) (JAR’08, LICS’12)

\[ [\alpha] \varphi \quad \alpha \quad \varphi \]

\[ [x \neq m] \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]
CPS Analysis

Concept (Differential Dynamic Logic) (JAR’08, LICS’12)

\[ [\alpha] \varphi \quad \varphi \]

\[ \begin{align*}
  x \neq m \\
  x \neq m \\
  x \neq m
\end{align*} \]

\[ \begin{align*}
  (\text{if}(SB(x, m)) & \quad a := -b) \\
  x' = v, v' = a
\end{align*} \]

André Platzer (CMU) Programming Cyber-Physical Systems With Logic POPL'19 6 / 66
CPS Analysis

Concept (Differential Dynamic Logic) (JAR’08, LICS’12)

\[ [\alpha] \varphi \quad \alpha \rightarrow \varphi \]

\((\text{if}(\text{SB}(x, m)) \quad a:= -b) ; \quad x' = v, v' = a\)

\(x\)

\(m\)

\(t\)

\(a\)

\(t\)

\(t\)

\(t\)

André Platzer (CMU)

Programming Cyber-Physical Systems With Logic
\( [\alpha] \varphi \Rightarrow \varphi \leq \alpha \)

\[
((\text{if}(SB(x,m)) \ a := -b) ; \ x' = v, v' = a)
\]

- \( a \) values: \(-2.5, -2.0, -1.5, -1.0, -0.5, 0.0, 0.5\)
- \( x \) values: \(-2.0, -1.5, 0.0, 0.5, 1.0, 2.0, 4.0, 8.0\)
- \( m \) values: \(-2.0, 0.0, 2.0, 4.0, 6.0, 8.0, 10.0\)

**Concept (Differential Dynamic Logic)** (JAR’08, LICS’12)

- **sequenced composition**: \( \text{seq. compose} \)
- **non-deterministic repetition**: \( \text{nondet. repeat} \)
- **assignment**: \( \text{assign} \)
- **test**: \( \text{test} \)

André Platzer (CMU)

Programming Cyber-Physical Systems With Logic

POPL’19 6 / 66
CPS Analysis

Concept (Differential Dynamic Logic) (JAR’08, LICS’12)

\[[\alpha]\varphi \rightarrow \varphi\]

\[[\alpha] x \neq m \rightarrow x \neq m\]

\[\left(\left(\text{if}(\text{SB}(x, m)) \ a := -b) ; \ x' = v, v' = a\right)^*\right] x \neq m\]

all runs

\[x \neq m\]

\[\text{post}\]

\[\varphi\]

\[\alpha\]

\[x \neq m\]

\[\varphi\]

\[\alpha\]
CPS Analysis

Concept (Differential Dynamic Logic) (JAR’08, LICS’12)

\[ [\alpha] \varphi \]

\[ \alpha \]

\[ \varphi \]

\[ x \neq m \land b > 0 \rightarrow \left[ \left( \text{init} \left( \text{if} \left( \text{SB}(x, m) \right) \right) \right) \quad a := -b ; \quad x' = v, v' = a \right]^* \]

All runs

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]
Concept (Differential Dynamic Logic) (JAR'08, LICS'12)

\[ [\alpha] \phi \rightarrow \phi \]

\[ x \neq m \land b > 0 \rightarrow \left( [\lnot S_B(x, m) \cup a := -b) ; x' = v, v' = a]^* \right) x \neq m \]

non-deterministic choice

\[ \text{init} \]

\[ \text{post} \]
Concept (Differential Dynamic Logic) (JAR’08, LICS’12)

\[ [\alpha] \varphi \] 

\[ \alpha \]

\[ x \neq m \land b > 0 \rightarrow \left[ (\neg \text{SB}(x, m) \cup a := -b) ; x' = v, v' = a \right]^{*} ] x \neq m \]

det.

choice test

\[ x \neq m \]

\[ x \neq m \]

\[ x \neq m \]

André Platzer (CMU) Programming Cyber-Physical Systems With Logic
Concept (Differential Dynamic Logic) (JAR’08, LICS’12)

$$\alpha \blacklozenge \phi$$

$$x \neq m$$

$$\neg SB(x, m) \cup a := -b; x' = v, v' = a \quad \ast \quad x \neq m$$

Hybrid program dynamics
Outline (Modeling CPS)

1. CPS are Multi-Dynamical Systems
2. CPS Programs
   - Syntax
   - Semantics
   - Examples
3. Differential Dynamic Logic
   - Syntax
   - Semantics
   - Example: Car Control Design
4. Dynamic Axioms for Dynamical Systems
   - Axiomatics
   - Safe CPS Programming & Proving in KeYmaera X
5. Differential Invariants for Differential Equations
6. Applications
7. Verified Compilation of CPS Programs
8. Summary
Example (Speedy the point)

\[ \{ x' = v, v' = a \} \]

Purely continuous dynamics

What about the cyber?
Example (Speedy the point)

\[ a := a + 1 \]

Purely discrete dynamics

How do both meet?
Playing with Acceleration and Braking

Example (Speedy the point)

\[ a := a + 1; \{ x' = v, v' = a \} \]

Hybrid dynamics, i.e., composition of continuous and discrete dynamics
Here: sequential composition first; second
Example (Speedy the point)

\[
\begin{align*}
a &:= -2; \quad \{ x' = v, v' = a \}; \\
a &:= 0.25; \quad \{ x' = v, v' = a \}; \\
a &:= -2; \quad \{ x' = v, v' = a \}; \\
a &:= 0.25; \quad \{ x' = v, v' = a \}; \\
a &:= -2; \quad \{ x' = v, v' = a \}; \\
a &:= 0.25; \quad \{ x' = v, v' = a \};
\end{align*}
\]
Playing with Acceleration and Braking

Example (Speedy the point)

\[
a := -2; \{ x' = v, v' = a \}; \\
a := 0.25; \{ x' = v, v' = a \}; \\
a := -2; \{ x' = v, v' = a \}; \\
a := 0.25; \{ x' = v, v' = a \}; \\
a := -2; \{ x' = v, v' = a \}; \\
a := 0.25; \{ x' = v, v' = a \}.
\]

How long to follow an ODE?
Playing with Acceleration and Braking

Example (Speedy the point)

\[
a := -2; \quad \{x' = v, v' = a\}; \\
\]

\[
a := 0.25; \quad \{x' = v, v' = a\}; \\
\]

\[
a := -2; \quad \{x' = v, v' = a\}; \\
\]

\[
a := 0.25; \quad \{x' = v, v' = a\}; \\
\]

\[
a := 0.25; \quad \{x' = v, v' = a\}; \\
\]

How to check conditions before actions?
Playing with Acceleration and Braking

Example (Speedy the point)

\[
\begin{align*}
\text{if}(v < 4) & \quad a := a + 1 \quad \text{else} \quad a := -b; \\
\{ x' = v, v' = a \}
\end{align*}
\]

Velocity-dependent control
Example (Speedy the point)

\[
\text{if}(x - m > s) a := a + 1 \text{ else } a := -b; \\
\{ x' = v, v' = a \}
\]

Distance-dependent control for obstacle \( m \)
Example (Speedy the point)

\[
\text{if}(x - m > s \land v < 4) \quad a := a + 1 \quad \text{else} \quad a := -b; \\
\{x' = v, v' = a\}
\]

Velocity and distance-dependent control

Iterative Design

Start as simple as possible, then add challenges once basics are correct.
Example (Speedy the point)

\[
\text{if}(x - m > s \land v < 4 \land \text{efficiency}) \ a := a + 1 \ \text{else} \ a := -b;
\]

\[
\{x' = v, \ v' = a\}
\]

Also only accelerate if it’s efficient to do so
Example (Speedy the point)

\[
\text{if}(x - m > s \land v < 4 \land \text{efficiency}) \quad a := a + 1 \quad \text{else} \quad a := -b;
\]
\[
\{x' = v, v' = a\}
\]

Exact models are unnecessarily complex. Not all features are safety-critical.
Example (Speedy the point)

\[(a := a + 1 \cup a := -b);\]
\[\{x' = v, v' = a\}\]

Nondeterministic choice \(\cup\) allows either side to be run, arbitrarily

**Power of Abstraction**

Only include relevant aspects, elide irrelevant detail. The model and its analysis become simpler. And apply to more systems.
Example (Speedy the point)

\[
(a := a + 1 \cup a := -b);
\{x' = v, v' = a\}
\]

Nondeterministic choice \(\cup\) allows either side to be run, arbitrarily.
Oops, now it got too simple! Not every choice is always acceptable.
### Example (Speedy the point)

\[
(? v < 4 ; a := a + 1 \cup a := -b) ;
\{ x' = v , v' = a \}
\]

Test \( ?Q \) checks if formula \( Q \) is true in current state.
Playing with Acceleration and Braking

Example (Speedy the point)

```
(?v < 4; a := a + 1 ∪ a := −b);
{x′ = v, v′ = a}
```

Test ?Q checks if formula Q is true in current state, otherwise run fails.

Discarding failed runs and backtracking

System runs that fail tests are discarded and not considered further.

```
?v < 4; v := v + 1  only runs if
v := v + 1; ?v < 4  only runs if
```

Broader significance of nondeterminism

Nondeterminism is a tool for abstraction to focus on critical aspects. Nondeterminism is essential to describe imperfectly known environment.
Playing with Acceleration and Braking

Example (Speedy the point)

\[(?v < 4; a := a + 1 \cup a := -b); \\
\{x' = v, v' = a\}\]

Test \(Q\) checks if formula \(Q\) is true in current state, otherwise run fails.

Discarding failed runs and backtracking

System runs that fail tests are discarded and not considered further.

\(?v < 4; v := v + 1\) only runs if \(v < 4\) initially true

\(v := v + 1; ?v < 4\) only runs if \(v < 3\) initially true

Broader significance of nondeterminism

Nondeterminism is a tool for abstraction to focus on critical aspects.
Nondeterminism is essential to describe imperfectly known environment.
Playing with Acceleration and Braking

Example (Speedy the point)

\((?v < 4; a := a + 1 \cup a := -b); \{x' = v, v' = a\};\)

\((?v < 4; a := a + 1 \cup a := -b); \{x' = v, v' = a\};\)

\((?v < 4; a := a + 1 \cup a := -b); \{x' = v, v' = a\}\)

Repeated control needs longer programs, e.g., by copy & paste
Example (Speedy the point)

\[
\left( (?v < 4; a := a + 1 \cup a := -b); \\
\{ x' = v, v' = a \} \right)^* 
\]

Nondeterministic repetition * repeats *any* arbitrary number of times
Definition (Syntax of hybrid program $\alpha$)

\[
\alpha, \beta ::= \textit{x} := e \mid \textit{?Q} \mid \textit{x}' = f(\textit{x}) \& \textit{Q} \mid \alpha \cup \beta \mid \alpha ; \beta \mid \alpha^*
\]
Hybrid Programs: Syntax

Definition (Syntax of hybrid program $\alpha$)

$$\alpha, \beta ::= x := e \mid ?Q \mid x' = f(x) \& Q \mid \alpha \cup \beta \mid \alpha; \beta \mid \alpha^*$$

Discrete Assign
Test Condition
Differential Equation
Nondet. Choice
Seq. Compose
Nondet. Repeat

Like regular expressions. Everything nondeterministic

Definition (Semantics of hybrid programs) ($[$ $]$ : $\text{HP} \to \wp(S \times S)$)

$$[$ x := e $]$ = \{ (\omega, \nu) : \nu = \omega \text{ except } \nu[$ x $] = \omega[$ e $] \}$$

$$[$ ?Q $]$ = \{ (\omega, \omega) : \omega \in [$ Q $] \}$$

$$[$ x' = f(x) \& Q $]$ = \{ (\phi(0), \phi(r)) : \phi \models x' = f(x) \text{ for some duration } r \geq 0 \}$$

$$[$ \alpha \cup \beta $]$ = [$ \alpha $] \cup [$ \beta $]$$

$$[$ \alpha ; \beta $]$ = [$ \alpha $] \circ [$ \beta $] = \{ (\omega, \nu) : (\omega, \mu) \in [$ \alpha $] \text{ and } (\mu, \nu) \in [$ \beta $] \}$$

$$[$ \alpha^* $]$ = [$ \alpha $] \ast = \bigcup_{n \in \mathbb{N}} [$ \alpha^n $]$$
Hybrid Programs: Syntax

Definition (Syntax of hybrid program $\alpha$)

$\alpha, \beta ::= x := e \mid \?Q \mid x' = f(x) \& Q \mid \alpha \cup \beta \mid \alpha; \beta \mid \alpha^*$


Like regular expressions. Everything nondeterministic
Hybrid Programs: Semantics

\[ x := e \]

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

\[ ?Q \]
\[ x := e \]

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

\[ \omega \rightarrow v \]

\[ t \]

- \( v \) if \( v(x) = \omega[e] \)
- \( \omega \) and \( v(z) = \omega(z) \) for \( z \neq x \)

\[ t \]

\[ \omega \rightarrow v \]

- \( v \) if \( \omega \in [Q] \)
- \( \omega \) if \( \omega \notin [Q] \)

\[ t \]

\[ \omega \rightarrow v \]

- No change if \( \omega \in [Q] \)
- Otherwise no transition
Hybrid Programs: Semantics

\[ x := e \]  

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

\[ ?Q \]

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

\[ x' = f(x) & Q \text{ if } \omega \in [Q] \]
\[ \omega \text{ if } \omega \not\in [Q] \]

\[ t \]

\[ 0 \]

\[ r \]

\[ x \]

\[ x' \]

Andre Platzer (CMU)  
Programming Cyber-Physical Systems With Logic  
POPL’19 11 / 66
Hybrid Programs: Semantics

\[ x := e \]

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

\[ ?Q \]
Hybrid Programs: Semantics

\[ x := e \]

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

\[ ?Q \]

\[ v \text{ if } v(x) = \omega[e] \]

\[ \omega \text{ and } v(z) = \omega(z) \text{ for } z \neq x \]

\[ x' = f(x) \& Q \]
Hybrid Programs: Semantics

\[ x := e \]

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

\[ ? Q \]
Hybrid Programs: Semantics

\[ x := e \]

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

\[ \text{if } \omega \in \llbracket Q \rrbracket \]

\[ v \text{ if } v(x) = \omega[e] \]

\[ \omega \text{ and } v(z) = \omega(z) \text{ for } z \neq x \]

\[ \text{no change if } \omega \in \llbracket Q \rrbracket \]
Hybrid Programs: Semantics

\[ x := e \]

\[ \nu(x) = \omega(e) \]

\[ \nu(z) = \omega(z) \text{ for } z \neq x \]

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

\[ \omega \text{ no change if } \omega \in [Q] \]

\[ \omega \text{ otherwise no transition} \]
Hybrid Programs: Semantics

\[
\omega \cup \beta
\]

\[
\omega ; \beta
\]

\[
\omega^* \rightarrow \nu
\]
Hybrid Programs: Semantics

\[ \alpha \cup \beta \]

\[ \omega \quad \rightarrow \quad v_1 \]

\[ \beta \quad \rightarrow \quad v_2 \]

\[ \alpha; \beta \]

\[ \omega \quad \rightarrow \quad v \]

\[ \alpha^* \]

\[ \omega \quad \rightarrow \quad v \]

\[ x \]

\[ t \]

\[ v_1 \]

\[ v_2 \]
Hybrid Programs: Semantics

\[ \omega \xrightarrow{\alpha} v_1 \]
\[ \omega \xrightarrow{\beta} v_2 \]
\[ v_1 \xrightarrow{\alpha \cup \beta} v_2 \]
\[ \alpha ; \beta \]

\[ \omega \xrightarrow{\alpha} \mu \xrightarrow{\beta} v \]

\[ \omega \xrightarrow{\alpha^*} v \]

\[ x \]
\[ \omega \]
\[ v_1 \]
\[ v_2 \]
\[ t \]

\[ x \]
\[ \omega \]
\[ v \]
\[ t \]

\[ \mu \]

\[ \text{André Platzer (CMU)} \]

Programming Cyber-Physical Systems With Logic

POPL'19 11 / 66
Plug-in for Semantics of Composed Hybrid Programs

\[ \alpha ; \beta \]

\[ \omega \xrightarrow{\alpha} \mu \xrightarrow{\beta} \nu \]

\[ \alpha^* \]

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

\[ \omega \xrightarrow{\alpha} \nu_1 \xrightarrow{\alpha \cup \beta} \nu_2 \xrightarrow{\beta} \nu \]
Hybrid Programs: Syntax & Semantics

Definition (Syntax of hybrid program $\alpha$)

$\alpha, \beta ::= x := e \mid ?Q \mid x' = f(x) \& Q \mid \alpha \cup \beta \mid \alpha;\beta \mid \alpha^*$

Definition (Semantics of hybrid programs) ($\llbracket \cdot \rrbracket : \text{HP} \to \mathcal{P}(S \times S)$)

$\llbracket x := e \rrbracket = \{(\omega, \nu) : \nu = \omega \text{ except } \nu[x] = \omega[e]\}$
$\llbracket ?Q \rrbracket = \{(\omega, \omega) : \omega \in \llbracket Q \rrbracket\}$
$\llbracket x' = f(x) \rrbracket = \{(\varphi(0), \varphi(r)) : \varphi \models x' = f(x) \text{ for some duration } r \geq 0\}$
$\llbracket \alpha \cup \beta \rrbracket = \llbracket \alpha \rrbracket \cup \llbracket \beta \rrbracket$
$\llbracket \alpha;\beta \rrbracket = \llbracket \alpha \rrbracket \circ \llbracket \beta \rrbracket = \{(\omega, \nu) : (\omega, \mu) \in \llbracket \alpha \rrbracket \text{ and } (\mu, \nu) \in \llbracket \beta \rrbracket\}$
$\llbracket \alpha^* \rrbracket = \llbracket \alpha \rrbracket^* = \bigcup_{n \in \mathbb{N}} \llbracket \alpha^n \rrbracket \quad \alpha^n \equiv \underbrace{\alpha;\alpha;\alpha;...;\alpha}_{n \text{ times}}$

André Platzer (CMU) Programming Cyber-Physical Systems With Logic
Hybrid Programs: Syntax & Semantics

Definition (Syntax of hybrid program $\alpha$)

$$\alpha, \beta ::= x := e \mid ?Q \mid x' = f(x) \& Q \mid \alpha \cup \beta \mid \alpha; \beta \mid \alpha^*$$

Definition (Semantics of hybrid programs) ($[[\cdot]] : \text{HP} \to \mathcal{P}(\mathcal{S} \times \mathcal{S})$)

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

Compositional

1. $\varphi(z)(x') = \frac{d\varphi(t)(x)}{dt}(z)$ exists at all times $0 \leq z \leq r$
2. $\varphi(z) \in [[x' = f(x) \& Q]]$ for all times $0 \leq z \leq r$
3. $\varphi(z) = \varphi(0)$ except at $x, x'$

André Platzer (CMU)
Example (Quantum the Bouncing Ball)
Example (Quantum the Bouncing Ball)

$$\{x' = v, v' = -g\}$$
Example (Quantum the Bouncing Ball)

\[ \{ x' = v, v' = -g \} \]
Example (Quantum the Bouncing Ball)

\[ \{ x' = v, v' = -g \land x \geq 0 \} \]
Example (Quantum the Bouncing Ball)

\[
\begin{align*}
{x'} &= v, \quad v' = -g \land x \geq 0; \\
\text{if} (x = 0) \quad &v := -cv
\end{align*}
\]
Example (Quantum the Bouncing Ball)

\[
\begin{align*}
\{ & x' = v, \ v' = -g & \& \ x \geq 0 \}; \\
\text{if} & \ (x = 0) \ v := -cv
\end{align*}
\]
Example (Quantum the Bouncing Ball)

\[
\{ x' = v, \ v' = -g \ \& \ x \geq 0 \}; \\
\text{if} ( x = 0 ) \ \ v := -cv \]"
Example (Quantum the Bouncing Ball)

\[
\left\{ x' = v, \quad v' = -g \land x \geq 0 \right\}; \\
\text{if} \ (x = 0) \quad v := -cv
\]
Example (Quantum the Bouncing Ball)

\[
\{ x' = v, \ v' = -g \ & x \geq 0 \}; \\
\text{if}(x = 0) \ v := -cv
\]
Example (Quantum the Bouncing Ball)

\[
\begin{align*}
\{ x' &= v, \ v' = -g \& x \geq 0 \}; \\
\text{if} (x = 0) &\quad v := -cv^* 
\end{align*}
\]
Example (Quantum the Bouncing Ball)

\[
\begin{align*}
\{(x = v, v' = -g \& x \geq 0) ;
& \quad \text{if}(x = 0) (v := -cv \cup v := 0) \}^* \\
& \text{if}(Q) \alpha \text{ else } \beta \equiv (Q; \alpha) \cup (\neg Q; \beta)
\end{align*}
\]
Example (Quantum the Bouncing Ball)

\[
\begin{align*}
\{x' = v, v' = -g & \land x \geq 0\}; \\
\text{if}(x = 0) (\text{c} := \ast; ?\text{c} \geq 0; \text{v} := -cv))^* 
\end{align*}
\]
Runaround Robot with Dubins Paths

André Platzer (CMU)
Example (Runaround Robot)

\[
\begin{align*}
((\omega := -1 \cup \omega := 1 \cup \omega := 0); \\
\{x' = v, y' = w, v' = \omega w, w' = -\omega v\}\}^*
\end{align*}
\]
Example (Runaround Robot)

\[
((?Q_{-1}; \omega := -1 \cup ?Q_1; \omega := 1 \cup ?Q_0; \omega := 0); \\
\{x' = v, y' = w, v' = \omega w, w' = -\omega v\})^*
\]
Example (Runaround Robot)

\[
((\text{?}Q_{-1}; \omega := -1 \cup \text{?}Q_{1}; \omega := 1 \cup \text{?}Q_{0}; \omega := 0); \\
\{x' = v, y' = w, \nu' = \omega w, w' = -\omega v\})^* 
\]
Runaround Robot with Dubins Paths

Example (Runaround Robot)

\[
\left( (?Q_{-1}; \omega := -1 \cup ?Q_1; \omega := 1 \cup ?Q_0; \omega := 0); \right) \\
\{ x' = v, y' = w, v' = \omega w, w' = -\omega v \}\)

\[ Q \]
Example (Runaround Robot)

\[
((?Q_{-1}; \omega := -1 \cup ?Q_1; \omega := 1 \cup ?Q_0; \omega := 0); \{x' = v, y' = w, v' = \omega w, w' = -\omega v\})^*
\]
Runaround Robot with Dubins Paths

Example (Runaround Robot)

\[
((?Q_{-1}; \omega := -1 \cup ?Q_1; \omega := 1 \cup ?Q_0; \omega := 0); \\
\{x' = v, y' = w, v' = \omega w, w' = -\omega v\})^*
\]
Example ( Runaround Robot)

\[
((?Q_{-1}; \omega := -1 \cup {?Q}; \omega := 1 \cup {?Q_0}; \omega := 0); \\
\{x' = v, y' = w, v' = \omega w, w' = -\omega v\})^*
\]
Example (Runaround Robot)

\[
((?Q_{-1}; \omega := -1 \cup ?Q_1; \omega := 1 \cup ?Q_0; \omega := 0); \\
\{x' = v, y' = w, v' = \omega w, w' = -\omega v\})^*\
\]
Runaround Robot with Dubins Paths

Example (Runaround Robot)

\[
(\mathcal{Q}_1; \omega := -1 \cup \mathcal{Q}_1; \omega := 1 \cup \mathcal{Q}_0; \omega := 0);
\{x' = v, y' = w, v' = \omega w, w' = -\omega v\}^*
\]
Example (Runaround Robot)

\[
\left( (?Q_{-1}; \omega := -1 \cup ?Q_1; \omega := 1 \cup ?Q_0; \omega := 0) ;
\{x' = v, y' = w, \nu' = \omega w, w' = -\omega v\}\right)^* 
\]
Example (Runaround Robot)

\[
((？Q_{-1}; \omega := -1 \cup ？Q_{1}; \omega := 1 \cup ？Q_{0}; \omega := 0); \{x' = v, y' = w, v' = \omega w, w' = -\omega v\})^*
\]
Runaround Robot with Dubins Paths

\[ \begin{align*}
\omega &:= -1 \\
\omega &:= 1 \\
\omega &:= 0
\end{align*} \]

\[ \begin{align*}
x' &= v \\
y' &= w \\
v' &= \omega w \\
w' &= -\omega v
\end{align*} \]

Example (Runaround Robot)

\[
((?Q_{-1}; \omega := -1 \cup ?Q_{1}; \omega := 1 \cup ?Q_{0}; \omega := 0); \\
\{x' = v, y' = w, v' = \omega w, w' = -\omega v\})^*
\]
Example (Runaround Robot)

\[
((?Q_1; \omega := -1 \cup ?Q_0; \omega := 0); \\
\{x' = v, y' = w, v' = \omega w, w' = -\omega v\})^*
\]
Runaround Robot with Dubins Paths

Example (Runaround Robot)

\[
\left(\left(\?Q_{-1}; \omega := -1 \cup \?Q_1; \omega := 1 \cup \?Q_0; \omega := 0\right); \left\{x' = v, y' = w, v' = \omega w, w' = -\omega v\right\}\right)^* 
\]
Runaround Robot with Dubins Paths

(\(x, y\))

(\(v, w\))

\(\omega \) = 0

\(\omega \) = 1

\(\omega \) = 1

\(x' = v\)

\(y' = w\)

\(v' = \omega w\)

\(w' = -\omega v\)

\((?Q_{-1}; \omega := -1 \cup ?Q_1; \omega := 1 \cup ?Q_0; \omega := 0);\)

\(\{x' = v, y' = w, v' = \omega w, w' = -\omega v\}\)
Example (Runaround Robot)

\[
\left( (?Q_{-1}; \omega := -1 \cup ?Q_1; \omega := 1 \cup ?Q_0; \omega := 0); \right)
\left\{ x' = v, y' = w, v' = \omega w, w' = -\omega v \right\}^* 
\]
\( \omega := -1 \quad \omega := 1 \quad \omega := 0 \)

\[
\begin{align*}
  x' &= v \\
  y' &= w \\
  v' &= \omega w \\
  w' &= -\omega v
\end{align*}
\]

Example (Runaround Robot)

\[
((?Q_{-1}; \omega := -1 \cup ?Q_1; \omega := 1 \cup ?Q_0; \omega := 0); \{x' = v, y' = w, v' = \omega w, w' = -\omega v\})^*
\]
Example (Runaround Robot)

\[
\left(\left(?Q_1; \omega := -1 \cup ?Q_1; \omega := 1 \cup ?Q_0; \omega := 0\right) ; \left\{x' = v, y' = w, v' = \omega w, w' = -\omega v\right\}\right)^* 
\]
Example (Runaround Robot)

\[
((?Q_{-1}; \omega := -1 \cup ?Q_1; \omega := 1 \cup ?Q_0; \omega := 0); \\
\{x' = v, y' = w, v' = \omega w, w' = -\omega v\})^*
\]
Outline (Specifying CPS)

1. CPS are Multi-Dynamical Systems
2. CPS Programs
   - Syntax
   - Semantics
   - Examples
3. Differential Dynamic Logic
   - Syntax
   - Semantics
   - Example: Car Control Design
4. Dynamic Axioms for Dynamical Systems
   - Axiomatics
   - Safe CPS Programming & Proving in KeYmaera X
5. Differential Invariants for Differential Equations
6. Applications
7. Verified Compilation of CPS Programs
8. Summary
Concept (Differential Dynamic Logic) (JAR’08, LICS’12)

\[
[\alpha] \varphi \rightarrow \varphi
\]

\[
x \neq m \land b > 0 \rightarrow [((\text{if}(SB(x, m)) \ a := -b) ; x' = v, v' = a)^*] x \neq m
\]

**init**

**all runs**

**post**
Example (Quantum the Bouncing Ball)

\[
\begin{align*}
\{x' = v, v' = -g & \land x \geq 0 \}; \\
\text{if}(x = 0) v & := -cv
\end{align*}
\]
Example (Quantum the Bouncing Ball)

\[
\text{ensures}(0 \leq x)
\]

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

\[
\text{if}(x = 0) v := -cv
\]
Example (Quantum the Bouncing Ball)

\begin{align*}
\text{ensures}(0 & \leq x) \\
\text{ensures}(x & \leq H) \\
\{x' = v, v' = -g & x \geq 0\}; \\
\text{if}(x = 0) v & := -cv
\end{align*}
Example (Quantum the Bouncing Ball)

\texttt{requires}(x = H)

\texttt{ensures}(0 \leq x)

\texttt{ensures}(x \leq H)

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

\(\text{if}(x = 0) v := -cv\)
Example (Quantum the Bouncing Ball)

- `requires(x = H)`
- `requires(0 ≤ H)`
- `ensures(0 ≤ x)`
- `ensures(x ≤ H)`
- `(\{x' = v, v' = -g & x \geq 0\};
  if(x = 0) v := -cv)^*`
Example (Quantum the Bouncing Ball)

\[
\begin{align*}
\text{requires} & (x = H) \\
\text{requires} & (0 \leq H) \\
\text{ensures} & (0 \leq x) \\
\text{ensures} & (x \leq H) \\
\{x' = v, v' = -g \land x \geq 0\} & \quad \text{if } (x = 0) \ v := -cv \\
\text{invariant} & (x \geq 0)
\end{align*}
\]
Example (Quantum the Bouncing Ball)

\[
\text{requires}(x = H)\\
\text{requires}(0 \leq H)\\
\text{ensures}(0 \leq x)\\
\text{ensures}(x \leq H)\\
\{x' = v, v' = -g & x \geq 0\};\\
\text{if}(x = 0) \ v := -cv)^* @\text{invariant}(x \geq 0)
\]
CPS contracts are crucial for CPS safety. We need to understand CPS programs and contracts and how we can convince ourselves that a CPS program respects its contract.

Contracts are at a disadvantage compared to full logic.

**Logic is for Specification and Reasoning**

1. Specification of a whole CPS program.
2. Analytic inspection of its parts.
3. Argumentative relations between contracts and program parts.

“Yes, this CPS program meets its contract, and here’s why . . . ”
Example (Quantum the Bouncing Ball)

\begin{align*}
\text{requires} & \left( x = H \right) \\
\text{requires} & \left( 0 \leq H \right) \\
\text{ensures} & \left( 0 \leq x \right) \\
\text{ensures} & \left( x \leq H \right) \\
\{ x' = v, v' = -g & x \geq 0 \} ; \\
\text{if} (x = 0) v := -cv \}
\end{align*}
Example (Quantum the Bouncing Ball)

- **requires**$(x = H)$
- **requires**$(0 \leq H)$
- **ensures**$(0 \leq x)$
- **ensures**$(x \leq H)$

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

if$(x = 0) v := -cv)^*$

**Precondition:**
$x = H \land 0 \leq H$ in FOL
Example (Quantum the Bouncing Ball)

\[ \text{requires}(x = H) \]
\[ \text{requires}(0 \leq H) \]
\[ \text{ensures}(0 \leq x) \]
\[ \text{ensures}(x \leq H) \]
\[
\{ x' = v, v' = -g \& x \geq 0 \}; \\
\text{if}(x = 0) v := -cv 
\]

Precondition:
\[ x = H \land 0 \leq H \text{ in FOL} \]

Postcondition:
\[ 0 \leq x \land x \leq H \text{ in FOL} \]
Example (Quantum the Bouncing Ball)

\[
\text{requires}(x = H) \quad \text{Precondition:} \quad x = H \land 0 \leq H \text{ in FOL}
\]

\[
\text{requires}(0 \leq H) \quad \text{Postcondition:} \quad 0 \leq x \land x \leq H \text{ in FOL}
\]

\[
\text{ensures}(0 \leq x)
\]

\[
\text{ensures}(x \leq H)
\]

\[
(\{x' = v, v' = -g \& x \geq 0\}; \quad \text{How to say post is true after all HP runs?}
\]

\[
\text{if}(x = 0) \quad v := -cv
\]
Example (Quantum the Bouncing Ball)

- `requires(x = H)`
  - Precondition: \( x = H \land 0 \leq H \) in FOL

- `requires(0 \leq H)`
  - Postcondition: \( 0 \leq x \land x \leq H \) in FOL

- `ensures(0 \leq x)`

- `ensures(x \leq H)`

- `\{ x' = v, v' = -g \land x \geq 0 \};`

- `if(x = 0) v := -cv` **(starred)**
Example (Quantum the Bouncing Ball)

**requires**$(x = H)$

**requires**$(0 \leq H)$

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

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

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

*if$(x = 0) v := -cv)^*$

Precondition:

$x = H \land 0 \leq H$ in FOL

Postcondition:

$0 \leq x \land x \leq H$ in FOL
Example (Quantum the Bouncing Ball)

- **requires**($x = H$)
- **requires**($0 \leq H$)
- **ensures**($0 \leq x$)
- **ensures**($x \leq H$)

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

\[
\text{if}(x = 0) \rightarrow v := -cv
\]

**Precondition:**
$x = H \land 0 \leq H$ in FOL

**Postcondition:**
$0 \leq x \land x \leq H$ in FOL
Example (Quantum the Bouncing Ball)

- \textbf{requires}(x = H)
- \textbf{requires}(0 \leq H)
- \textbf{ensures}(0 \leq x)
- \textbf{ensures}(x \leq H)

\[
\{x' = v, v' = -g \& x \geq 0\};
\]
\[
\text{if}(x = 0) \quad v := -cv
\]*

---

Precondition:

\[
x = H \land 0 \leq H \text{ in FOL}
\]

Postcondition:

\[
0 \leq x \land x \leq H \text{ in FOL}
\]
Example (Quantum the Bouncing Ball)

\[
\begin{align*}
\text{requires} & \ (x = H) \\
\text{requires} & \ (0 \leq H) \\
\text{ensures} & \ (0 \leq x) \\
\text{ensures} & \ (x \leq H) \\
\{x' = v, v' = -g \& x \geq 0\}; & \text{if}(x=0) \ v := -cv)
\end{align*}
\]

Precondition: \(x = H \land 0 \leq H\) in FOL

Postcondition: \(0 \leq x \land x \leq H\) in FOL

\[
\left\{\{x' = v, v' = -g \& x \geq 0\}; \text{if}(x = 0) \ v := -cv\right\}^*
\]
Example (Quantum the Bouncing Ball)

requires \( x = H \)

requires \( 0 \leq H \)

ensures \( 0 \leq x \)

ensures \( x \leq H \)

\[
\left(\{ x' = v, v' = -g \wedge x \geq 0 \}; \text{if}(x = 0) v := -cv \right)^* [x \leq H]
\]

Precondition:
\( x = H \wedge 0 \leq H \) in FOL

Postcondition:
\( 0 \leq x \wedge x \leq H \) in FOL
Example (Quantum the Bouncing Ball)

**requires** \(x = H\)  

**requires** \(0 \leq H\)  

**ensures** \(0 \leq x\)  

**ensures** \(x \leq H\)  

\(\{x' = v, v' = -g \& x \geq 0\}; \text{if}(x = 0) \ v := -cv\)^* \(x \leq H\) 

\(\{x' = v, v' = -g \& x \geq 0\}; \text{if}(x = 0) \ v := -cv\)^* \(x \leq H\)
Example (Quantum the Bouncing Ball)

- **requires** \((x = H)\)
- **requires** \((0 \leq H)\)
- **ensures** \((0 \leq x)\)
- **ensures** \((x \leq H)\)

\[
\begin{align*}
[&\{x' = v, v' = -g & x \geq 0\}; \text{if}(x=0) \ v := -cv]^*](0 \leq x) \\
[&\{x' = v, v' = -g & x \geq 0\}; \text{if}(x=0) \ v := -cv]^*](x \leq H) \\
[&\{x' = v, v' = -g & x \geq 0\}; \text{if}(x=0) \ v := -cv]^*](0 \leq x \land x \leq H)
\end{align*}
\]

**Precondition:**
\(x = H \land 0 \leq H\) in FOL

**Postcondition:**
\(0 \leq x \land x \leq H\) in FOL
Example (Quantum the Bouncing Ball)

**Precondition:**

\[
[\{(x' = v, v' = -g \land x \geq 0) \land (x = 0) \implies v := -cv\}^*](0 \leq x) \land \left[\{(x' = v, v' = -g \land x \geq 0) \land (x = 0) \implies v := -cv\}^*](x \leq H) \land \left[\{(x' = v, v' = -g \land x \geq 0) \land (x = 0) \implies v := -cv\}^*](0 \leq x \land x \leq H)
\]

**Postcondition:**

\[
0 \leq x \land x \leq H \text{ in FOL}
\]
Contracts for Quantum the Acrophobic Bouncing Ball

Example (Quantum the Bouncing Ball)

\[
[\{ \{ x' = v, v' = -g & x \geq 0 \}; \text{if}(x = 0) v := -cv \}^*](0 \leq x)
\]
Example (Quantum the Bouncing Ball)

**requires** \( (x = H) \)

Precondition:
\( x = H \land 0 \leq H \) in FOL

**requires** \( (0 \leq H) \)

Postcondition:
\( 0 \leq x \land x \leq H \) in FOL

**ensures** \( (0 \leq x) \)

\( \{x' = v, v' = -g \land x \geq 0\}; \text{if}(x = 0) v := -c v \}^* \)

\( 0 \leq x \)

\( x \leq H \)
Contracts for Quantum the Acrophobic Bouncing Ball

\[ 0 \leq x \land x = H \rightarrow [(\{x' = v, v' = -g \land x \geq 0\} ; \text{if}(x=0) v := -cv)^*](0 \leq x) \]

**Example (Quantum the Bouncing Ball)**

- **requires** \( x = H \)
- **requires** \( 0 \leq H \)
- **ensures** \( 0 \leq x \)
- **ensures** \( x \leq H \)

\[
\{(x' = v, v' = -g \land x \geq 0) ; \text{if}(x = 0) v := -cv \}^* \]

**Precondition:**
\( x = H \land 0 \leq H \) in FOL

**Postcondition:**
\( 0 \leq x \land x \leq H \) in FOL
Definition (Syntax of differential dynamic logic)

The formulas of differential dynamic logic are defined by the grammar:

\[ P, Q ::= e \geq \tilde{e} \mid \neg P \mid P \land Q \mid P \lor Q \mid P \rightarrow Q \mid \forall x \, P \mid \exists x \, P \mid [\alpha]P \mid \langle \alpha \rangle P \]
Definition (Syntax of differential dynamic logic)

The formulas of differential dynamic logic are defined by the grammar:

\[
P, Q ::= e \geq \bar{e} \mid \neg P \mid P \land Q \mid P \lor Q \mid P \rightarrow Q \mid \forall x P \mid \exists x P \mid [\alpha]P \mid \langle \alpha \rangle P
\]
Definition (dL Formulas)

\[ [\alpha]P \]

\[ \omega \]

\[ P \]

\[ P \]

\[ P \]
Definition (dL Formulas)

$$\langle \alpha \rangle P \text{ and } \alpha \text{-span } \left[ \alpha \right] P$$

André Platzer (CMU)
Definition (dL Formulas)

\[
\omega \quad \frac{\alpha}{P} \quad \alpha\text{-span}
\]
Definition (dL Formulas)

\[ [\alpha]P \]

\[ \langle \beta \rangle P \]

\[ \omega \]

\[ \beta\text{-span} \]

\[ \alpha\text{-span} \]
Definition (dL Formulas)

\[ \omega \]

\[ [\alpha]P \]

\[ \langle \beta \rangle P \]

\[ \beta\text{-span} \]

\[ \alpha\text{-span} \]
Differential Dynamic Logic: Syntax & Semantics

Definition (Syntax of differential dynamic logic)

The formulas of differential dynamic logic are defined by the grammar:

\[ P, Q ::= e \geq \tilde{e} \mid \neg P \mid P \land Q \mid P \lor Q \mid P \to Q \mid \forall x \ P \mid \exists x \ P \mid [\alpha]P \mid \langle \alpha \rangle P \]

Definition (dL semantics) \([\cdot] : \text{Fml} \to \mathcal{P}(\mathcal{S})\)

\[
\begin{align*}
[ e \geq \tilde{e} ] &= \{ \omega : \omega[e] \geq \omega[\tilde{e}] \} \\
[\neg P] &= [P]^c = \mathcal{S} \setminus [P] \\
[P \land Q] &= [P] \cap [Q] \\
[P \lor Q] &= [P] \cup [Q] \\
[P \to Q] &= [P]^c \cup [Q] \\
[\langle \alpha \rangle P] &= [\alpha] \circ [P] = \{ \omega : \exists \nu : (\omega, \nu) \in [\alpha] \} \\
[[\alpha]P] &= [\neg \langle \alpha \rangle \neg P] = \{ \omega : \forall \nu : (\omega, \nu) \in [\alpha] \} \\
[\exists x \ P] &= \{ \omega : \omega_x^r \in [P] \text{ for some } r \in \mathbb{R} \} \\
[\forall x \ P] &= \{ \omega : \omega_x^r \in [P] \text{ for all } r \in \mathbb{R} \} \\
\end{align*}
\]

\[ \omega^d_x(y) = \begin{cases} 
  d & \text{if } y = x \\
  \omega(y) & \text{if } y \neq x 
\end{cases} \]
\( [P] \) the set of states in which formula \( P \) is true

\( \omega \in [P] \) formula \( P \) is true in state \( \omega \), alias \( \omega \models P \)

\( \models P \) formula \( P \) is valid, i.e., true in all states \( \omega \), i.e., \( [P] = \mathcal{I} \)

---

**Definition (dL semantics) \((\llbracket \cdot \rrbracket : \text{Fml} \rightarrow \wp(\mathcal{I}))\)**

\[
\begin{align*}
\llbracket e \geq \tilde{e} \rrbracket &= \{ \omega : \omega[e] \geq \omega[\tilde{e}] \} \\
\llbracket \neg P \rrbracket &= [P]^c = \mathcal{I} \setminus [P] \\
\llbracket P \land Q \rrbracket &= [P] \cap [Q] \\
\llbracket P \lor Q \rrbracket &= [P] \cup [Q] \\
\llbracket P \rightarrow Q \rrbracket &= [P]^c \cup [Q] \\
\llbracket \langle \alpha \rangle P \rrbracket &= [\alpha] \circ [P] = \{ \omega : \nu \in [P] \text{ for some } \nu : (\omega, \nu) \in [\alpha] \} \\
\llbracket [\alpha] P \rrbracket &= \llbracket \neg \langle \alpha \rangle \neg P \rrbracket = \{ \omega : \nu \in [P] \text{ for all } \nu : (\omega, \nu) \in [\alpha] \} \\
\llbracket \exists x P \rrbracket &= \{ \omega : \omega'_{x} \in [P] \text{ for some } r \in \mathbb{R} \} \\
\llbracket \forall x P \rrbracket &= \{ \omega : \omega'_{x} \in [P] \text{ for all } r \in \mathbb{R} \}
\end{align*}
\]
**Differential Dynamic Logic: Syntax & Semantics**

The set of states in which formula $P$ is true is denoted by $\llbracket P \rrbracket$. A state $\omega$ is in $\llbracket P \rrbracket$ if $P$ is true in that state, i.e., $\omega \models P$. A formula $P$ is valid, i.e., true in all states, if $\llbracket P \rrbracket = S$.

For example,

- $\exists d [ x := 1; x' = d ] x \geq 0$ and
- $[ x := x + 1; x' = d ] x \geq 0$ and
- $\langle x' = d \rangle x \geq 0$

**Definition (dL semantics)**

$(\llbracket \cdot \rrbracket : \text{Fml} \to \mathcal{P}(S))$

- $\llbracket e \geq \tilde{e} \rrbracket = \{ \omega : \omega[e] \geq \omega[\tilde{e}] \}$
- $\llbracket \neg P \rrbracket = \llbracket P \rrbracket^c = S \setminus \llbracket P \rrbracket$
- $\llbracket P \land Q \rrbracket = \llbracket P \rrbracket \cap \llbracket Q \rrbracket$
- $\llbracket P \lor Q \rrbracket = \llbracket P \rrbracket \cup \llbracket Q \rrbracket$
- $\llbracket P \rightarrow Q \rrbracket = \llbracket P \rrbracket^c \cup \llbracket Q \rrbracket$
- $\llbracket \langle \alpha \rangle P \rrbracket = [\alpha] \circ \llbracket P \rrbracket = \{ \omega : \nu \in \llbracket P \rrbracket \text{ for some } \nu : (\omega, \nu) \in [\alpha] \}$
- $\llbracket [\alpha] P \rrbracket = [\neg \langle \alpha \rangle \neg P] = \{ \omega : \nu \in \llbracket P \rrbracket \text{ for all } \nu : (\omega, \nu) \in [\alpha] \}$
- $\llbracket \exists x P \rrbracket = \{ \omega : \omega'_x \in \llbracket P \rrbracket \text{ for some } r \in \mathbb{R} \}$
- $\llbracket \forall x P \rrbracket = \{ \omega : \omega'_x \in \llbracket P \rrbracket \text{ for all } r \in \mathbb{R} \}$
Differential Dynamic Logic: Syntax & Semantics

\([P]\) the set of states in which formula \(P\) is true
\(\omega \in [P]\) formula \(P\) is true in state \(\omega\), alias \(\omega \models P\)
\(\models P\) formula \(P\) is valid, i.e., true in all states \(\omega\), i.e., \([P]\) = \(\mathcal{I}\)

\(\models \exists d [x := 1; x' = d] x \geq 0\) and \(\not\models [x := x + 1; x' = d] x \geq 0\) and \(\not\models \langle x' = d \rangle x \geq 0\)

**Definition (dL semantics)**

\([e \geq \tilde{e}]\) = \(\{ \omega : \omega[e] \geq \omega[\tilde{e}] \}\)
\([\neg P]\) = \([P]^c = \mathcal{I} \setminus [P]\)
\([P \land Q]\) = \([P]\) \cap \([Q]\)
\([P \lor Q]\) = \([P]\) \cup \([Q]\)
\([P \rightarrow Q]\) = \([P]^c \cup [Q]\)
\([\langle \alpha \rangle P]\) = \([\alpha] \circ [P] = \{ \omega : \nu \in [P] \text{ for some } \nu : (\omega, \nu) \in [\alpha] \}\)
\([\lbrack \alpha \rbrack P]\) = \([\neg \langle \alpha \rangle \neg P]\) = \(\{ \omega : \nu \in [P] \text{ for all } \nu : (\omega, \nu) \in [\alpha] \}\)
\([\exists x P]\) = \(\{ \omega : \omega_x' \in [P] \text{ for some } r \in \mathbb{R} \}\)
\([\forall x P]\) = \(\{ \omega : \omega_x' \in [P] \text{ for all } r \in \mathbb{R} \}\)

\(\llbracket \cdot \rrbracket : \text{Fml} \rightarrow \mathcal{P}(\mathcal{I})\)
Example (Bouncing Ball)

\[
\begin{align*}
\{ x' = v, v' = -g & \land x \geq 0 \}; \\
\text{if}(x = 0) v & := -cv^* \\
\end{align*}
\]
$H = x \geq 0$ \quad \rightarrow \quad [\{ x' = v, v' = -g \land x \geq 0 \};$
\[ \text{if}(x = 0) v := -cv \] $0 \leq x \leq H$
Quantum the Acrophobic Bouncing Ball

Example (Bouncing Ball)

\[ H = x \geq 0 \quad \rightarrow \quad \{ x' = v, v' = -g & x \geq 0 \}; \]
\[ \text{if}(x = 0) \quad v := -cv \] * \[ 0 \leq x \leq H \]

Not if \( g < 0 \) in anti-gravity
Example (Bouncing Ball)

\[ H = x \geq 0 \land g > 0 \rightarrow \left[ \{ x' = v, v' = -g \land x \geq 0 \}; \right. \]
\[ \left. \text{if } (x = 0) \ v := -cv \right]^* \] 0 \leq x \leq H
Quantum the Acrophobic Bouncing Ball

Not if $c > 1$ for anti-damping

Example (Bouncing Ball)

$$H = x \geq 0 \land g > 0 \quad \rightarrow \quad \left( \{ x' = v, v' = -g \land x \geq 0 \}; \right.$$

\[ \text{if} (x = 0) v := -cv \right) \quad 0 \leq x \leq H \]
Example (Bouncing Ball)

\[ 1 \geq c \geq 0 \land H = x \geq 0 \land g > 0 \rightarrow \left[ \left( \{ x' = v, v' = -g \land x \geq 0 \} ; \right. \right. \]
\[
\text{if} (x = 0) \ v := -cv \left. \left. \right)^* \right] 0 \leq x \leq H \]
Quantum the Acrophobic Bouncing Ball

Example (Bouncing Ball)

\[ 1 \geq c \geq 0 \land H = x \geq 0 \land g > 0 \rightarrow \left( \{ x' = v, v' = -g \land x \geq 0 \}; \right. \]

\[ \text{if}(x = 0) v := -cv \left. \right)^* \right] 0 \leq x \leq H \]
\[ v \leq 0 \land 1 \geq c > 0 \land H = x \geq 0 \land g > 0 \rightarrow \left[ \{ x' = v, v' = -g \land x \geq 0 \}; \right. \]
\[ \text{if}(x = 0) v := -cv \right] 0 \leq x \leq H \]
Quantum the Acrophobic Bouncing Ball

\[ v \leq 0 \land 1 \geq c \geq 0 \land H = x \geq 0 \land g > 0 \rightarrow \begin{cases} \{ x' = v, v' = -g \land x \geq 0 \}; \\
\text{if}(x = 0) v := -cv \end{cases} \] 0 \leq x \leq H

Not if \( v \ll 0 \) initial dribbling
$$v = 0 \land 1 \geq c \geq 0 \land H = x \geq 0 \land g > 0 \rightarrow \left( \{ x' = v, v' = -g \land x \geq 0 \} ; \right.$$ 

$$\text{if}(x = 0) v := -cv \right)^* \left. \right\} 0 \leq x \leq H$$
Repeat control decisions

Example (Single car $\textit{cars}$)

$$((a := A \cup a := -b); \{x' = v, v' = a\})^*$$
Ex: Car Control Programs

How does this model brake?

Example (Single car $\text{car}_s$)

\[
\left( (a := A \cup a := -b); \{x' = v, v' = a\} \right)^* 
\]
Ex: Car Control Programs

Velocity bound $v \geq 0$ in evolution domain

Example (Single car $car_s$)

$$((( a := A \cup a := -b); \{x' = v, v' = a \& v \geq 0\})^*$$
Ex: Car Control Programs

Acceleration not always safe

Example (Single car $\text{car}_s$)

\[
((a := A \cup a := -b); \{x' = v, v' = a \& v \geq 0\})^*\]
Ex: Car Control Programs

Acceleration condition $Q$

Example (Single car $car_s$)

$((Q, a := A) \cup a := -b); \{x' = v, v' = a \& v \geq 0\})^*$

\[ a \]
\[ v \]
\[ x \]

\[ m \]
Ex: Car Control Properties

\[ Q \equiv \]

Example (Single car \( \text{car}_\varepsilon \) time-triggered)

\[
(((?Q; a := A) \cup a := -b); t := 0; \{ x' = v, v' = a, t' = 1 & v \geq 0 \land t \leq \varepsilon \})^* 
\]

Example (\( \text{Safely stays before traffic light } m \))

\[
A \geq 0 \land b > 0 \rightarrow [\text{car}_\varepsilon] x \leq m 
\]
Example (Single car $\text{car}_\varepsilon$ time-triggered)

$$((?Q; a := A) \cup a := -b); t := 0; \{x' = v, v' = a, t' = 1 \land v \geq 0 \land t \leq \varepsilon\})^*$$

Example (Safely stays before traffic light $m$)

$$v^2 \leq 2b(m - x) \land A \geq 0 \land b > 0 \rightarrow [\text{car}_\varepsilon] x \leq m$$
Ex: Car Control Properties

\[ Q \equiv 2b(m - x) \geq v^2 + (A + b)(A\varepsilon^2 + 2\varepsilon v) \]

Example (Single car \( \text{car}_\varepsilon \) time-triggered)

\[ (((?Q; a := A) \cup a := -b); t := 0; \{ x' = v, v' = a, t' = 1 \land v \geq 0 \land t \leq \varepsilon \})^* \]

Example (Safety stays before traffic light \( m \))

\[ v^2 \leq 2b(m - x) \land A \geq 0 \land b > 0 \rightarrow [\text{car}_\varepsilon] x \leq m \]
Ex: Car Control Properties

\[ Q \equiv 2b(m - x) \geq v^2 + (A + b)(A\epsilon^2 + 2\epsilon v) \]

Example (Single car \( \text{car}_\epsilon \) time-triggered)

\[
(((?Q; a := A) \cup a := -b); t := 0; \{x' = v, v' = a, t' = 1 \& v \geq 0 \& t \leq \epsilon\})^* 
\]

Example (Live, can move everywhere)

\[ \epsilon > 0 \land A > 0 \land b > 0 \rightarrow \forall p \exists m \langle \text{car}_\epsilon \rangle x \geq p \]
Example (dL-based model-predictive control design)

\[
\begin{align*}
\land v \geq 0 \land A \geq 0 \land b > 0 & \Rightarrow \\
(( & )
\end{align*}
\]

\[
\begin{align*}
a & := A) \\
\cup a & := -b); \\
t & := 0; \{x' = v, v' = a, t' = 1 & \land v \geq 0 \land t \leq \varepsilon\}^* \} x \leq m
\end{align*}
\]
Example (dL-based model-predictive control design)

\[
??? \quad \land v \geq 0 \land A \geq 0 \land b > 0 \rightarrow \\
[(\(?

(?

a := A) \\
\cup a := -b); \\
t := 0; \{x' = v, v' = a, t' = 1 \land v \geq 0 \land t \leq \varepsilon \})^* \] x \leq m
Example (dL-based model-predictive control design)

\[ x' = v, v' = -b \] \( x \leq m \) \( \land v \geq 0 \) \( \land A \geq 0 \) \( \land b > 0 \) \( \rightarrow \)

\[ (((
(?
(a := A);
\cup a := -b);
\{ x' = v, v' = a, t' = 1 \& v \geq 0 \& t \leq \epsilon \})^*) \] \( x \leq m \)
Example (dL-based model-predictive control design)

\[ x' = v, v' = -b \] 
\[ x \leq m \land v \geq 0 \land A \geq 0 \land b > 0 \rightarrow \]

\[
[((
?? \quad ???
\quad ;
\quad a := A)
\quad \cup a := -b); \\
\quad t := 0; \{x' = v, v' = a, t' = 1 \land v \geq 0 \land t \leq \varepsilon\}^*] x \leq m
\]
Example (dL-based model-predictive control design)

\[
\begin{align*}
  [x' = v, v' = -b]x \leq m \land v \geq 0 \land A \geq 0 \land b > 0 \rightarrow \\
  \left[ \left( \\
    [t := 0; x' = v, v' = A, t' = 1 \land v \geq 0 \land t \leq \varepsilon] [x' = v, v' = -b] x \leq m \\
    a := A \\
    \cup a := -b \\
    t := 0; \{x' = v, v' = a, t' = 1 \land v \geq 0 \land t \leq \varepsilon\}^* \right) \right] x \leq m
\end{align*}
\]
Example (dL-based model-predictive control design)

\[ [x' = v, v' = -b]x \leq m \land v \geq 0 \land A \geq 0 \land b > 0 \rightarrow \]

\[ (((
(?[t := 0; x' = v, v' = A, t' = 1 \& v \geq 0 \land t \leq \varepsilon][x' = v, v' = -b]x \leq m \land t' = 1 \& v \geq 0 \land t \leq \varepsilon)^* ) x \leq m) \]

\[ a := A \]

\[ \cup a := -b \);

\[ t := 0; \{x' = v, v' = a, t' = 1 \& v \geq 0 \land t \leq \varepsilon\}^* ] x \leq m \]
Example (dL-based model-predictive control design)

\[ v^2 \leq 2b(m-x) \land v \geq 0 \land A \geq 0 \land b > 0 \rightarrow \]

\[
\left( \left( [t:=0; x' = v, v' = A, t' = 1 \land v \geq 0 \land t \leq \epsilon] [x' = v, v' = -b] x \leq m \right) ;
\right.

\[ a := A \)

\[ \cup a := -b \right) ;

\[ t := 0; \{ x' = v, v' = a, t' = 1 \land v \geq 0 \land t \leq \epsilon \}^* \right) x \leq m \]
Ex: Car Control Design

Example (dL-based model-predictive control design)

\[ v^2 \leq 2b(m-x) \land v \geq 0 \land A \geq 0 \land b > 0 \rightarrow \\
\left[ \left( \left( \\
{[t:=0; x'=v, v'=A, t' = 1 \land v \geq 0 \land t \leq \epsilon][x'=v, v'=b]x \leq m \right) \cup a:=A \right) \right] \]

\[ t:=0; \ \{ x'=v, v'=a, t' = 1 \land v \geq 0 \land t \leq \epsilon \}^* \] \ x \leq m
Example (▶ dL-based model-predictive control design)

\[
\begin{align*}
\nu^2 &\leq 2b(m-x) \land \nu \geq 0 \land A \geq 0 \land b > 0 \rightarrow \\
\left( (2b(m-x) \geq \nu^2 + (A+b)(A\epsilon^2 + 2\epsilon\nu) \right) ; \\
\mu a := A) \\
\cup a := -b) \\
t := 0; \{x' = \nu, \nu' = a, t' = 1 \land \nu \geq 0 \land t \leq \epsilon\}^* \right] x \leq m
\end{align*}
\]
Runaround Robot with Dubins Paths

$\omega(x, y)$

Example (Runaround Robot)

$(x, y) \neq o \rightarrow \left\{ \omega := -1 \cup \omega := 1 \cup \omega := 0 ; 
\begin{align*}
  x' &= v, \\
  y' &= w, \\
  v' &= \omega w, \\
  w' &= -\omega v
\end{align*} \right\}^*$

André Platzer (CMU)
Programming Cyber-Physical Systems With Logic

POPL'19 28 / 66
Example (Runaround Robot)

\[
((\omega := -1 \cup \omega := 1 \cup \omega := 0); \\
\{x' = v, y' = w, v' = \omega w, w' = -\omega v\})^*
\]
Example (Runaround Robot)

\[(x, y) \neq o \rightarrow \left( (\omega := -1 \cup \omega := 1 \cup \omega := 0); \right. \]
\[\{ x' = v, y' = w, v' = \omega w, w' = -\omega v \} \left. \right\}^* \right) (x, y) \neq o\]
Example (Runaround Robot)

\[(x, y) \neq o \rightarrow \left( \left( ?Q_{-1}; \omega := -1 \cup ?Q_1; \omega := 1 \cup ?Q_0; \omega := 0 \right); \{x' = v, y' = w, v' = \omega w, w' = -\omega v \} \right)^* \right) (x, y) \neq o\]
Outline (Proving CPS)

1. CPS are Multi-Dynamical Systems

2. CPS Programs
   - Syntax
   - Semantics
   - Examples

3. Differential Dynamic Logic
   - Syntax
   - Semantics
   - Example: Car Control Design

4. Dynamic Axioms for Dynamical Systems
   - Axiomatics
   - Safe CPS Programming & Proving in KeYmaera X

5. Differential Invariants for Differential Equations

6. Applications

7. Verified Compilation of CPS Programs

8. Summary
Differential Dynamic Logic: Axiomatization

\[ x := e \] \[ P(x) \leftrightarrow P(e) \]

\[ ? \] \[ ?Q] P \leftrightarrow (Q \rightarrow P) \]

\[ ' \] \[ x' = f(x) \] \[ P \leftrightarrow \forall t \geq 0 [x := y(t)] P \quad \text{(} y'(t) = f(y) \text{)} \]

\[ \cup \] \[ \alpha \cup \beta \] \[ P \leftrightarrow [\alpha]P \wedge [\beta]P \]

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

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

K \[ [\alpha](P \rightarrow Q) \rightarrow ([\alpha]P \rightarrow [\alpha]Q) \]

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

C \[ [\alpha^*]\forall v > 0 (P(v) \rightarrow \langle\alpha\rangle P(v - 1)) \rightarrow \forall v (P(v) \rightarrow \langle\alpha^*\rangle \exists v \leq 0 P(v)) \]
Dynamic Axioms for Dynamical Systems

\[ \text{[:=]} \ [x := e] p(x) \iff \]

\begin{tikzpicture}
    
    
    
    \end{tikzpicture}
\[ [:=] \; [x := e]p(x) \leftrightarrow p(e) \]
[:=] \([x := e]p(x) \iff p(e)\)

[\prime] \([x' = f(x)]p(x) \iff\)
Dynamic Axioms for Dynamical Systems

\[ \text{[:=]} \ [x := e]p(x) \leftrightarrow p(e) \]

\[ \text{[']} \ [x' = f(x)]p(x) \leftrightarrow [x := y(t)]p(x) \]
Dynamic Axioms for Dynamical Systems

\[ := \ [x := e] p(x) \leftrightarrow p(e) \]

\[ \prime \] \[ x' = f(x) \] \[ \forall t \geq 0 \ [x := y(t)] p(x) \]
Dynamic Axioms for Dynamical Systems

\[\begin{align*}
[&:] [x := e]p(x) &\leftrightarrow p(e) \\
['] [x' = f(x)]p(x) &\leftrightarrow \forall t \geq 0 [x := y(t)]p(x) \\
['] [x' = f(x) \& q(x)]p(x) &\leftrightarrow \forall t \geq 0 \left([x := y(t)]p(x)\right)
\end{align*}\]
Dynamic Axioms for Dynamical Systems

\[\begin{align*}
[=] & \quad [x := e]p(x) \leftrightarrow p(e) \\
[\prime] & \quad [x' = f(x)]p(x) \leftrightarrow \forall t \geq 0 [x := y(t)]p(x) \\
[\prime] & \quad [x' = f(x) \& q(x)]p(x) \leftrightarrow \forall t \geq 0 (\forall 0 \leq s \leq t q(y(s)) \rightarrow [x := y(t)]p(x))
\end{align*}\]
Dynamic Axioms for Dynamical Systems

\[ \text{[:=]} \ [x := e]p(x) \leftrightarrow p(e) \]

\[ \text{['] } [x' = f(x)]p(x) \leftrightarrow \forall t \geq 0 [x := y(t)]p(x) \]

\[ \text{['] } [x' = f(x) \& q(x)]p(x) \leftrightarrow \forall t \geq 0 (\forall 0 \leq s \leq t q(y(s)) \rightarrow [x := y(t)]p(x)) \]

\[ \text{[?] } [? Q] P \leftrightarrow \]

if \( \omega \in \llbracket Q \rrbracket \)
Dynamic Axioms for Dynamical Systems

\[
\begin{align*}
[\!:=\!] & \quad [x := e] p(x) \leftrightarrow p(e) \\
[\!'] & \quad [x' = f(x)] p(x) \leftrightarrow \forall t \geq 0 [x := y(t)] p(x) \\
[\!''] & \quad [x' = f(x) \& q(x)] p(x) \leftrightarrow \forall t \geq 0 \left( \forall 0 \leq s \leq t q(y(s)) \rightarrow [x := y(t)] p(x) \right) \\
[?] & \quad [?Q] P \leftrightarrow (Q \rightarrow P) \\
\end{align*}
\]
Dynamic Axioms for Dynamical Systems

compositional semantics $\Rightarrow$ compositional proofs
\[[\bigcup] \ [\alpha \cup \beta] P \leftrightarrow \]
\[ \bigcup \ [\alpha \cup \beta] P \leftrightarrow [\alpha] P \land [\beta] P \]
Dynamic Axioms for Dynamical Systems

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

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

\[ P \]
[∪] [α ∪ β]P ↔ [α]P ∧ [β]P

[;] [α; β]P ↔ [α][β]P
Dynamic Axioms for Dynamical Systems

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

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

\[ ^* \ [\alpha^*]P \leftrightarrow \]
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
\[ \text{[\text{\cup}] } [\alpha \cup \beta]P \iff [\alpha]P \land [\beta]P \]

\[ \text{[;]} [\alpha; \beta]P \iff [\alpha][\beta]P \]

\[ \text{[\text{\lnot}] } [\alpha^*]P \iff P \land \]

\[ [\alpha^*]P \iff P \land \]
Dynamic Axioms for Dynamical Systems

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

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

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

\[ P \rightarrow [\alpha]P \]
Dynamic Axioms for Dynamical Systems

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

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

\[ \cdot [\alpha^*]P \leftrightarrow P \land [\alpha^*](P \rightarrow [\alpha]P) \]
[∪] \([\alpha \cup \beta]P \leftrightarrow [\alpha]P \land [\beta]P\)

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

\(\vdash [\alpha^*]P \leftrightarrow P \land [\alpha^*](P \rightarrow [\alpha]P)\)
Dynamic Axioms for Dynamical Systems

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

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

\[ ! \ [\alpha^*]P \leftrightarrow P \land [\alpha^*](P \rightarrow [\alpha]P) \]
Dynamic Axioms for Dynamical Systems

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

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

$[;] [\alpha*]P \leftrightarrow P \land [\alpha^*](P \rightarrow [\alpha]P)$
Dynamic Axioms for Dynamical Systems

\[
\bigcup (a \cup b) P \leftrightarrow [a]P \land [b]P
\]

\[
; (a; b) P \leftrightarrow [a][b]P
\]

\[\mathcal{I} \quad [a^*]P \leftrightarrow P \land [a^*](P \rightarrow [a]P)\]
Dynamic Axioms for Dynamical Systems

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

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

\[ \vdash [\alpha^*]P \leftrightarrow P \land [\alpha^*](P \rightarrow [\alpha]P) \]
Proof Rule: Loop Invariants

\[
\begin{align*}
G & \quad \frac{P}{[\alpha]P} \\
I & \quad \frac{[\alpha^*]P \leftrightarrow P \land [\alpha^*](P \rightarrow [\alpha]P)}{}
\end{align*}
\]

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

Lemma (Loop invariant rule is derived)

\[
\frac{
\begin{array}{c}
\Gamma \vdash J, \Delta \\
J \vdash [\alpha]J \\
J \vdash P
\end{array}
}{
\Gamma \vdash [\alpha^*]P, \Delta
}\]

Finding invariant \(J\) can be a challenge. Misplaced \([\alpha^*]\) suggests that \(J\) needs to carry along info about \(\alpha^*\) history.

André Platzer (CMU) Programming Cyber-Physical Systems With Logic POPL'19 32 / 66
Proof Rule: Loop Invariants

\[
\begin{array}{c}
P \\
 \frac{\alpha \vdash P}{[\alpha]P}
\end{array}
\]

<table>
<thead>
<tr>
<th>G</th>
<th>[\alpha]P</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>[\alpha^<em>]P \leftrightarrow P \land [\alpha^</em>](P \rightarrow [\alpha]P)</td>
</tr>
<tr>
<td>M[\cdot]</td>
<td>\frac{P \rightarrow Q}{[\alpha]P \rightarrow [\alpha]Q}</td>
</tr>
</tbody>
</table>

Lemma (Loop invariant rule is derived)

\[
\begin{array}{c}
\Gamma \vdash J, \Delta \\
\frac{J \vdash [\alpha]J \quad J \vdash P}{\Gamma \vdash [\alpha^*]P, \Delta}
\end{array}
\]

Proof (Derived rule).

\[
\begin{array}{c}
\Gamma \vdash J, \Delta \\
\frac{J \vdash [\alpha]J}{G} \\
\frac{J \vdash J \land [\alpha^*](J \rightarrow [\alpha]J)}{I} \\
\frac{J \vdash [\alpha^*]J}{M[\cdot]} \\
\frac{J \vdash P}{ \frac{J \vdash [\alpha^*]J}{\frac{\Gamma \vdash J, \Delta}{[\alpha^*]J \vdash [\alpha^*]P}}}
\end{array}
\]

Finding invariant \(J\) can be challenging. Misplaced \([\alpha^*]\) suggests that \(J\) needs to carry along info about \(\alpha^*\) history.
Proof Rule: Loop Invariants

\[
\frac{P}{G \vdash [\alpha]P}
\quad I \quad [\alpha^*]P \leftrightarrow P \land [\alpha^*](P \to [\alpha]P)
\quad M[\cdot] \quad \frac{P \to Q}{[\alpha]P \to [\alpha]Q}
\]

Lemma (Loop invariant rule is derived)

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

Proof (Derived rule).

\[
\frac{J \vdash [\alpha]J}{G \vdash J \land [\alpha^*](J \to [\alpha]J)}
\quad I \quad \frac{J \vdash [\alpha^*]J}{\Gamma \vdash J, \Delta}
\quad \frac{J \vdash P}{\Gamma \vdash [\alpha^*]P, \Delta}
\]

Finding invariant \( J \) can be a challenge. Misplaced \([\alpha^*]\) suggests that \( J \) needs to carry along info about \( \alpha^* \) history.
\( v = 0 \land 1 \geq c \geq 0 \land H = x \geq 0 \land g > 0 \rightarrow \left[ \{ x' = v, v' = -g \land x \geq 0 \}; \right.
\]
\[
\text{if}(x = 0) v := -cv \left] \right. 0 \leq x \leq H
\]
A ⊢ [(grav; (?x=0; v:=−cv) ∪ ?x≠0)) *]B(x,v)

A ≜ 0 ≤ x ∧ x = H ∧ v = 0 ∧ g > 0 ∧ 1 ≥ c ≥ 0

B(x,v) ≜ 0 ≤ x ∧ x ≤ H

grav ≜ \{ x' = v, v' = −g & x ≥ 0 \}
\[
\frac{A \vdash j(x, v)}{\text{loop}}
\]

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

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

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

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

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

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

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

\[ A \vdash j(x,v) \]

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

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

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

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

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

$\left[=\right]$

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

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

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

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

$[?], \rightarrow_{R}$

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

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

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

$\frac{j(x, v) \vdash [?x = 0; v := -cv \cup ?x \neq 0]j(x, v)}{\frac{j(x, v) \vdash [?x = 0; v := -cv]j(x, v) \quad [\cup] \quad j(x, v) \vdash [?x \neq 0]j(x, v)}{j(x, v) \vdash [?x = 0; v := -cv \cup ?x \neq 0]j(x, v)}}$
A ⊢ j(x,ν)  
j(x,ν) ⊢ [grav](j(x,ν))  
j(x,ν), x=0 ⊢ j(x,(−cv))  
j(x,ν), x≠0 ⊢ j(x,ν)  
j(x,ν) ⊢ B(x,ν)

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

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

\[ \text{grav} \equiv \{ x' = \nu, \nu' = -g \land x \geq 0 \} \]
0 ≤ x ∧ x = H ∧ v = 0 ∧ g > 0 ∧ 1 ≥ c ≥ 0 ⊢ j(x, v)

j(x, v) ⊢ [\{x' = v, v' = -g & x ≥ 0\}](j(x, v))

j(x, v), x = 0 ⊢ j(x, (-c v))

j(x, v), x ≠ 0 ⊢ j(x, v)

j(x, v) ⊢ 0 ≤ x ∧ x ≤ H

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

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

grav \equiv \{x' = v, v' = -g & x \geq 0\}
\(0 \leq x \land x = H \land v = 0 \land g > 0 \land 1 \geq c \geq 0\) ⊨ \(j(x,v)\)

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

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

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

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

\(\frac{2}{2}\)

\(j(x,v) \equiv 0 \leq x \land x \leq H\)

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

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

\(\text{grav} \equiv \{ x' = v, v' = -g \& x \geq 0 \}\)
0 ≤ x ∧ x = H ∧ v = 0 ∧ g > 0 ∧ 1 ≥ c ≥ 0 ⊢ j(x,v)

\[ j(x,v) ⊢ [\{x' = v, v' = -g & x ≥ 0\}] (j(x,v)) \]

\[ j(x,v), x = 0 ⊢ j(x,(-c)v) \]

\[ j(x,v), x ≠ 0 ⊢ j(x,v) \]

\[ j(x,v) ⊢ 0 ≤ x ∧ x ≤ H \]

\[ j(x,v) ≡ 0 ≤ x ∧ x ≤ H \]

weak: fails ODE if \( v \gg 0 \)

\[ A ≡ 0 ≤ x ∧ x = H ∧ v = 0 ∧ g > 0 ∧ 1 ≥ c ≥ 0 \]

\[ B(x,v) ≡ 0 ≤ x ∧ x ≤ H \]

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

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

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

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

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

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

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

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

grav \equiv \{x' = v, v' = -g \land x \geq 0\}
0 ≤ x ∧ x = H ∧ v = 0 ∧ g > 0 ∧ 1 ≥ c ≥ 0 ⊢ j(x,v)

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

j(x,v), x=0 ⊢ j(x,(-cv))

j(x,v), x≠0 ⊢ j(x,v)

j(x,v) ⊢ 0 ≤ x ∧ x ≤ H

1. j(x,v) ≡ x ≥ 0  weaker: fails postcondition if x > H
2. j(x,v) ≡ 0 ≤ x ∧ x ≤ H  weak: fails ODE if v ≫ 0

\[
A ≡ 0 ≤ x ∧ x = H ∧ v = 0 ∧ g > 0 ∧ 1 ≥ c ≥ 0
\]

B(x,v) ≡ 0 ≤ x ∧ x ≤ H

grav ≡ \{x' = v, v' = -g \& x ≥ 0\}
Proving Quantum the Acrophobic Bouncing Ball

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

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

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

\[ j(x,v), x \neq 0 \vdash j(x,v) \]

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

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

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

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

\[ \text{grav} \equiv \{x' = v, v' = -g \land x \geq 0\} \]
Proving Quantum the Acrophobic Bouncing Ball

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

1. \( j(x,v) \equiv x \geq 0 \) weaker: fails postcondition if \( x > H \)
2. \( j(x,v) \equiv 0 \leq x \land x \leq H \) weak: fails ODE if \( v \gg 0 \)
3. \( j(x,v) \equiv x = 0 \land v = 0 \) strong: fails initial condition if \( x > 0 \)

\[ A \equiv 0 \leq x \land x = H \land v = 0 \land g > 0 \land 1 \geq c \geq 0 \]
\[ B(x,v) \equiv 0 \leq x \land x \leq H \]
\[ \text{grav} \equiv \{ x' = v, v' = -g \land x \geq 0 \} \]
\( 0 \leq x \land x = H \land v = 0 \land g > 0 \land 1 \geq c \geq 0 \vdash j(x,v) \)
\( j(x,v) \vdash [\{ x' = v, v' = -g \land x \geq 0 \}] (j(x,v)) \)
\( j(x,v), x = 0 \vdash j(x,(-cv)) \)
\( j(x,v), x \neq 0 \vdash j(x,v) \)
\( j(x,v) \vdash 0 \leq x \land x \leq H \)

1. \( j(x,v) \equiv x \geq 0 \) weaker: fails postcondition if \( x > H \)
2. \( j(x,v) \equiv 0 \leq x \land x \leq H \) weak: fails ODE if \( v \gg 0 \)
3. \( j(x,v) \equiv x = 0 \land v = 0 \) strong: fails initial condition if \( x > 0 \)
4. \( j(x,v) \equiv x = 0 \lor x = H \land v = 0 \)

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

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

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

\[ j(x,v), x \neq 0 \vdash j(x,v) \]

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

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

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

\[ \text{grav} \equiv \{ x' = v, v' = -g \land x \geq 0 \} \]

1. \[ j(x,v) \equiv x \geq 0 \] weaker: fails postcondition if \( x > H \)
2. \[ j(x,v) \equiv 0 \leq x \land x \leq H \] weak: fails ODE if \( v \gg 0 \)
3. \[ j(x,v) \equiv x = 0 \land v = 0 \] strong: fails initial condition if \( x > 0 \)
4. \[ j(x,v) \equiv x = 0 \lor x = H \land v = 0 \] no space for intermediate states
Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

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

\[
A \equiv 0 \leq x \land x = H \land v = 0 \land g > 0 \land 1 \geq c \geq 0
\]
\[ B(x,v) \equiv 0 \leq x \land x \leq H \]
\[ \text{grav} \equiv \{ x' = v, v' = -g \land x \geq 0 \} \]
Proving Quantum the Acrophobic Bouncing Ball

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

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

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

\[ j(x,v), x\neq 0 \vdash j(x,v) \]

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

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

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

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

\[ \text{grav} \equiv \{ x' = v, v' = -g \land x \geq 0 \} \]
Proving Quantum the Acrophobic Bouncing Ball

\[ 0 \leq x \land x = H \land v = 0 \land g > 0 \land 1 \geq c \geq 0 \vdash 2gx = 2gH - v^2 \land x \geq 0 \]

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

\[ 2gx = 2gH - v^2 \land x \geq 0, x = 0 \vdash 2gx = 2gH - (-cv)^2 \land x \geq 0 \]

\[ 2gx = 2gH - v^2 \land x \geq 0, x \neq 0 \vdash 2gx = 2gH - v^2 \land x \geq 0 \]

\[ 2gx = 2gH - v^2 \land x \geq 0 \vdash 0 \leq x \land x \leq H \]

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

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

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

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

5. \( j(x, v) \equiv 2gx = 2gH - v^2 \land x \geq 0 \)
   works: implicitly links \( v \) and \( x \)
Proving Quantum the Acrophobic Bouncing Ball

\[ 0 \leq x \land x = H \land v = 0 \land g > 0 \land 1 \geq c \geq 0 \vdash 2gx = 2gH - v^2 \land x \geq 0 \]

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

\[ 2gx = 2gH - v^2 \land x \geq 0, x = 0 \vdash 2gx = 2gH - (-cv)^2 \land x \geq 0 \]

\[ 2gx = 2gH - v^2 \land x \geq 0, x \neq 0 \vdash 2gx = 2gH - v^2 \land x \geq 0 \]

\[ 2gx = 2gH - v^2 \land x \geq 0 \vdash 0 \leq x \land x \leq H \]

\[ j(x,v) \equiv x \geq 0 \quad \text{weaker: fails postcondition if } x > H \]

\[ j(x,v) \equiv 0 \leq x \land x \leq H \quad \text{weak: fails ODE if } v \gg 0 \]

\[ j(x,v) \equiv x = 0 \land v = 0 \quad \text{strong: fails initial condition if } x > 0 \]

\[ j(x,v) \equiv x = 0 \lor x = H \land v = 0 \quad \text{no space for intermediate states} \]

\[ j(x,v) \equiv 2gx = 2gH - v^2 \land x \geq 0 \quad \text{works: implicitly links } v \text{ and } x \]
0 ≤ x ∧ x = H ∧ v = 0 ∧ g > 0 ∧ 1 ≥ c ≥ 0 ⊢ 2gx = 2gH − v^2 ∧ x ≥ 0
2gx = 2gH − v^2 ∧ x ≥ 0 ⊢ [x' = v, v' = −g & x ≥ 0](2gx = 2gH − v^2 ∧ x ≥ 0)
✓ 2gx = 2gH − v^2 ∧ x ≥ 0, x = 0 ⊢ 2gx = 2gH − (−cv)^2 ∧ x ≥ 0 if c = 1…
2gx = 2gH − v^2 ∧ x ≥ 0, x ≠ 0 ⊢ 2gx = 2gH − v^2 ∧ x ≥ 0
2gx = 2gH − v^2 ∧ x ≥ 0 ⊢ 0 ≤ x ∧ x ≤ H

1. j(x, v) ≡ x ≥ 0 weaker: fails postcondition if x > H
2. j(x, v) ≡ 0 ≤ x ∧ x ≤ H weak: fails ODE if v ≫ 0
3. j(x, v) ≡ x = 0 ∧ v = 0 strong: fails initial condition if x > 0
4. j(x, v) ≡ x = 0 ∨ x = H ∧ v = 0 no space for intermediate states
5. j(x, v) ≡ 2gx = 2gH − v^2 ∧ x ≥ 0 works: implicitly links v and x
Proving Quantum the Acrophobic Bouncing Ball

\[
0 \leq x \land x = H \land v = 0 \land g > 0 \land 1 \geq c \geq 0 \vdash 2gx=2gH−v^2 \land x \geq 0
\]
\[
2gx=2gH−v^2 \land x \geq 0 \vdash [\{x' = v, v' = −g \& x \geq 0\}](2gx=2gH−v^2 \land x \geq 0)
\]
\[
\checkmark \quad 2gx=2gH−v^2 \land x \geq 0, x=0 \vdash 2gx=2gH−(−cv)^2 \land x \geq 0 \quad \text{if } c = 1 \ldots
\]
\[
2gx=2gH−v^2 \land x \geq 0, x \neq 0 \vdash 2gx=2gH−v^2 \land x \geq 0
\]
\[
2gx=2gH−v^2 \land x \geq 0 \vdash 0 \leq x \land x \leq H
\]

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

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

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

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

5. \(j(x,v) \equiv 2gx=2gH−v^2 \land x \geq 0\)
   works: implicitly links \(v\) and \(x\)
Proving Quantum the Acrophobic Bouncing Ball

\[
0 \leq x \land x = H \land v = 0 \land g > 0 \land 1 \geq c \geq 0 \vdash 2gx = 2gH - v^2 \land x \geq 0
\]

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

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

✓ \[
2gx = 2gH - v^2 \land x \geq 0, x \neq 0 \vdash 2gx = 2gH - v^2 \land x \geq 0
\]

\[
2gx = 2gH - v^2 \land x \geq 0 \vdash 0 \leq x \land x \leq H
\]

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

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

\[2gx = 2gH - v^2 \land x \geq 0 \vdash 0 \leq x \land x \leq H\]

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

2gx = 2gH − v^2 ∧ x ≥ 0 ⊢ [\{x' = v, v' = -g & x ≥ 0\}](2gx = 2gH − v^2 ∧ x ≥ 0)

✓ 2gx = 2gH − v^2 ∧ x ≥ 0, x=0 ⊢ 2gx = 2gH − (−cv)^2 ∧ x ≥ 0  if c = 1 ...

✓ 2gx = 2gH − v^2 ∧ x ≥ 0, x ≠ 0 ⊢ 2gx = 2gH − v^2 ∧ x ≥ 0

✓ 2gx = 2gH − v^2 ∧ x ≥ 0 ⊢ 0 ≤ x ∧ x ≤ H  because g > 0

1. j(x,v) ≡ x ≥ 0  weaker: fails postcondition if x > H

2. j(x,v) ≡ 0 ≤ x ∧ x ≤ H  weak: fails ODE if v ≫ 0

3. j(x,v) ≡ x = 0 ∧ v = 0  strong: fails initial condition if x > 0

4. j(x,v) ≡ x = 0 ∨ x = H ∧ v = 0  no space for intermediate states

5. j(x,v) ≡ 2gx = 2gH − v^2 ∧ x ≥ 0  works: implicitly links v and x
0 ≤ x ∧ x = H ∧ v = 0 ∧ g > 0 ∧ 1 ≥ c ≥ 0 ⊢ 2gx = 2gH − v^2 ∧ x ≥ 0

2gx = 2gH − v^2 ∧ x ≥ 0 ⊢ [\{x' = v, v' = −g & x ≥ 0\}] (2gx = 2gH − v^2 ∧ x ≥ 0)

✓ 2gx = 2gH − v^2 ∧ x ≥ 0, x = 0 ⊢ 2gx = 2gH − (−cv)^2 ∧ x ≥ 0 if c = 1 ...

✓ 2gx = 2gH − v^2 ∧ x ≥ 0, x ≠ 0 ⊢ 2gx = 2gH − v^2 ∧ x ≥ 0

✓ 2gx = 2gH − v^2 ∧ x ≥ 0 ⊢ 0 ≤ x ∧ x ≤ H because g > 0

1. j(x, v) ≡ x ≥ 0 weaker: fails postcondition if x > H
2. j(x, v) ≡ 0 ≤ x ∧ x ≤ H weak: fails ODE if v ≫ 0
3. j(x, v) ≡ x = 0 ∧ v = 0 strong: fails initial condition if x > 0
4. j(x, v) ≡ x = 0 ∨ x = H ∧ v = 0 no space for intermediate states
5. j(x, v) ≡ 2gx = 2gH − v^2 ∧ x ≥ 0 works: implicitly links v and x
Proving Quantum the Acrophobic Bouncing Ball

\[ 0 \leq x \land x = H \land v = 0 \land g > 0 \land 1 \geq c \geq 0 \vdash 2gx = 2gH - v^2 \land x \geq 0 \]

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

\[ 2gx = 2gH - v^2 \land x \geq 0, x = 0 \vdash 2gx = 2gH - (-cv)^2 \land x \geq 0 \quad \text{if } c = 1 \ldots \]

\[ 2gx = 2gH - v^2 \land x \geq 0, x \neq 0 \vdash 2gx = 2gH - v^2 \land x \geq 0 \]

\[ 2gx = 2gH - v^2 \land x \geq 0 \vdash 0 \leq x \land x \leq H \quad \text{because } g > 0 \]

1. \( j(x, v) \equiv x \geq 0 \) \quad \text{weaker: fails postcondition if } x > H

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

3. \( j(x, v) \equiv x = 0 \land v = 0 \) \quad \text{strong: fails initial condition if } x > 0

4. \( j(x, v) \equiv x = 0 \lor x = H \land v = 0 \) \quad \text{no space for intermediate states}

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

\[ x(t) = H - \frac{g}{2} t^2 \]

\[ v(t) = -gt \]
Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

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

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

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

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

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

$x(t) = H - \frac{g}{2}t^2 \leadsto 2gx(t) = 2gH - g^2t^2 \quad v(t)^2 = g^2t^2 \leadsto v(t) = -gt$
Quantum the Acrophobic Bouncing Ball

Example (Bouncing Ball)

\[ v = 0 \land 1 \geq c \geq 0 \land H = x \geq 0 \land g > 0 \rightarrow \left[ \left( \{ x' = v, v' = -g \land x \geq 0 \} ; \right. \right. \]
\[ \left. \left. \text{if}(x = 0) v := -cv \right) ^* \right] 0 \leq x \leq H \]
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**
Example (Runaround Robot)

\[(x, y) \neq o \rightarrow \left[ ((Q_{-1}; \omega=-1 \cup \omega = 1 \cup Q_0; \omega=0); \right.
\left. \{x' = v, y' = w, v' = \omega w, w' = -\omega v \})^* \right] (x, y) \neq o\]
Runaround Robot with Dubins Paths

\[ Q_\omega \equiv (x + \frac{w}{\omega} - o_x)^2 + (y - \frac{v}{\omega} - o_y)^2 \neq (\frac{v}{\omega})^2 + (\frac{w}{\omega})^2 \]

\[ Q_0 \equiv (x - o_x)w \neq (y - o_y)v \]

1. Obstacle not on tangential circle
2. Obstacle not on ray \((x, y) + \mathbb{R}(v, w)\)

Example (Runaround Robot)

\((x, y) \neq o \rightarrow [((?Q_{\omega = -1} \cup ?Q_1; \omega := 1 \cup ?Q_0; \omega := 0); \\
\{x' = v, y' = w, v' = \omega w, w' = -\omega v\})^*] (x, y) \neq o\)
KeYmaera X aXiomatic Tactical Theorem Prover for CPS

Proof search

KeYmaera X

Model

ctrl: \( a := -b \);
plant: \( x'' = a \)

generates proofs

ModelPlex proof

Trustworthy
Uniform substitution
Sound & complete
Small core: 1700 LOC

Flexible
Proof automation
Interactive UI
Programmable

Customizable
Scala+Java API
Command line
REST API

Model Safety
Compliance Monitor
Disclaimer: Self-reported estimates of the soundness-critical lines of code + rules
Uniform Substitution

**Theorem (Soundness)**

`US` replace all occurrences of `p(·)`

\[
\begin{align*}
\text{US} & \quad \frac{\phi}{\sigma(\phi)} \\
\text{provided } & \quad \text{FV}(\sigma_{\Sigma(\theta)}) \cap \text{BV}(\otimes(\cdot)) = \emptyset \text{ for each operation } \otimes(\theta) \text{ in } \phi
\end{align*}
\]

i.e. bound variables `U = BV(\otimes(\cdot))` of operator `\otimes`

are not free in the substitution on its argument `\theta`  

(U-admissible)

\[
\begin{align*}
\text{US} & \quad \frac{[a \cup b]p(\bar{x}) \iff [a]p(\bar{x}) \land [b]p(\bar{x})}{[\text{x := x + 1} \cup x' = 1]x \geq 0 \iff [\text{x := x + 1}]x \geq 0 \land [x' = 1]x \geq 0}
\end{align*}
\]
Theorem (Soundness) replace all occurrences of \( p(\cdot) \)

\[
\begin{align*}
\text{US} & \quad \frac{\phi}{\sigma(\phi)} \\
\end{align*}
\]

provided \( FV(\sigma|\Sigma(\theta)) \cap BV(\otimes(\cdot)) = \emptyset \) for each operation \( \otimes(\theta) \) in \( \phi \)

i.e. bound variables \( U = BV(\otimes(\cdot)) \) of operator \( \otimes \) are not free in the substitution on its argument \( \theta \) \hspace{1cm} (U-admissible)

Uniform substitution \( \sigma \) replaces all occurrences of \( p(\theta) \) for any \( \theta \) by \( \psi(\theta) \)

function \( f(\theta) \) for any \( \theta \) by \( \eta(\theta) \)

quantifier \( C(\phi) \) for any \( \phi \) by \( \psi(\theta) \)

program const. \( a \) by \( \alpha \)

\[
\begin{align*}
\text{US} & \quad \frac{[a \cup b]p(\bar{x}) \leftrightarrow [a]p(\bar{x}) \land [b]p(\bar{x})}{[x := x + 1 \cup x' = 1]x \geq 0 \leftrightarrow [x := x + 1]x \geq 0 \land [x' = 1]x \geq 0}
\end{align*}
\]
Differential Equation Axiomatization

- Classical approach: ① Given ODE ② Solve ODE ③ Analyze solution
- Descriptive power of ODEs: ODE much easier than its solution
- Analyzing ODEs via their solutions undoes their descriptive power!

![Diagram showing describe ODE ↔ analyze ODE and describe solution ↔ analyze solution]

1. Logical foundations of differential equation invariants
2. Decide invariance by dL proof

Poincaré 1881

LICS’18

x'' = −x

has x(t) = sin(t) = t − \frac{t^3}{3!} + \frac{t^5}{5!} − \frac{t^7}{7!} + \frac{t^9}{9!} − \ldots

x''(t) = e^{t^2}

has no elementary closed-form solution
Properties of Differential Equations

Concept (Differential Dynamic Logic) (JAR’08, LICS’12)

\[ u'^2 \leq v'^2 + \frac{9}{2} \rightarrow [u' = -v + \frac{u}{4} (1 - u^2 - v^2), v' = u + \frac{v}{4} (1 - u^2 - v^2)] u'^2 \leq v'^2 + \frac{9}{2} \]

\[ u^2 + v^2 = 1 \rightarrow [u' = -v + \frac{u}{4} (1 - u^2 - v^2), \quad v' = u + \frac{v}{4} (1 - u^2 - v^2)] u^2 + v^2 = 1 \]
\textit{dL calculus is a sound & complete axiomatization of arithmetic invariants of differential equations. They are decidable with a derived axiom.}
**Theorem (Invariant Completeness) (LICS’18)**

\( dL \) calculus is a sound & complete axiomatization of arithmetic invariants of differential equations. They are decidable with a derived axiom.

**Theorem (Sound & Complete) (JAR’08, LICS’12, JAR’17)**

\( dL \) calculus is a sound & complete axiomatization of hybrid systems relative to either differential equations or to discrete dynamics.
Differential Invariants for Differential Equations

**Differential Invariant**

\[
x' = f(x) \land Q
\]

**Differential Cut**

\[
x' = f(x) \land Q
\]

**Differential Ghost**

\[
x' = f(x) \land Q
\]
Differential Invariants for Differential Equations

Differential Invariant

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

Differential Cut

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

Differential Ghost

\[ x' = f(x) \& Q \]
Differential Invariants for Differential Equations

Differential Invariant

Differential Cut

Differential Ghost

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

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

\[ x' = f(x) \& Q \]
Differential Invariants for Differential Equations

Differential Invariant

Differential Cut

Differential Ghost

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

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

\[ x' = f(x) & Q \]
### Differential Invariants for Differential Equations

<table>
<thead>
<tr>
<th>Differential Invariant</th>
<th>Differential Cut</th>
<th>Differential Ghost</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Differential Invariant" /></td>
<td><img src="image" alt="Differential Cut" /></td>
<td><img src="image" alt="Differential Ghost" /></td>
</tr>
</tbody>
</table>

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

- **Differential Invariant**
- **Differential Cut**
- **Differential Ghost**

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

- **André Platzer (CMU)**
- **Programming Cyber-Physical Systems With Logic**
- **POPL'19 45 / 66**
Differential Invariants for Differential Equations

Differential Invariant

\[ \begin{align*}
x' &= f(x) & Q \\
x &= u & w \\
r &= 0 & Q
\end{align*} \]

Differential Cut

\[ \begin{align*}
x' &= f(x) & Q \\
x &= u & w \\
r &= 0 & Q
\end{align*} \]

Differential Ghost

\[ \begin{align*}
x' &= f(x) & Q \\
x &= u & w \\
r &= 0 & Q
\end{align*} \]
Differential Invariants for Differential Equations

Differential Invariant

Differential Cut

Differential Ghost

\[ x' = f(x) \]

\[ y' = g(x, y) \]

\[ t \]

\[ x \]

\[ 0 \]

\[ x' = f(x) \]

\[ r \]

\[ Q \]

\[ w \]

\[ u \]

\[ 0 \]

\[ x' = f(x) \]

\[ r \]

\[ Q \]

\[ w \]

\[ u \]

\[ 0 \]

\[ x' = f(x) \]

\[ r \]

\[ Q \]

\[ u \]
<table>
<thead>
<tr>
<th>Differential Invariant</th>
<th>Differential Cut</th>
<th>Differential Ghost</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x' = f(x) &amp; Q$</td>
<td>$x' = f(x) &amp; Q$</td>
<td>$y' = g(x, y)$</td>
</tr>
</tbody>
</table>

André Platzer (CMU) Programming Cyber-Physical Systems With Logic

POPL'19 45 / 66
Differential Invariants for Differential Equations

**Differential Invariant**

\[
x' = f(x) \land Q
\]

**Differential Cut**

\[
x' = f(x) \land Q
\]

**Differential Ghost**

\[
y' = g(x, y)
\]
Differential Invariants for Differential Equations

**Differential Invariant**

\[ Q \vdash [x' := f(x)](P)' \]
\[ P \vdash [x' = f(x) \& Q]P \]

**Differential Cut**

\[ P \vdash [x' = f(x) \& Q]C \quad P \vdash [x' = f(x) \& Q \land C]P \]
\[ P \vdash [x' = f(x) \& Q]P \]

**Differential Ghost**

\[ P \leftrightarrow \exists y G \quad G \vdash [x' = f(x), y' = g(x, y) \& Q]G \]
\[ P \vdash [x' = f(x) \& Q]P \]

deductive power adds DI $\prec$ DC $\prec$ DG

JLogComput’10, LMCS’12, LICS’12, JAR’17, LICS’18
Differential Invariant for Differential Equations

**Differential Invariant**

\[ Q \vdash [x' := f(x)](P)' \]

\[ P \vdash [x' = f(x) \& Q]P \]

**Differential Cut**

\[ P \vdash [x' = f(x) \& Q]C \]

\[ P \vdash [x' = f(x) \& Q \land C]P \]

\[ P \vdash [x' = f(x) \& Q]P \]

**Differential Ghost**

\[ P \leftrightarrow \exists y G \]

\[ G \vdash [x' = f(x), y' = g(x, y) \& Q]G \]

\[ P \vdash [x' = f(x) \& Q]P \]

if new \( y' = g(x, y) \) has long enough solution

JLogComput’10, LMCS’12, LICS’12, JAR’17, LICS’18
$$\omega^2 x^2 + y^2 \leq c^2 \vdash [x' = y, y' = -\omega^2 x - 2d\omega y \& \omega \geq 0 \land d \geq 0] \omega^2 x^2 + y^2 \leq c^2$$
\[ \omega^2 x^2 + y^2 \leq c^2 \vdash [x' = y, y' = -\omega^2 x - 2d \omega y & \omega \geq 0 \land d \geq 0] \] \[ \omega^2 x^2 + y^2 \leq c^2 \]

damped oscillator
$\omega \geq 0 \land d \geq 0 \vdash [x' := y][y' := -\omega^2 x - 2d \omega y] 2\omega^2 xx' + 2yy' \leq 0$

$\omega^2 x^2 + y^2 \leq c^2 \vdash [x' = y, y' = -\omega^2 x - 2d \omega y \land \omega \geq 0 \land d \geq 0] \omega^2 x^2 + y^2 \leq c^2$

damped oscillator
\[
\omega \geq 0 \land d \geq 0 \vdash 2 \omega^2 xy + 2y(-\omega^2 x - 2d \omega y) \leq 0
\]

\[
\omega \geq 0 \land d \geq 0 \vdash [x' := y][y' := -\omega^2 x - 2d \omega y] 2 \omega^2 xx' + 2yy' \leq 0
\]

\[
\omega^2 x^2 + y^2 \leq c^2 \vdash [x' = y, y' = -\omega^2 x - 2d \omega y \& \omega \geq 0 \land d \geq 0] \omega^2 x^2 + y^2 \leq c^2
\]

damped oscillator
Differential Invariants for Differential Equations

\[
\omega \geq 0 \land d \geq 0 \vdash 2\omega^2 xy + 2y(-\omega^2 x - 2d\omega y) \leq 0
\]

\[
\omega \geq 0 \land d \geq 0 \vdash [x' := y][y' := -\omega^2 x - 2d\omega y] 2\omega^2 xx' + 2yy' \leq 0
\]

\[
\omega^2 x^2 + y^2 \leq c^2 \vdash [x' = y, y' = -\omega^2 x - 2d\omega y & \omega \geq 0 \land d \geq 0] \omega^2 x^2 + y^2 \leq c^2
\]

damped oscillator
\[
\omega \geq 0 \land d \geq 0 \vdash 2 \omega^2 xy + 2y(-\omega^2 x - 2d\omega y) \leq 0
\]
\[
\omega \geq 0 \land d \geq 0 \vdash [x' := y][y' := -\omega^2 x - 2d\omega y] 2\omega^2 xx' + 2yy' \leq 0
\]
\[
\omega^2 x^2 + y^2 \leq c^2 \vdash [x' = y, y' = -\omega^2 x - 2d\omega y \& \omega \geq 0 \land d \geq 0] \omega^2 x^2 + y^2 \leq c^2
\]
\[ \omega^2 x^2 + y^2 \leq c^2 \vdash [x' = y, y' = -\omega^2 x - 2d \omega y, d' = 7 \land \omega \geq 0] \omega^2 x^2 + y^2 \leq c^2 \]
\begin{align*}
\omega^2 x^2 + y^2 &\leq c^2 \quad \vdash [x' = y, y' = -\omega^2 x - 2d \omega y, d' = 7 \land \omega \geq 0] \omega^2 x^2 + y^2 \leq c^2
\end{align*}

increasingly damped oscillator
\[ \omega^2 x^2 + y^2 \leq c^2 \vdash [x' = y, y' = -\omega^2 x - 2d \omega y, d' = 7 & \omega \geq 0 \land d \geq 0] \omega^2 x^2 + y^2 \leq c^2 \]

increasingly damped oscillator
\[
\omega^2 x^2 + y^2 \leq c^2 \vdash [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 & \omega \geq 0 & d \geq 0] \omega^2 x^2 + y^2 \leq c^2
\]

\[
\omega^2 x^2 + y^2 \leq c^2 \vdash [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 & \omega \geq 0] \omega^2 x^2 + y^2 \leq c^2
\]

\[
d \geq 0 \vdash [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 & \omega \geq 0] d \geq 0
\]

increasingly damped oscillator
\( \omega^2 x^2 + y^2 \leq c^2 \vdash [x' = y, y' = -\omega^2 x - 2d \omega y, d' = 7 \land \omega \geq 0 \land d \geq 0] \omega^2 x^2 + y^2 \leq c^2 \)

\( \omega^2 x^2 + y^2 \leq c^2 \vdash [x' = y, y' = -\omega^2 x - 2d \omega y, d' = 7 \land \omega \geq 0] \omega^2 x^2 + y^2 \leq c^2 \)

\[ \omega \geq 0 \vdash [d' := 7] d' \geq 0 \]

\[ d \geq 0 \vdash [x' = y, y' = -\omega^2 x - 2d \omega y, d' = 7 \land \omega \geq 0] d \geq 0 \]

increasingly damped oscillator
\( \omega^2 x^2 + y^2 \leq c^2 \vdash [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 & \omega \geq 0 \land d \geq 0] \omega^2 x^2 + y^2 \leq c^2 \)

\[ \omega \geq 0 \vdash 7 \geq 0 \]

\[ \omega \geq 0 \vdash [d' := 7] d' \geq 0 \]

\[ d \geq 0 \vdash [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 & \omega \geq 0] d \geq 0 \]

increasingly damped oscillator
\[ \omega^2 x^2 + y^2 \leq c^2 \vdash [x' = y, y' = -\omega^2 x - 2d \omega y, d' = 7 \& \omega \geq 0 \land d \geq 0] \omega^2 x^2 + y^2 \leq c^2 \]

\[ \omega^2 x^2 + y^2 \leq c^2 \vdash [x' = y, y' = -\omega^2 x - 2d \omega y, d' = 7 \& \omega \geq 0] \omega^2 x^2 + y^2 \leq c^2 \]

\[ \omega \geq 0 \vdash 7 \geq 0 \]

\[ \omega \geq 0 \vdash [d' := 7] d' \geq 0 \]

\[ d \geq 0 \vdash [x' = y, y' = -\omega^2 x - 2d \omega y, d' = 7 \& \omega \geq 0] d \geq 0 \]

increasingly damped oscillator
\( \omega \geq 0 \land d \geq 0 \vdash [x' := y, y' := -\omega^2 x - 2d \omega y] \omega^2 xx' + 2yy' \leq 0 \)

\( \omega^2 x^2 + y^2 \leq c^2 \vdash [x' = y, y' = -\omega^2 x - 2d \omega y, d' = 7 \land \omega \geq 0 \land d \geq 0] \omega^2 x^2 + y^2 \leq c^2 \)

\( \omega \geq 0 \vdash 7 \geq 0 \)

\( \omega \geq 0 \vdash [d' := 7] d' \geq 0 \)

\( d \geq 0 \vdash [x' = y, y' = -\omega^2 x - 2d \omega y, d' = 7 \land \omega \geq 0] d \geq 0 \)

increasingly damped oscillator
\( \omega \geq 0 \land d \geq 0 \vdash 2\omega^2 xy + 2y(-\omega^2 x - 2d\omega y) \leq 0 \)

\( \omega \geq 0 \land d \geq 0 \vdash [x' := y][y' := -\omega^2 x - 2d\omega y] 2\omega^2 xx' + 2yy' \leq 0 \)

\( \omega^2 x^2 + y^2 \leq c^2 \vdash [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 \land \omega \geq 0 \land d \geq 0] \omega^2 x^2 + y^2 \leq c^2 \)

\( \omega^2 x^2 + y^2 \leq c^2 \vdash [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 \land \omega \geq 0] \omega^2 x^2 + y^2 \leq c^2 \)

\( \omega \geq 0 \vdash 7 \geq 0 \)

\( \omega \geq 0 \vdash [d' := 7] d' \geq 0 \)

\( d \geq 0 \vdash [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 \land \omega \geq 0] d \geq 0 \)

increasingly damped oscillator
\[ \begin{align*}
\omega \geq 0 \land d \geq 0 \vdash & & 2\omega^2 xy + 2y(-\omega^2 x - 2d\omega y) \leq 0 \\
\omega \geq 0 \land d \geq 0 \vdash & & [x' := y] [y' := -\omega^2 x - 2d\omega y] \ 2\omega^2 xx' + 2yy' \leq 0 \\
\omega^2 x^2 + y^2 \leq c^2 \vdash & & [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 \land \omega \geq 0 \land d \geq 0] \ \omega^2 x^2 + y^2 \leq c^2 \\
\omega^2 x^2 + y^2 \leq c^2 \vdash & & [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 \land \omega \geq 0] \ \omega^2 x^2 + y^2 \leq c^2 \\
\omega \geq 0 \vdash & & 7 \geq 0 \\
\omega \geq 0 \vdash & & [d' := 7] \ d' \geq 0 \\
d \geq 0 \vdash & & [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 \land \omega \geq 0] \ d \geq 0
\end{align*} \]

increasingly damped oscillator
Differential Cuts for Differential Equations

\[
\omega \geq 0 \land d \geq 0 \vdash 2 \omega^2 xy + 2y(-\omega^2 x - 2d\omega y) \leq 0
\]

\[
\omega \geq 0 \land d \geq 0 \vdash [x' := y][y' := -\omega^2 x - 2d\omega y] 2\omega^2 xx' + 2yy' \leq 0
\]

\[
\omega^2 x^2 + y^2 \leq c^2 \vdash [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 \land \omega \geq 0 \land d \geq 0] \omega^2 x^2 + y^2 \leq c^2
\]

\[
\omega^2 x^2 + y^2 \leq c^2 \vdash [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 \land \omega \geq 0] \omega^2 x^2 + y^2 \leq c^2
\]

\[
\omega \geq 0 \vdash 7 \geq 0
\]

\[
\omega \geq 0 \vdash [d' := 7] d' \geq 0
\]

\[
d \geq 0 \vdash [x' = y, y' = -\omega^2 x - 2d\omega y, d' = 7 \land \omega \geq 0] d' \geq 0
\]

Could repeatedly diffcut in formulas to help the proof
Assuming Differential Invariance

\[ Q \vdash [x' := f(x)](F)' \]
\[ \frac{F \vdash [x' = f(x) & Q]F}{F \vdash [x' = f(x) & Q]F} \]

\[ F \land Q \vdash [x' := f(x)](F)' \]
\[ \frac{F \vdash [x' = f(x) & Q]F}{F \vdash [x' = f(x) & Q]F} \]
Assuming Differential Invariance

\[ Q \vdash [x' := f(x)](F)' \]

\[ F \vdash [x' = f(x) \& Q]F \]

\[ F \land Q \vdash [x' := f(x)](F)' \]

\[ F \vdash [x' = f(x) \& Q]F \]

Example (Inductive hypothesis)

\[ v^2 - 2v + 1 = 0 \vdash [v' = w, w' = -v]v^2 - 2v + 1 = 0 \]
Assuming Differential Invariance

\[ Q \vdash [x' := f(x)](F)' \]
\[ F \vdash [x' = f(x) \& Q]F \]

\[ F \land Q \vdash [x' := f(x)](F)' \]
\[ F \vdash [x' = f(x) \& Q]F \]

Example (Inductive hypothesis)

\[ v^2 - 2v + 1 = 0 \vdash [v' := w][w' := -v]2v v' - 2v' = 0 \]
\[ v^2 - 2v + 1 = 0 \vdash [v' = w, w' = -v]v^2 - 2v + 1 = 0 \]
Assuming Differential Invariance

\[ Q \vdash [x' := f(x)](F)' \]
\[ \frac{F \vdash [x' = f(x) \& Q]}{F \vdash [x' = f(x) \& Q]F} \]

Example (Inductive hypothesis)

\[ v^2 - 2v + 1 = 0 \vdash 2vw - 2w = 0 \]
\[ v^2 - 2v + 1 = 0 \vdash [v' := w][w' := -v]2vv' - 2v' = 0 \]
\[ v^2 - 2v + 1 = 0 \vdash [v' = w, w' = -v]v^2 - 2v + 1 = 0 \]
Assuming Differential Invariance

\[ \neg F \]

\[ Q \vdash [x' := f(x)](F)' \]

\[ F \vdash [x' = f(x) \& Q]F \]

\[ F \land Q \vdash [x' := f(x)](F)' \]

\[ F \vdash [x' = f(x) \& Q]F \]

Example (Inductive hypothesis is unsound!)

(unsound)

\[ v^2 - 2v + 1 = 0 \vdash 2vw - 2w = 0 \]

\[ v^2 - 2v + 1 = 0 \vdash [v' := w][w' := -v]2vv' - 2v' = 0 \]

\[ v^2 - 2v + 1 = 0 \vdash [v' = w, w' = -v]v^2 - 2v + 1 = 0 \]
ODE Axiomatization

Local coordinates: \( \frac{\dot{x}}{\dot{y}} \)

Proofs use continuously changing basis to keep invariants at constant local coordinates

Local coordinates: \( \frac{\dot{z}}{\dot{g}} \)

Proofs with higher Lie derivatives
- \( p'' \) safe
- \( p'' \) inconclusive
- \( p' \) inconclusive

Sound and complete ODE invariance proofs
Example (Parachute)
Example (Parachute)

\[
\left(\left(\left(Q \land r = a\right) \cup r := p\right); t := 0; \right.
\left.\{x' = v, v' = -g + rv^2, t' = 1 \land t \leq T \land x \geq 0 \land v < 0\}\right)^* 
\]
Ex: Parachute Open or Keep Closed

Conservatively bounded next velocity above parachute’s limit velocity.

Limit by differential ghost:

\[ y' = -p^2 (v - \sqrt{g / p}) y^2 (v + \sqrt{g / p}) \geq 0 \]

\[ v \geq v_{\text{old}} (v - gt) \text{ if closed} \]

Example (Parachute)

\[ \rightarrow \left[ \left( (Q \land r = a) \lor r := p \right); t := 0; \right. \]

\[ \{ x' = v, v' = -g + rv^2, t' = 1 & t \leq T \land x \geq 0 \land v < 0 \}^* \]

\[ (x = 0 \rightarrow v \geq m) \]
Ex: Parachute Open or Keep Closed

Conservatively bounded next velocity above parachute’s limit velocity.
Limit by differential ghost:
\[ y' = -p(v - \sqrt{g/p})y^2(v + \sqrt{g/p}) > 0 \]

\[ v \geq v_{\text{old}}(v) - gt \text{ if closed} \]

Example (Parachute)

\[ \rightarrow [( (\exists (Q \land r = a) \cup r := p); t := 0; \\
\{ x' = v, v' = -g + rv^2, t' = 1 & t \leq T \land x \geq 0 \land v < 0 \} )^* ] \]

\[ (x = 0 \rightarrow v \geq m) \]
Ex: Parachute Open or Keep Closed

\[ Q \equiv v - gT > -\sqrt{g/p} \]

Conservatively bounded next velocity above parachute’s limit velocity.

Example (Parachute)

\[ m < -\sqrt{g/p} \rightarrow \left[ \left( (Q \land r = a) \lor r := p \right) ; t := 0; \left\{ x' = v, v' = -g + rv^2, t' = 1 \land t \leq T \land x \geq 0 \land v < 0 \right\} \right]^* \]

\[ (x = 0 \rightarrow v \geq m) \]
$Q \equiv v - gT > -\sqrt{g/p}$

Conservatively bounded next velocity above parachute’s limit velocity. Limit by differential ghost:

\[ y' = -\frac{p}{2}(v - \sqrt{g/p}) \quad y^2(v + \sqrt{g/p}) = 1 \]

Example (Parachute)

\[
m < -\sqrt{g/p} \rightarrow \left( (\neg(Q \land r = a) \cup r := p) ; t := 0; \right.
\]
\[
\left. \{ x' = v, v' = -g + rv^2, t' = 1 \land t \leq T \land x \geq 0 \land v < 0 \} \right)^* \]
\[
(x = 0 \rightarrow v \geq m)
\]
Conservatively bounded next velocity above parachute’s limit velocity.

Limit by differential ghost:

\[ y' = -\frac{p}{2}(v - \sqrt{g/p}) \quad y^2(v + \sqrt{g/p}) > 0 \]

\[ v \geq \text{old}(v) - gt \text{ if closed} \]

**Example (Parachute)**

\[ m < -\sqrt{g/p} \rightarrow \left[ (\{(Q \land r = a) \lor r := p\}; t := 0; \left\{ x' = v, v' = -g + rv^2, t' = 1 \land t \leq T \land x \geq 0 \land v < 0 \right\})^* \right] \]

\[ (x = 0 \rightarrow v \geq m) \]
Outline (CPS Application Highlights)

1. CPS are Multi-Dynamical Systems
2. CPS Programs
   - Syntax
   - Semantics
   - Examples
3. Differential Dynamic Logic
   - Syntax
   - Semantics
   - Example: Car Control Design
4. Dynamic Axioms for Dynamical Systems
   - Axiomatics
   - Safe CPS Programming & Proving in KeYmaera X
5. Differential Invariants for Differential Equations
6. Applications
7. Verified Compilation of CPS Programs
8. Summary
Airborne Collision Avoidance System ACAS X: Verify

- Developed by the FAA to replace current TCAS in aircraft
- Approximately optimizes Markov Decision Process on a grid
- Advisory from lookup tables with numerous 5D interpolation regions

1. Identified safe region for each advisory symbolically
2. Proved safety for hybrid systems flight model in KeYmaera X
ACAS X table comparison shows safe advisory in 97.7% of the 648,591,384,375 states compared (15,160,434,734 counterexamples).

ACAS X issues DNC advisory, which induces collision unless corrected.
Airborne Collision Avoidance System ACAS X: Refine

- Conservative, so too many counterexamples
- Settle for: safe for a little while, with safe future advisory possibility
- Safeable advisory: a subsequent advisory can safely avoid collision

1. Identified safeable region for each advisory symbolically
2. Proved safety for hybrid systems flight model in KeYmaera X

STTT’17
ACAS X table comparison shows safeable advisory in more of the 648,591,384,375 states compared ($\approx 899 \times 10^6$ counterexamples).

**Counterexample:** Action Issued = Maintain
Followed by Most Extreme Up/Down-sense Advisory Available

ACAS X issues Maintain advisory instead of CL1500
ACAS X table comparison shows safeable advisory in more of the 648,591,384,375 states compared (≈899 $10^6$ counterexamples).

ACAS X issues Maintain advisory instead of CL1500

Safe Version: Action Issued = CL1500
Followed by Most Extreme Up/Down-sense Available
Ground Robot Obstacle Avoidance: Verify

- Fundamental safety question for ground robot navigation
- When will which control decision avoid obstacles?
- Depends on safety objective, physical capabilities of robot + obstacle

1. Identified safe region for each safety notion symbolically
2. Proved safety for hybrid systems ground robot model in KeYmaera X
Ground Robot Obstacle Avoidance: Verify

- Fundamental safety question for ground robot navigation
- When will which control decision avoid obstacles?
- Depends on safety objective, physical capabilities of robot + obstacle

1. Identified safe region for each safety notion symbolically
2. Proved safety for hybrid systems ground robot model in KeYmaera X

André Platzer (CMU)  Programming Cyber-Physical Systems With Logic

POPL’19  56 / 66
Fundamental safety question for ground robot navigation
When will which control decision avoid obstacles?
Depends on safety objective, physical capabilities of robot + obstacle

1. Identified safe region for each safety notion symbolically
2. Proved safety for hybrid systems ground robot model in KeYmaera X
Ground Robot Obstacle Avoidance: Verify

- Fundamental safety question for ground robot navigation
- When will which control decision avoid obstacles?
- Depends on safety objective, physical capabilities of robot + obstacle

<table>
<thead>
<tr>
<th>Acceleration</th>
<th>Speed</th>
<th>Time</th>
<th>Static</th>
<th>Passive</th>
<th>Orientation</th>
<th>Safety</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pass parking</td>
<td>Avoid/Follow</td>
<td>Head-on</td>
<td>Turn</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. Identified safe region for each safety notion symbolically
2. Proved safety for hybrid systems ground robot model in KeYmaera X

André Platzer (CMU) Programming Cyber-Physical Systems With Logic POPL’19 56 / 66
Ground Robot Obstacle Avoidance: Verify

- Fundamental safety question for ground robot navigation
- When will which control decision avoid obstacles?
- Depends on safety objective, physical capabilities of robot + obstacle

<table>
<thead>
<tr>
<th>Orientation</th>
<th>Passive-friendly</th>
<th>Passive</th>
<th>Static</th>
<th>Avoid/Follow</th>
<th>Head-on</th>
<th>Turn</th>
</tr>
</thead>
<tbody>
<tr>
<td>Orientation</td>
<td>Orientation</td>
<td>Orientation</td>
<td>Orientation</td>
<td>Orientation</td>
<td>Orientation</td>
<td>Orientation</td>
</tr>
</tbody>
</table>

1. Identified safe region for each safety notion symbolically
2. Proved safety for hybrid systems ground robot model in KeYmaera X
<table>
<thead>
<tr>
<th>Safety</th>
<th>Invariant + Safe Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>static</td>
<td>$|p - o|_{\infty} &gt; \frac{s^2}{2b} + \left(\frac{A}{b} + 1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon s\right)$</td>
</tr>
<tr>
<td>passive</td>
<td>$s \neq 0 \rightarrow |p - o|_{\infty} &gt; \frac{s^2}{2b} + V\frac{s}{b} + \left(\frac{A}{b} + 1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon(s + V)\right)$</td>
</tr>
<tr>
<td>+ sensor</td>
<td>$|\hat{p} - o|_{\infty} &gt; \frac{s^2}{2b} + V\frac{s}{b} + \left(\frac{A}{b} + 1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon(s + V)\right) + \Delta_p$</td>
</tr>
<tr>
<td>+ disturb.</td>
<td>$|p - o|_{\infty} &gt; \frac{s^2}{2b\Delta_a} + V\frac{s}{b\Delta_a} + \left(\frac{A}{b\Delta_a} + 1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon(s + V)\right)$</td>
</tr>
<tr>
<td>+ failure</td>
<td>$|\hat{p} - o|_{\infty} &gt; \frac{s^2}{2b} + V\frac{s}{b} + \left(\frac{A}{b} + 1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon(v + V)\right) + \Delta_p + g\Delta$</td>
</tr>
<tr>
<td>friendly</td>
<td>$|p - o|_{\infty} &gt; \frac{s^2}{2b} + \frac{V^2}{2b_0} + V\left(\frac{s}{b} + \tau\right) + \left(\frac{A}{b} + 1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon(s + V)\right)$</td>
</tr>
</tbody>
</table>
## Ground Robot Invariants and Safe Control Constraints

<table>
<thead>
<tr>
<th>Safety</th>
<th>Invariant</th>
<th>+ Safe Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>static</td>
<td>$|p - o|_\infty &gt; \frac{s^2}{2b}$</td>
<td>$+ \left( \frac{A}{b} + 1 \right) \left( \frac{A}{2} \varepsilon^2 + \varepsilon s \right)$</td>
</tr>
<tr>
<td>passive</td>
<td>$s \neq 0 \rightarrow |p - o|_\infty &gt; \frac{s^2}{2b}$</td>
<td>$+ V \frac{s}{b} + \left( \frac{A}{b} + 1 \right) \left( \frac{A}{2} \varepsilon^2 + \varepsilon (s + V) \right)$</td>
</tr>
<tr>
<td>+ sensor</td>
<td>$|p - o|_\infty$</td>
<td>$+ A \varepsilon^2 + \varepsilon (s + V)$</td>
</tr>
<tr>
<td>+ disturb.</td>
<td>$|p - o|_\infty &gt; \frac{s^2}{2b} \Delta_a + V \frac{s}{b} \Delta_a$</td>
<td>$+ \left( \frac{A}{b} + 1 \right) \left( \frac{A}{2} \varepsilon^2 + \varepsilon (s + V) \right)$</td>
</tr>
<tr>
<td>+ failure</td>
<td>$|\hat{p} - o|_\infty &gt; \frac{s^2}{2b} \Delta_a + V \frac{s}{b} \Delta_a$</td>
<td>$+ \left( \frac{A}{b} + 1 \right) \left( \frac{A}{2} \varepsilon^2 + \varepsilon (v + V) \right) + \Delta_p + g \Delta$</td>
</tr>
<tr>
<td>friendly</td>
<td>$|p - o|_\infty &gt; \frac{s^2}{2b} + V^2 \frac{s}{2b_o}$</td>
<td>$+ V \left( \frac{s}{b} + \tau \right) + \left( \frac{A}{b} + 1 \right) \left( \frac{A}{2} \varepsilon^2 + \varepsilon (s + V) \right)$</td>
</tr>
</tbody>
</table>

### Question

How to find and justify constraints? Proof!
VeriPhy: Automatic, Verified EXEs from Controllers

Hybrid Systems Theorem Proving

Abstract Controllers and Monitors

Sound Discrete Arithmetic

Sound Monitor Compilation

Cyber Physical System
VeriPhy: Automatic, Verified EXEs from Controllers

Hybrid Systems Theorem Proving → Abstract Controllers and Monitors → Sound Discrete Arithmetic → Sound Monitor Compilation → Cyber Physical System

Small Prover Core Proven Sound → Provably Correct Monitoring Conditions → Formalized Soundness Theorem → Verified Compiler → Verified Executable
VeriPhy: Automatic, Verified EXEs from Controllers

Hybrid Systems Theorem Proving → Abstract Controllers and Monitors → Sound Discrete Arithmetic → Sound Monitor Compilation → Cyber Physical System

Small Prover Core Proven Sound → Provably Correct Monitoring Conditions → Formalized Soundness Theorem → Verified Compiler → Verified Executable

KeYmaera X → Isabelle/HOL → HOL4

André Platzer (CMU) Programming Cyber-Physical Systems With Logic POPL’19 58 / 66
VeriPhy: Automatic, Verified EXEs from Controllers

PLDI'18

André Platzer (CMU)

Programming Cyber-Physical Systems With Logic

POPL'19 58 / 66
CakeML Compiler Preserves Guarantees

Andre Platzer (CMU)

Programming Cyber-Physical Systems With Logic
VeriPhy: Takeaway Metaphor

Your Model

Low-Level Proofs

Safe CPS
ModelPlex ensures that verification results about models apply to CPS implementations.

Contributions:
- Verification results about models transfer to CPS when validating model compliance.
- Compliance with model is characterizable in logic.
- Compliance formula transformed by proof to monitor.
- Correct-by-construction provably correct model validation at runtime.
ModelPlex ensures that verification results about models apply to CPS implementations.

Contributions:

- Verification results about models transfer to CPS when validating model compliance.
- Compliance with model is characterizable in logic.
- Compliance formula transformed by proof to monitor.
- Correct-by-construction provably correct model validation at runtime.

Questions:

- Model adequate?
- Control safe?
- Until next cycle?
Sandboxed controller uses external controller when decision is safe, else uses verified fallback. Detects non-compliant plants.

\[ \phi \rightarrow [(\text{ctrl}; \text{plant})^*] \psi \]

\[
\vec{x} := \text{extCtrl};
\]

\[
(?\phi;
( \vec{x}^+ := \text{extCtrl};
( ?\text{ctrlMon}(\vec{x}, \vec{x}^+) \\
\cup \text{fallback} );
\vec{x} := \vec{x}^+;
\vec{x}^+ := \star;
?	ext{plantMon}(\vec{x}, \vec{x}^+);
\vec{x} := (\vec{x}^+)^*)
\]
Outline (Programming CPS with Logic)

1. CPS are Multi-Dynamical Systems
2. CPS Programs
   - Syntax
   - Semantics
   - Examples
3. Differential Dynamic Logic
   - Syntax
   - Semantics
   - Example: Car Control Design
4. Dynamic Axioms for Dynamical Systems
   - Axiomatics
   - Safe CPS Programming & Proving in KeYmaera X
5. Differential Invariants for Differential Equations
6. Applications
7. Verified Compilation of CPS Programs
8. Summary
Acknowledgments

Logical Systems Lab at Carnegie Mellon University
Yong Kiam Tan, Brandon Bohrer, Nathan Fulton, Sarah Loos
Stefan Mitsch, Khalil Ghorbal, Jean-Baptiste Jeannin, Andrew Sogokon
differential dynamic logic

\[ dL = DL + HP \]

- Multi-dynamical systems
- Hybrid programs + dL logic
- Compositional proofs
- Logic impacts CPS

1. Analytic foundations
2. Practical proving
3. Significant applications
4. Bring sciences together

Programming CPS ≠ program cyber || program physics (mutual ignorance)
Further CPS Topics

Numerous wonders remain to be discovered

- Verified CPS implementations by ModelPlex
- Correct CPS execution
- CPS proof and tactic languages+libraries
- Big CPS built from safe components
- Stochastic hybrid systems
- Invariant generation
- Safe AI autonomy in CPS
- Correct model transformation
- Refinement + system property proofs
- CPS information flow
- Hybrid games

= CPSs deserve proofs as safety evidence!

I Part: Elementary Cyber-Physical Systems

2. Differential Equations & Domains
3. Choice & Control
4. Safety & Contracts
5. Dynamical Systems & Dynamic Axioms
6. Truth & Proof
7. Control Loops & Invariants
8. Events & Responses
9. Reactions & Delays

II Part: Differential Equations Analysis

10. Differential Equations & Differential Invariants
11. Differential Equations & Proofs
12. Ghosts & Differential Ghosts
13. Differential Invariants & Proof Theory

III Part: Adversarial Cyber-Physical Systems

14-17. Hybrid Systems & Hybrid Games

IV Part: Comprehensive CPS Correctness
Appendix

- Soundness and Completeness
- Differentials
- Differential Ghosts
- Differential Radical Invariants
Theorem (Sound & Complete) (JAR’08, LICS’12, JAR’17)

$dL$ calculus is a sound & complete axiomatization of hybrid systems relative to either differential equations or to discrete dynamics.

Corollary (Complete Proof-theoretical Bridge)

proving continuous = proving hybrid = proving discrete

$\vdash P \iff \text{FODE} \vdash_{dL} P$
Theorem (Sound & Complete) (JAR’08, LICS’12, JAR’17)

\[ dL \text{ calculus is a sound & complete axiomatization of hybrid systems relative to either differential equations or to discrete dynamics.} \]

Corollary (Complete Proof-theoretical Bridge)

proving continuous = proving hybrid = proving discrete
Theorem (Sound & Complete) (JAR’08, LICS’12, JAR’17)

dL calculus is a sound & complete axiomatization of hybrid systems relative to either differential equations or to discrete dynamics.

Corollary (Complete Proof-theoretical Bridge)

proving continuous = proving hybrid = proving discrete
### Differentials

#### Syntax
\[
e ::= x \mid x' \mid c \mid e + k \mid e \cdot k \mid (e)'
\]

#### Semantics
\[
\omega[(e)'] = \sum_x \omega(x') \frac{\partial[e]}{\partial x}(\omega)
\]

#### Axioms
\[
\begin{align*}
(e + k)' &= (e)' + (k)' \\
(e \cdot k)' &= (e)' \cdot k + e \cdot (k)' \\
(c())' &= 0 & \text{for constants/numbers } c() \\
(x)' &= x' & \text{for variables } x \in \mathcal{V}
\end{align*}
\]

#### ODE
\[
[x' = f(x) \land Q] = \{(\varphi(0)|_{\{x'\}^C}, \varphi(r)) : \varphi \models x' = f(x) \land Q
\}
\text{ for some } \varphi : [0, r] \to \mathcal{S}, \text{ some } r \in \mathbb{R}
\]
Differential Substitution Lemmas

Lemma (Differential lemma) (Differential value vs. Time-derivative)

If $\phi \models x' = f(x) \wedge Q$ for duration $r > 0$, then for all $0 \leq z \leq r$, $FV(e) \subseteq \{x\}$:

$$\phi(z)[(e)'] = \frac{d\phi(t)[e]}{dt}(z)$$

Lemma (Differential assignment) (Effect on Differentials)

If $\phi \models x' = f(x) \wedge Q$ then $\phi \models P \iff [x' := f(x)]P$

Lemma (Derivations) (Equations of Differentials)

$$(e + k)' = (e)' + (k)'$$

$$(e \cdot k)' = (e)' \cdot k + e \cdot (k)'$$

$$(c())' = 0 \quad \text{for constants/numbers } c()$$

$$(x)' = x' \quad \text{for variables } x \in \mathcal{V}$$
# Differential Substitution Lemmas \leadsto Proofs

## Lemma (Differential lemma) (Differential value vs. Time-derivative)

If $\varphi \models x' = f(x) \land Q$ for duration $r > 0$, then for all $0 \leq z \leq r$, $FV(e) \subseteq \{x\}$:

$$\varphi(z)[(e)'] = \frac{d\varphi(t)[e]}{dt}(z)$$

### Syntactic

### Analytic

## Lemma (Differential assignment) (Effect on Differentials)

$$DE \ [x' = f(x) \& Q]P \leftrightarrow [x' = f(x) \& Q][x' := f(x)]P$$

## Lemma (Derivations) (Equations of Differentials)

<table>
<thead>
<tr>
<th>Operator</th>
<th>Equation</th>
</tr>
</thead>
<tbody>
<tr>
<td>$+'$</td>
<td>$(e + k)' = (e)' + (k)'$</td>
</tr>
<tr>
<td>$' \cdot$</td>
<td>$(e \cdot k)' = (e)' \cdot k + e \cdot (k)'$</td>
</tr>
<tr>
<td>$c'$</td>
<td>$(c())' = 0$</td>
</tr>
<tr>
<td>$x'$</td>
<td>$(x)' = x'$</td>
</tr>
</tbody>
</table>
Darboux inequalities are DG

\[
\begin{align*}
Q \vdash p' &\geq gp \\
p \geq 0 \vdash [x' = f(x) & Q] p \geq 0
\end{align*}
\]
\[(g \in \mathbb{R}[x])\]

\[
(1-u^2-v^2)' \geq -\frac{1}{2}(u^2+v^2)(1-u^2-v^2)
\]

\[
\vdash u' = -v + \frac{u}{4}(1-u^2-v^2)
\]

\[
v' = u + \frac{v}{4}(1-u^2-v^2)
\]

\[
1-u^2-v^2 > 0
\]
Darboux inequalities are DG

\[ Q \vdash p' \geq gp \]

\[ p \succcurlyeq 0 \vdash [x' = f(x) \& Q]p \succcurlyeq 0 \]

\[
\begin{align*}
(1-u^2-v^2)' & \geq -\frac{1}{2}(u^2+v^2)(1-u^2-v^2) \\
\vdots & \vdash [u' = -v + \frac{u}{4}(1-u^2-v^2) \\
v' & = u + \frac{v}{4}(1-u^2-v^2) \\
y' & = \frac{1}{2}(u^2+v^2)y \\
\] 1-u^2-v^2 & > 0 \\
\end{align*}
\]

\[
(1-u^2-v^2)y > 0
\]
Darboux Inequalities are Differential Ghosts: Details

\[ (-gy)z^2 + y(2z(\frac{g}{2}z)) = 0 \]

\[ yz^2 = 1 \vdash [x' = f(x), y' = -gy, z' = \frac{g}{2}z & Q] yz^2 = 1 \]

\[ y > 0 \vdash \exists z [x' = f(x), y' = -gy, z' = \frac{g}{2}z & Q] \]

\[ y > 0 \vdash [x' = f(x), y' = -gy & Q] y > 0 \]

\[ Q \vdash p' \geq gp \]

\[ \mathbb{R} \quad p' \geq gp, y > 0 \vdash p'y - gyp \geq 0 \]

\[ \begin{align*}
Q, y > 0 & \vdash p'y - gyp \geq 0 \\
p \geq 0, y > 0 & \vdash [x' = f(x), y' = -gy & Q \land y > 0] py \geq 0
\end{align*} \]

\[ p \geq 0, y > 0 \vdash [x' = f(x), y' = -gy & Q] (y > 0 \land py \geq 0) \]

\[ p \geq 0 \vdash \exists y [x' = f(x), y' = -gy & Q] p \geq 0 \]

\[ p \geq 0 \vdash [x' = f(x) & Q] p \geq 0 \]

P.S. \( z' = \frac{g}{2}z \) superfluous for open inequalities \( p > 0 \) and \( p \neq 0 \).
Theorem (Differential radical invariant characterization)

\[ h = 0 \rightarrow \bigwedge_{i=1}^{N-1} h^{(i)}_p = 0 \]
\[ h = 0 \rightarrow [x' = p]h = 0 \]

characterizes all algebraic invariants, where \( N = \text{ord} \sqrt[\prime]{h} \), i.e.

\[ h^{(N)}_p = \sum_{i=0}^{N-1} g_i h^{(i)}_p \quad (g_i \in \mathbb{R}[x]) \quad h^{(i+1)}_p = [x' := p](h^{(i)}_p)' \]

Corollary (Algebraic Invariants Decidable)

Algebraic invariants of algebraic differential equations are decidable.
Example: Longitudinal Dynamics of an Airplane

Study (6th Order Longitudinal Flight Equations)

\[ u' = \frac{X}{m} - g \sin(\theta) - qw \quad \text{axial velocity} \]
\[ w' = \frac{Z}{m} + g \cos(\theta) + qu \quad \text{vertical velocity} \]
\[ x' = \cos(\theta)u + \sin(\theta)w \quad \text{range} \]
\[ z' = -\sin(\theta)u + \cos(\theta)w \quad \text{altitude} \]
\[ \theta' = q \quad \text{pitch angle} \]
\[ q' = \frac{M}{I_{yy}} \quad \text{pitch rate} \]

\( X \): thrust along \( u \) \quad \( Z \): thrust along \( w \) \quad \( M \): thrust moment for \( w \)
\( g \): gravity \quad \( m \): mass \quad \( I_{yy} \): inertia second diagonal

with Khalil Ghorbal TACAS’14

André Platzer (CMU)
Programming Cyber-Physical Systems With Logic
POPL’19 73 / 66
Case Study: Longitudinal Dynamics of an Airplane

Result (DRI Automatically Generates Invariant Functions)

\[
\frac{M_z}{I_{yy}} + g\theta + \left(\frac{X}{m} - qw\right)\cos(\theta) + \left(\frac{Z}{m} + qu\right)\sin(\theta)
\]

\[
\frac{M_x}{I_{yy}} - \left(\frac{Z}{m} + qu\right)\cos(\theta) + \left(\frac{X}{m} - qw\right)\sin(\theta)
\]

\[-q^2 + \frac{2M\theta}{I_{yy}}\]

with Khalil Ghorbal TACAS'14

Andre Platzer (CMU)
Programming Cyber-Physical Systems With Logic
POPL'19 74 / 66
Example: Dubins Dynamics of 2 Airplanes

Result (DRI Automatically Generates Invariants)

\[ \omega_1 = 0 \land \omega_2 = 0 \rightarrow v_2 \sin \vartheta x = (v_2 \cos \vartheta - v_1)y > p(v_1 + v_2) \]

\[ \omega_1 \neq 0 \lor \omega_2 \neq 0 \rightarrow -\omega_1 \omega_2(x^2 + y^2) + 2v_2 \omega_1 \sin \vartheta x + 2(v_1 \omega_2 - v_2 \omega_1 \cos \vartheta)y + 2v_1 v_2 \cos \vartheta > 2v_1 v_2 + 2p(v_2|\omega_1| + v_1|\omega_2|) + p^2|\omega_1 \omega_2| \]
André Platzer.  
*Logical Foundations of Cyber-Physical Systems.*  
Springer, Cham, 2018.  
URL: [http://www.springer.com/978-3-319-63587-3](http://www.springer.com/978-3-319-63587-3),  
doi:10.1007/978-3-319-63588-0.

André Platzer.  
Logic & proofs for cyber-physical systems.  
doi:10.1007/978-3-319-40229-1_3.

André Platzer.  
Logics of dynamical systems.  
In LICS [22], pages 13–24.  

André Platzer.  
A complete uniform substitution calculus for differential dynamic logic.  
André Platzer.
Differential dynamic logic for hybrid systems.

André Platzer.
Differential game logic.

André Platzer.
Differential hybrid games.

Stefan Mitsch, Khalil Ghorbal, David Vogelbacher, and André Platzer.
Formal verification of obstacle avoidance and navigation of ground robots.
André Platzer and Jan-David Quesel.
European Train Control System: A case study in formal verification.

Stefan Mitsch, Marco Gario, Christof J. Budnik, Michael Golm, and André Platzer.
Formal verification of train control with air pressure brakes.
doi:10.1007/978-3-319-68499-4_12.

Jean-Baptiste Jeannin, Khalil Ghorbal, Yanni Kouskoulas, Aurora Schmidt, Ryan Gardner, Stefan Mitsch, and André Platzer.
A formally verified hybrid system for safe advisories in the next-generation airborne collision avoidance system.
André Platzer.
The complete proof theory of hybrid systems.
In LICS [22], pages 541–550.
doi:10.1109/LICS.2012.64.

Nathan Fulton, Stefan Mitsch, Jan-David Quesel, Marcus Völп, and André Platzer.
KeYmaera X: An axiomatic tactical theorem prover for hybrid systems.
doi:10.1007/978-3-319-21401-6_36.

Stefan Mitsch and André Platzer.
ModelPlex: Verified runtime validation of verified cyber-physical system models.
Special issue of selected papers from RV’14.

André Platzer.
Differential-algebraic dynamic logic for differential-algebraic programs.
André Platzer.

Nathan Fulton, Stefan Mitsch, Brandon Bohrer, and André Platzer.
Bellerophon: Tactical theorem proving for hybrid systems.
doi:10.1007/978-3-319-66107-0_14.

André Platzer.
Stochastic differential dynamic logic for stochastic hybrid programs.
doi:10.1007/978-3-642-22438-6_34.

Khalil Ghorbal and André Platzer.
Characterizing algebraic invariants by differential radical invariants.
Thomas A. Henzinger.
The theory of hybrid automata.
doi:10.1109/LICS.1996.561342.

Jennifer M. Davoren and Anil Nerode.
Logics for hybrid systems.
doi:10.1109/5.871305.