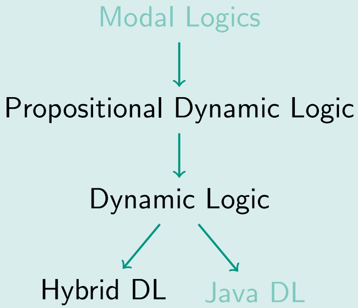
Formale Systeme II: Theorie

SS 2016

Prof. Dr. Bernhard Beckert · Dr. Mattias Ulbrich
Slides by courtesy of André Platzer, CMU

Roadmap

Overview – a family of logics



Modal Logics

Propositional Dynamic Logic

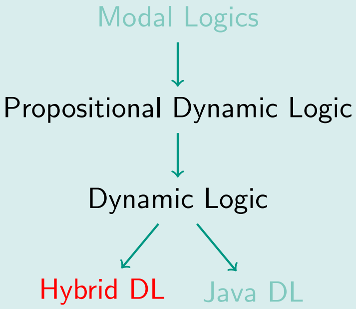
Dynamic Logic

Hybrid DL

Java DL

Roadmap

Overview – a family of logics



Modal Logics

Propositional Dynamic Logic

Dynamic Logic

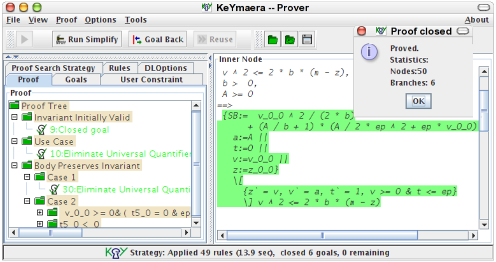
Hybrid DL

Java DL

Goals

- hybrid dynamic logic
- differential equations
- quantifier elimination for $\mathbb{R}$
- modelling cyberphysical systems
- modelling pitfalls and opportunities
- differential invariants

A. Platzer, KeYmaera



```
Proof
Proof Tree
  Invariant Initially Valid
    9:Closed goal
  Use Case
    10:Eliminate Universal Quantifier
  Body Preserves Invariant
    Case 1
      30:Eliminate Universal Quanti
    Case 2
      v_0_0 >= 0& ( t5_0 = 0 & ep
      t5_0 < 0
```

```
 v ^ 2 <= 2 * b * (m - z),
 b >  0,
 A >= 0
==>
 {SB:=  v_0_0 ^ 2 / (2 * b)
      + (A / b + 1) * (A / 2 * ep ^ 2 + ep * v_0_0)
   a:=A ||
   t:=0 ||
   v:=v_0_0 ||
   z:=z_0_0}
   \[
     {z` = v, v` = a, t` = 1, v >= 0 & t <= ep}
    \] v ^ 2 <= 2 * b * (m - z)
```

Proof closed

Proved.
Statistics:
Nodes:50
Branches: 6

Strategy: Applied 49 rules (13.9 sec), closed 6 goals, 0 remaining

`http://www.symbolaris.com`

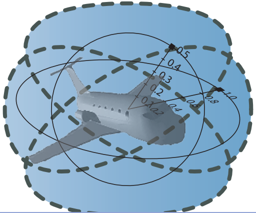
15-424/15-624: Foundations of Cyber-Physical Systems

01: Overview

André Platzer

aplatzer@cs.cmu.edu
Carnegie Mellon University, Pittsburgh, PA

http://symbolaris.com/course/fcps16.html
http://www.cs.cmu.edu/~aplatzer/course/fcps16.html



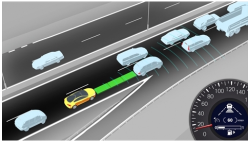
Cyber-Physical Systems Analysis: Aircraft Example

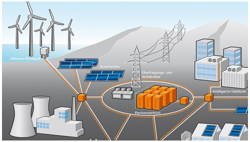
Which control decisions are safe for aircraft collision avoidance?

CPSs Promise Transformative Impact!

Prospects: Safe & Efficient

Driver assistance	Pilot decision support	Train protection
Autonomous cars	Autopilots / UAVs	Robots help people





Prerequisite: CPS need to be safe

How do we make sure CPS make the world a better place?

Can you trust a computer to control physics?

Rationale

1. Safety guarantees require analytic foundations.
2. Foundations revolutionized digital computer science & our society.
3. Need even stronger foundations when software reaches out into our physical world.

How can we provide people with cyber-physical systems they can bet their lives on? — Jeannette Wing

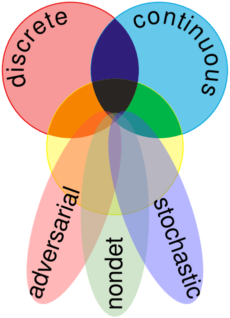
Cyber-physical Systems

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

CPSs are Multi-Dynamical Systems

CPS Dynamics

CPS are characterized by multiple facets of dynamical systems.



CPS Compositions

CPS combine multiple simple dynamical effects.

Tame Parts

Exploiting compositionality tames CPS complexity.

Hybrid Systems & Cyber-Physical Systems

Mathematical model for complex physical systems:

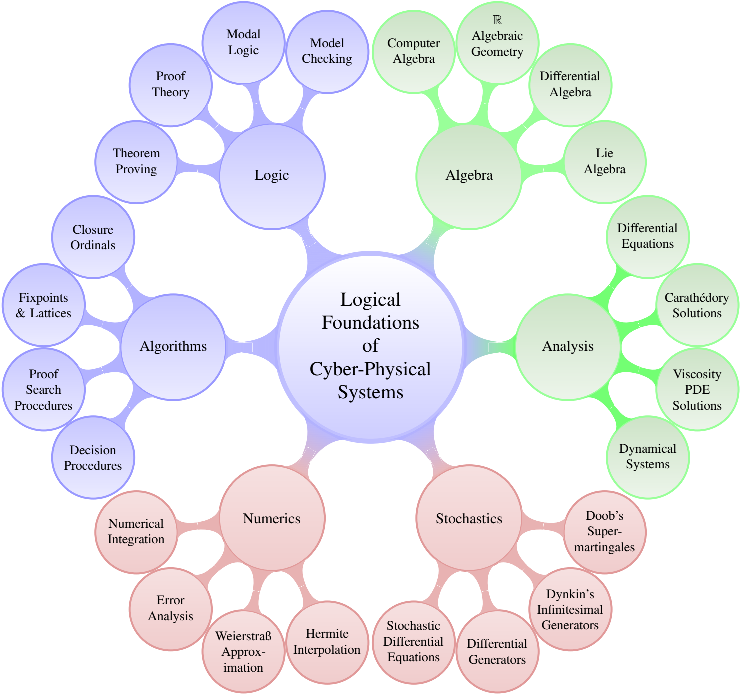
Definition (Hybrid Systems)

systems with interacting discrete and continuous dynamics

Technical characteristics:

Definition (Cyber-Physical Systems)

(Distributed network of) computerized control for physical system
Computation, communication and control for physics



Logical Foundations of Cyber-Physical Systems

- Logic
  - Theorem Proving
  - Proof Theory
  - Modal Logic
  - Model Checking
- Algebra
  - Computer Algebra
  - ℝ Algebraic Geometry
  - Differential Algebra
  - Lie Algebra
- Analysis
  - Differential Equations
  - Carathédory Solutions
  - Viscosity PDE Solutions
  - Dynamical Systems
- Stochastics
  - Doob's Super-martingales
  - Dynkin's Infinitesimal Generators
  - Differential Generators
  - Stochastic Differential Equations
- Numerics
  - Hermite Interpolation
  - Weierstraß Approx-imation
  - Error Analysis
  - Numerical Integration
- Algorithms
  - Decision Procedures
  - Proof Search Procedures
  - Fixpoints & Lattices
  - Closure Ordinals

How to Teach Cyber-Physical Systems?

Onion Model

1. Going outside in
2. Unpeel layer by layer
3. Progress when all prereqs are covered
4. First study CS $\land$ math $\land$ engineering
5. Talk about CPS in the big finale

Scenic Tour Model

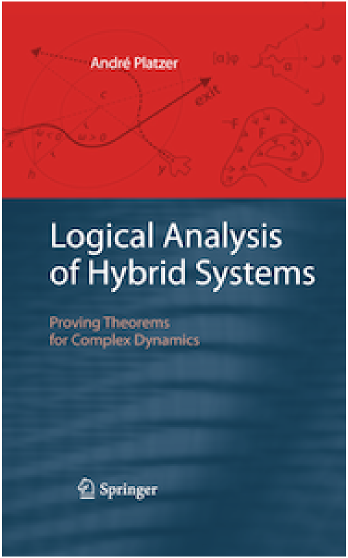
1. Start at the heart: CPS
2. Go on scenic expeditions into various directions
3. Explore the world around us as we find the need
4. Stay on CPS the whole time
5. Leverage CPS as the guiding motivation for understanding more about connected areas

Computational Thinking for CPS

Logical scrutiny, formalization, and correctness proofs are critical for CPS!

1. CPSs are so easy to get wrong.
2. These logical aspects are an integral part of CPS design.
3. Critical to your understanding of the intricate complexities of CPS.
4. Tame complexity by a simple programming language for core aspects.

Lecture Notes and Book



André Platzer.
Foundations of Cyber-Physical Systems.
Lecture notes.
Computer Science Department
Carnegie Mellon University.
`http://symbolaris.com/course/fcps16-schedule.html`

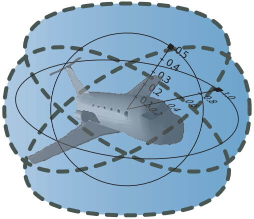
André Platzer.
Logical Analysis of Hybrid Systems.
Springer, 426p., 2010.
DOI 10.1007/978-3-642-14509-4
`http://symbolaris.com/lahs/`
CMU library e-book

02: Differential Equations & Domains

15-424: Foundations of Cyber-Physical Systems

André Platzer

`aplatzer@cs.cmu.edu`
Computer Science Department
Carnegie Mellon University, Pittsburgh, PA



Outline

Outline

1. Introduction

2. Differential Equations

3. Examples of Differential Equations

4. Domains of Differential Equations

Differential Equations as Models of Continuous Processes

Example (Vector field and one solution of a differential equation)

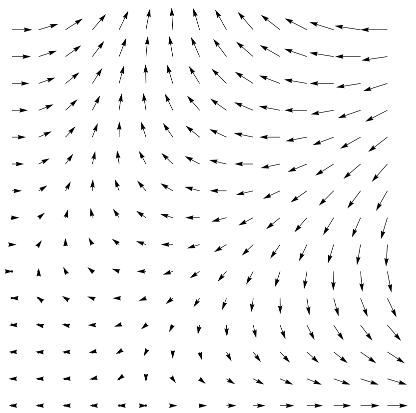
$$\left[\begin{array}{ll} y'(t) = & f(t,y) \\ y(t_0) = & y_0 \end{array}\right]$$

Intuition:

Differential Equations as Models of Continuous Processes

Example (Vector field and one solution of a differential equation)

$$\left[\begin{array}{ll} y'(t) = & f(t,y) \\ y(t_0) = & y_0 \end{array}\right]$$



Intuition:

1. At each point in space, plot the value of $f(t,y)$ as a vector

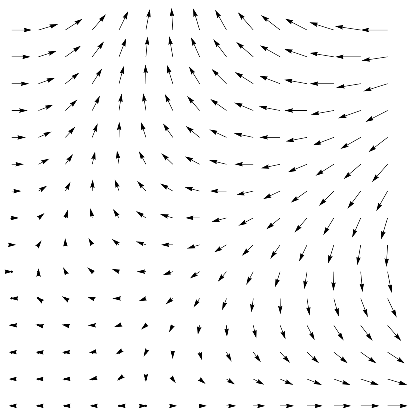
Differential Equations as Models of Continuous Processes

Example (Vector field and one solution of a differential equation)

$$\begin{bmatrix} y'(t) = & f(t,y) \\ y(t_0) = & y_0 \end{bmatrix}$$

Intuition:

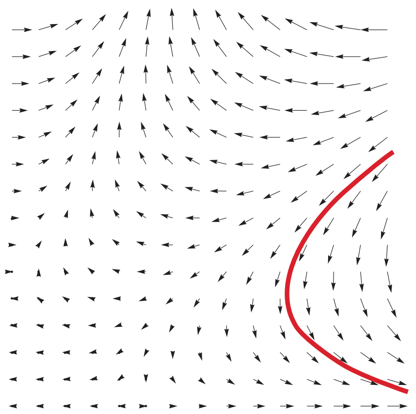
1. At each point in space, plot the value of $f(t,y)$ as a vector
2. Start at initial state y_0 at initial time t_0



Differential Equations as Models of Continuous Processes

Example (Vector field and one solution of a differential equation)

$$\left[\begin{array}{ll} y'(t) = & f(t,y) \\ y(t_0) = & y_0 \end{array}\right]$$



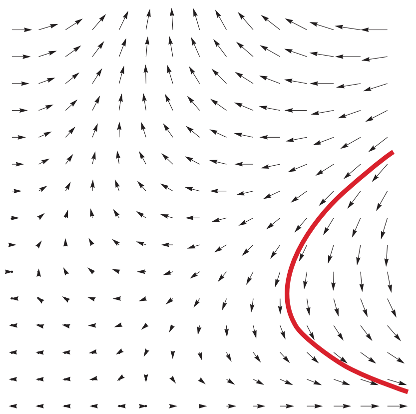
Intuition:

1. At each point in space, plot the value of $f(t,y)$ as a vector
2. Start at initial state y_0 at initial time t_0
3. Follow the direction of the vector

Differential Equations as Models of Continuous Processes

Example (Vector field and one solution of a differential equation)

$$\left[\begin{array}{rl} y'(t) = & f(t,y) \\ y(t_0) = & y_0 \end{array}\right]$$



Intuition:

1. At each point in space, plot the value of $f(t,y)$ as a vector
2. Start at initial state y_0 at initial time t_0
3. Follow the direction of the vector

↯ The diagram should show infinitely many vectors . . .

Differential Equations as Models of Continuous Processes

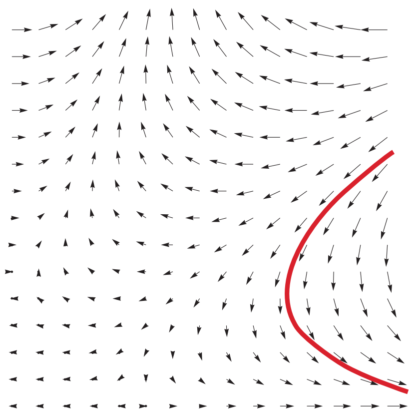
Example (Vector field and one solution of a differential equation)

$$\begin{bmatrix} y'(t) = & f(t,y) \\ y(t_0) = & y_0 \end{bmatrix}$$

Intuition:

1. At each point in space, plot the value of $f(t,y)$ as a vector
2. Start at initial state y_0 at initial time t_0
3. Follow the direction of the vector

- ↯ The diagram should show infinitely many vectors . . .

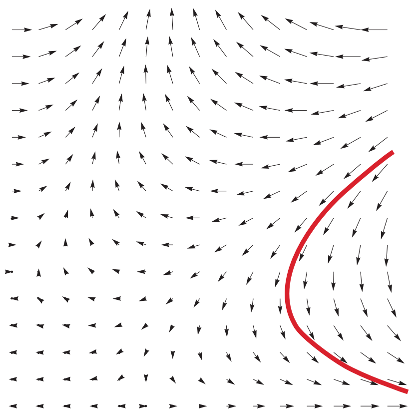


Your car's ODE $x' = v, v' = a$

Differential Equations as Models of Continuous Processes

Example (Vector field and one solution of a differential equation)

$$\left[\begin{array}{rl} y'(t) = & f(t,y) \\ y(t_0) = & y_0 \end{array}\right]$$



Intuition:

1. At each point in space, plot the value of $f(t,y)$ as a vector
2. Start at initial state y_0 at initial time t_0
3. Follow the direction of the vector

↯ The diagram should show infinitely many vectors . . .

Your car's ODE $x' = v, v' = a$

Well it's a wee bit more complicated

Outline

1. Introduction
2. Differential Equations
3. Examples of Differential Equations
4. Domains of Differential Equations

The Meaning of Differential Equations

1. What exactly is a vector field?
2. What does it mean to describe directions of evolution at every point in space?
3. Could directions possibly contradict each other?

Importance of meaning

The physical impacts of CPSs do not leave much room for failure, so we immediately want to get into the mood of consistently studying the behavior and exact meaning of all relevant aspects of CPS.

Differential Equations & Initial-Value Problems

Definition (Ordinary Differential Equation, ODE)

$f : D \to \mathbb{R}^n$ on domain $D \subseteq \mathbb{R} \times \mathbb{R}^n$ (i.e., open connected). Then $Y : I \to \mathbb{R}^n$ is *solution* of initial value problem (IVP)

$$\left[\begin{array}{rl} y'(t) = & f(t, y) \\ y(t_0) = & y_0 \end{array}\right]$$

on interval $I \subseteq \mathbb{R}$, iff, for all times $t \in I$,

Differential Equations & Initial-Value Problems

Definition (Ordinary Differential Equation, ODE)

$f : D \to \mathbb{R}^n$ on domain $D \subseteq \mathbb{R} \times \mathbb{R}^n$ (i.e., open connected). Then $Y : I \to \mathbb{R}^n$ is *solution* of initial value problem (IVP)

$$\left[\begin{array}{rl} y'(t) = & f(t, y) \\ y(t_0) = & y_0 \end{array}\right]$$

on interval $I \subseteq \mathbb{R}$, iff, for all times $t \in I$,

1. $(t, Y(t)) \in D$

Differential Equations & Initial-Value Problems

Definition (Ordinary Differential Equation, ODE)

$f : D \to \mathbb{R}^n$ on domain $D \subseteq \mathbb{R} \times \mathbb{R}^n$ (i.e., open connected). Then $Y : I \to \mathbb{R}^n$ is *solution* of initial value problem (IVP)

$$\left[\begin{array}{rl} y'(t) = & f(t, y) \\ y(t_0) = & y_0 \end{array}\right]$$

on interval $I \subseteq \mathbb{R}$, iff, for all times $t \in I$,

1. $(t, Y(t)) \in D$
2. $Y'(t)$ exists and $Y'(t) = f(t, Y(t))$.

Differential Equations & Initial-Value Problems

Definition (Ordinary Differential Equation, ODE)

$f : D \to \mathbb{R}^n$ on domain $D \subseteq \mathbb{R} \times \mathbb{R}^n$ (i.e., open connected). Then $Y : I \to \mathbb{R}^n$ is *solution* of initial value problem (IVP)

$$\left[\begin{array}{rl} y'(t) = & f(t, y) \\ y(t_0) = & y_0 \end{array} \right]$$

on interval $I \subseteq \mathbb{R}$, iff, for all times $t \in I$,

1. $(t, Y(t)) \in D$
2. $Y'(t)$ exists and $Y'(t) = f(t, Y(t))$.
3. $Y(t_0) = y_0$

Differential Equations & Initial-Value Problems

Definition (Ordinary Differential Equation, ODE)

$f : D \to \mathbb{R}^n$ on domain $D \subseteq \mathbb{R} \times \mathbb{R}^n$ (i.e., open connected). Then $Y : I \to \mathbb{R}^n$ is *solution* of initial value problem (IVP)

$$\left[\begin{array}{rl} y'(t) = & f(t,y) \\ y(t_0) = & y_0 \end{array}\right]$$

on interval $I \subseteq \mathbb{R}$, iff, for all times $t \in I$,

1. $(t, Y(t)) \in D$
2. $Y'(t)$ exists and $Y'(t) = f(t, Y(t))$.
3. $Y(t_0) = y_0$

If $f \in C(D, \mathbb{R}^n)$, then $Y \in C^1(I, \mathbb{R}^n)$.

Differential Equations & Initial-Value Problems

Definition (Ordinary Differential Equation, ODE)

$f : D \to \mathbb{R}^n$ on domain $D \subseteq \mathbb{R} \times \mathbb{R}^n$ (i.e., open connected). Then $Y : I \to \mathbb{R}^n$ is *solution* of initial value problem (IVP)

$$\left[\begin{array}{rl} y'(t) = & f(t,y) \\ y(t_0) = & y_0 \end{array}\right]$$

on interval $I \subseteq \mathbb{R}$, iff, for all times $t \in I$,

1. $(t, Y(t)) \in D$
2. $Y'(t)$ exists and $Y'(t) = f(t, Y(t))$.
3. $Y(t_0) = y_0$

If $f \in C(D, \mathbb{R}^n)$, then $Y \in C^1(I, \mathbb{R}^n)$.
If f continuous, then Y continuously differentiable.

Outline

1. Introduction
2. Differential Equations
3. Examples of Differential Equations
4. Domains of Differential Equations

Example: A Constant Differential Equation

Example (Initial value problem)

$$\begin{bmatrix} x'(t) = & 5 \\ x(0) = & 2 \end{bmatrix}$$

has a solution

Example: A Constant Differential Equation

Example (Initial value problem)

$$\begin{bmatrix} x'(t) = & 5 \\ x(0) = & 2 \end{bmatrix}$$

has a solution $x(t) = 5t + 2$

Example: A Constant Differential Equation

Example (Initial value problem)

$$\left[\begin{array}{rl} x'(t) = & 5 \\ x(0) = & 2 \end{array}\right]$$

has a solution $x(t) = 5t + 2$

Check by inserting solution into ODE+IVP.

$$\left[\begin{array}{rl} (x(t))' = & (5t+2)' = 5 \\ x(0) = & 5 \cdot 0 + 2 = 2 \end{array}\right]$$

$\square$

Example: A Linear Differential Equation from before

Example (Initial value problem)

$$\left[\begin{array}{rl} x'(t) = & \frac{1}{4}x(t) \\ x(0) = & 1 \end{array}\right]$$

has a solution

Example: A Linear Differential Equation from before

Example (Initial value problem)

$$\begin{bmatrix} x'(t) = & \frac{1}{4}x(t) \\ x(0) = & 1 \end{bmatrix}$$

has a solution $x(t) = e^{\frac{t}{4}}$

Example: A Linear Differential Equation from before

Example (Initial value problem)

$$\begin{bmatrix} x'(t) = & \frac{1}{4}x(t) \\ x(0) = & 1 \end{bmatrix}$$

has a solution $x(t) = e^{\frac{t}{4}}$

Check by inserting solution into ODE+IVP.

$$\begin{bmatrix} (x(t))' = & (e^{\frac{t}{4}})' = e^{\frac{t}{4}}(\frac{t}{4})' = e^{\frac{t}{4}}\frac{1}{4} = \frac{1}{4}x(t) \\ x(0) = & e^{\frac{0}{4}} = 1 \end{bmatrix}$$

☐

ODE Examples

ODE	Solution
$x' = 1, x(0) = x_0$	$x(t) = x_0 + t$

ODE Examples

ODE	Solution
$x' = 1, x(0) = x_0$	$x(t) = x_0 + t$
$x' = 5, x(0) = x_0$	$x(t) = x_0 + 5t$

ODE Examples

ODE	Solution
$x' = 1, x(0) = x_0$	$x(t) = x_0 + t$
$x' = 5, x(0) = x_0$	$x(t) = x_0 + 5t$
$x' = x, x(0) = x_0$	$x(t) = x_0 e^t$

ODE Examples

ODE	Solution
$x' = 1, x(0) = x_0$	$x(t) = x_0 + t$
$x' = 5, x(0) = x_0$	$x(t) = x_0 + 5t$
$x' = x, x(0) = x_0$	$x(t) = x_0 e^t$
$x' = x^2, x(0) = x_0$	$x(t) = \frac{x_0}{1-tx_0}$

ODE Examples

ODE	Solution
$x' = 1, x(0) = x_0$	$x(t) = x_0 + t$
$x' = 5, x(0) = x_0$	$x(t) = x_0 + 5t$
$x' = x, x(0) = x_0$	$x(t) = x_0 e^t$
$x' = x^2, x(0) = x_0$	$x(t) = \frac{x_0}{1 - t x_0}$
$x' = \frac{1}{x}, x(0) = 1$	$x(t) = \sqrt{1 + 2t} \ldots$

ODE Examples

ODE	Solution
$x' = 1, x(0) = x_0$	$x(t) = x_0 + t$
$x' = 5, x(0) = x_0$	$x(t) = x_0 + 5t$
$x' = x, x(0) = x_0$	$x(t) = x_0 e^t$
$x' = x^2, x(0) = x_0$	$x(t) = \frac{x_0}{1-tx_0}$
$x' = \frac{1}{x}, x(0) = 1$	$x(t) = \sqrt{1+2t} \dots$
$y'(x) = -2xy, y(0) = 1$	$y(x) = e^{-x^2}$
$x'(t) = tx, x(0) = x_0$	$x(t) = x_0 e^{\frac{t^2}{2}}$
$x' = \sqrt{x}, x(0) = x_0$	$x(t) = \frac{t^2}{4} \pm t\sqrt{x_0} + x_0$
$x' = y, y' = -x, x(0) = 0, y(0) = 1$	$x(t) = \sin t, y(t) = \cos t$

ODE Examples

ODE	Solution
$x' = 1, x(0) = x_0$	$x(t) = x_0 + t$
$x' = 5, x(0) = x_0$	$x(t) = x_0 + 5t$
$x' = x, x(0) = x_0$	$x(t) = x_0 e^t$
$x' = x^2, x(0) = x_0$	$x(t) = \frac{x_0}{1-tx_0}$
$x' = \frac{1}{x}, x(0) = 1$	$x(t) = \sqrt{1+2t} \dots$
$y'(x) = -2xy, y(0) = 1$	$y(x) = e^{-x^2}$
$x'(t) = tx, x(0) = x_0$	$x(t) = x_0 e^{\frac{t^2}{2}}$
$x' = \sqrt{x}, x(0) = x_0$	$x(t) = \frac{t^2}{4} \pm t\sqrt{x_0} + x_0$
$x' = y, y' = -x, x(0) = 0, y(0) = 1$	$x(t) = \sin t, y(t) = \cos t$
$x' = 1 + x^2, x(0) = 0$	$x(t) = \tan t$
$x'(t) = \frac{2}{t^3} x(t)$	$x(t) = e^{-\frac{1}{t^2}}$ non-analytic
$x' = x^2 + x^4$	???
$x'(t) = e^{t^2}$	non-elementary

ODE Examples Solutions more complicated than ODE

ODE	Solution
$x' = 1, x(0) = x_0$	$x(t) = x_0 + t$
$x' = 5, x(0) = x_0$	$x(t) = x_0 + 5t$
$x' = x, x(0) = x_0$	$x(t) = x_0 e^t$
$x' = x^2, x(0) = x_0$	$x(t) = \frac{x_0}{1-tx_0}$
$x' = \frac{1}{x}, x(0) = 1$	$x(t) = \sqrt{1+2t} \dots$
$y'(x) = -2xy, y(0) = 1$	$y(x) = e^{-x^2}$
$x'(t) = tx, x(0) = x_0$	$x(t) = x_0 e^{\frac{t^2}{2}}$
$x' = \sqrt{x}, x(0) = x_0$	$x(t) = \frac{t^2}{4} \pm t\sqrt{x_0} + x_0$
$x' = y, y' = -x, x(0) = 0, y(0) = 1$	$x(t) = \sin t, y(t) = \cos t$
$x' = 1 + x^2, x(0) = 0$	$x(t) = \tan t$
$x'(t) = \frac{2}{t^3} x(t)$	$x(t) = e^{-\frac{1}{t^2}}$ non-analytic
$x' = x^2 + x^4$	???
$x'(t) = e^{t^2}$	non-elementary

Takeaway Message

Descriptive power of differential equations

1. Solutions of differential equations can be much more involved than the differential equations themselves.
2. Representational and descriptive power of differential equations!
3. Simple differential equations can describe quite complicated physical processes.
4. Local description as the direction into which the system evolves.

Outline

1. Introduction
2. Differential Equations
3. Examples of Differential Equations
4. Domains of Differential Equations

Evolution Domain Constraints

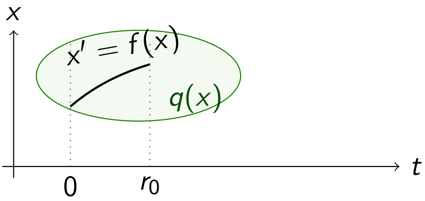
Enable Cyber to interact with Physics

Definition (Evolution domain constraints)

A *differential equation* $x' = f(x)$ *with evolution domain* $q(x)$ is denoted by

$$x' = f(x) \,\&\, q(x)$$

conjunctive notation (&) signifies that the system obeys the differential equation $x' = f(x)$ and the evolution domain $q(x)$.



Evolution Domain Constraints

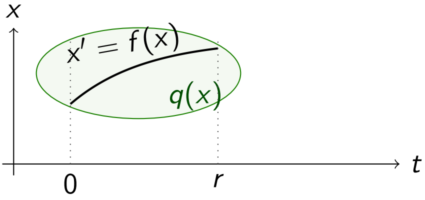
Enable Cyber to interact with Physics

Definition (Evolution domain constraints)

A *differential equation* $x' = f(x)$ *with evolution domain* $q(x)$ is denoted by

$$x' = f(x) \,\&\, q(x)$$

conjunctive notation (&) signifies that the system obeys the differential equation $x' = f(x)$ and the evolution domain $q(x)$.



Evolution Domain Constraints

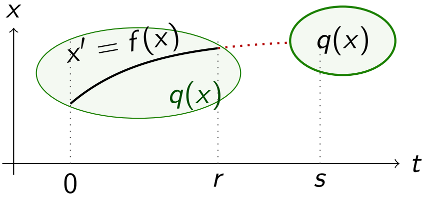
Enable Cyber to interact with Physics

Definition (Evolution domain constraints)

A *differential equation* $x' = f(x)$ *with evolution domain* $q(x)$ is denoted by

$$x' = f(x) \,\&\, q(x)$$

conjunctive notation (&) signifies that the system obeys the differential equation $x' = f(x)$ and the evolution domain $q(x)$.

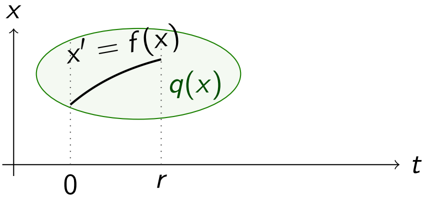


Semantics of ODE with Evolution Constraints

Definition (Semantics of differential equations)

A function $\varphi : [0, r] \to \mathcal{S}$ of some duration $r \geq 0$ satisfies the differential equation $x' = f(x) \,\&\, q(x)$, written $K, \varphi \models x' = f(x) \land q(x)$, iff:

1. $\varphi(\zeta)(x') = \frac{\mathrm{d}\varphi(t)(x)}{\mathrm{d}t}(\zeta)$ exists at for all times $0 \leq \zeta \leq r$
2. $\varphi(\zeta) \in [\![x' = f(x) \land q(x)]\!]$ for all times $0 \leq \zeta \leq r$

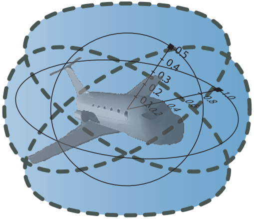


04: Safety & Contracts

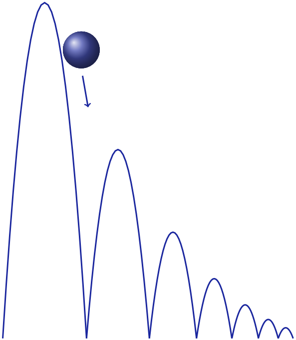
15-424: Foundations of Cyber-Physical Systems

André Platzer

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

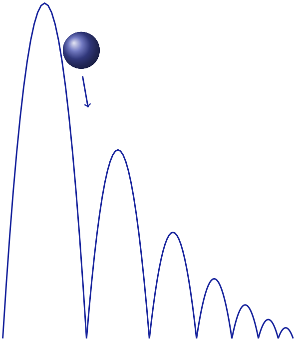


Quantum the Acrophobic Bouncing Ball



Example (Quantum the Bouncing Ball)

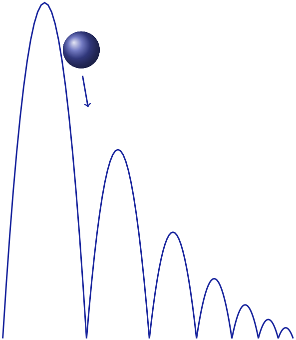
Quantum the Acrophobic Bouncing Ball



Example (Quantum the Bouncing Ball)

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

Quantum the Acrophobic Bouncing Ball

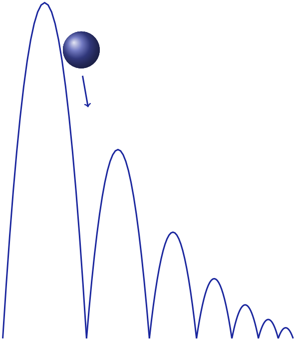


Example (Quantum the Bouncing Ball)

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

$$\mathtt{if}(x = 0)\; v := -cv$$

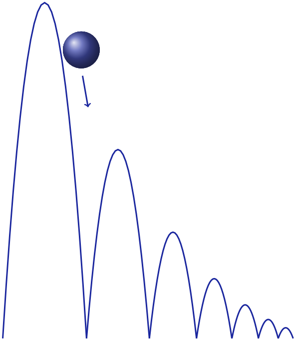
Quantum the Acrophobic Bouncing Ball



Example (Quantum the Bouncing Ball)

$$\big(x' = v, v' = -g \,\&\, x \geq 0;$$
$$\texttt{if}(x = 0)\, v := -cv\big)^*$$

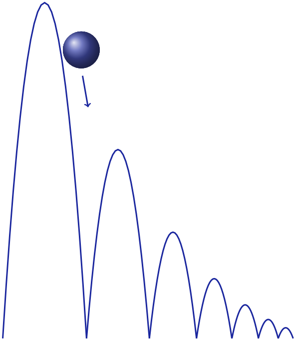
Quantum the Acrophobic Bouncing Ball



Example (Quantum the Bouncing Ball)

$$\big(x' = v, v' = -g \,\&\, x \geq 0;$$
$$\texttt{if}(x = 0)\, v := -cv\big)^*$$

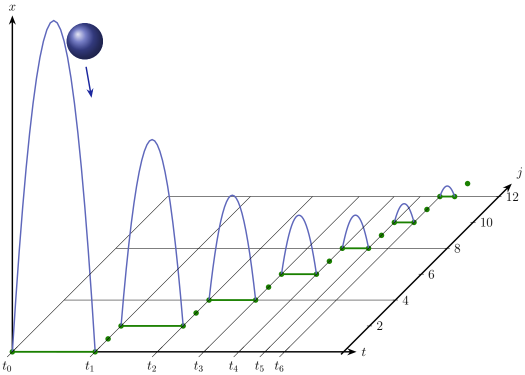
Quantum Discovered a Crack in the Fabric of Time



Example (Quantum the Bouncing Ball)

$$\big(x' = v, v' = -g \,\&\, x \geq 0;\\ \mathtt{if}(x = 0)\, v := -cv\big)^*$$

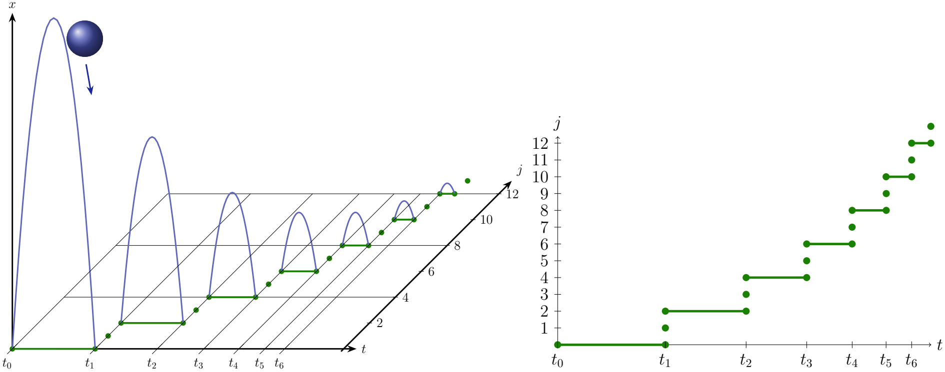
Quantum Discovered a Crack in the Fabric of Time



Example (Quantum the Bouncing Ball)

$$\big(x' = v, v' = -g \,\&\, x \geq 0;\\ \mathtt{if}(x = 0)\, v := -cv\big)^*$$

Quantum Discovered a Crack in the Fabric of Time



Example (Quantum the Bouncing Ball)

$$\left(x' = v, v' = -g \,\&\, x \geq 0;\right.$$
$$\left.\mathtt{if}(x = 0)\, v := -cv\right)^*$$

Differential Dynamic Logic d$\mathcal{L}$: Semantics

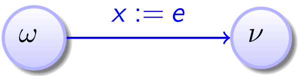
Definition (Hybrid program semantics) $(\llbracket\cdot\rrbracket : \text{HP} \to \wp(\mathcal{S} \times \mathcal{S}))$

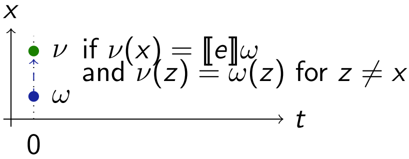
$$
\begin{aligned}
\llbracket x := e \rrbracket &= \{(\omega,\nu) \ : \ \nu = \omega \text{ except } \llbracket x \rrbracket \nu = \llbracket e \rrbracket \omega\} \\
\llbracket ?Q \rrbracket &= \{(\omega,\omega) \ : \ \omega \in \llbracket Q \rrbracket\} \\
\llbracket x' = f(x) \rrbracket &= \{(\varphi(0),\varphi(r))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

Definition (d$\mathcal{L}$ semantics) $(\llbracket\cdot\rrbracket : \text{Fml} \to \wp(\mathcal{S}))$

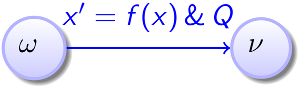
$$
\begin{aligned}
\llbracket \theta \geq \eta \rrbracket &= \{\omega \ : \ \llbracket \theta \rrbracket \omega \geq \llbracket \eta \rrbracket \omega\} \\
\llbracket \neg\phi \rrbracket &= (\llbracket \phi \rrbracket)^{\complement} \\
\llbracket \phi \land \psi \rrbracket &= \llbracket \phi \rrbracket \cap \llbracket \psi \rrbracket \\
\llbracket \langle\alpha\rangle\phi \rrbracket &= \llbracket \alpha \rrbracket \circ \llbracket \phi \rrbracket = \{\omega \ : \ \nu \in \llbracket \phi \rrbracket \text{ for some } \nu : \ (\omega,\nu) \in \llbracket \alpha \rrbracket\} \\
\llbracket [\alpha]\phi \rrbracket &= \llbracket \neg\langle\alpha\rangle\neg\phi \rrbracket = \{\omega \ : \ \nu \in \llbracket \phi \rrbracket \text{ for all } \nu : \ (\omega,\nu) \in \llbracket \alpha \rrbracket\} \\
\llbracket \exists x\, \phi \rrbracket &= \{\omega \ : \ \omega_x^r \in \llbracket \phi \rrbracket \text{ for some } r \in \mathbb{R}\}
\end{aligned}
$$

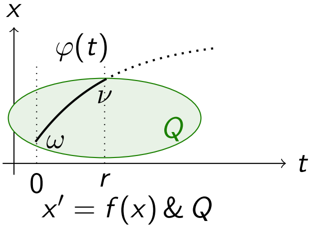
Differential Dynamic Logic d$\mathcal{L}$: Transition Semantics

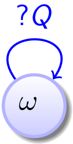




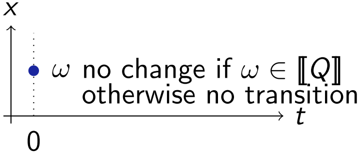
if $\nu(x) = [\![e]\!]\omega$
and $\nu(z) = \omega(z)$ for $z \neq x$





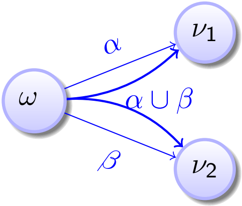


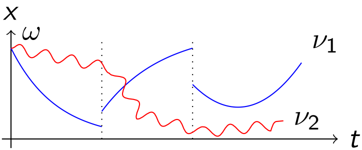
if $\omega \in [\![Q]\!]$

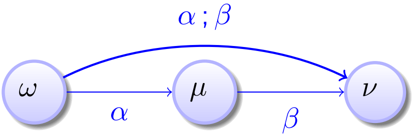


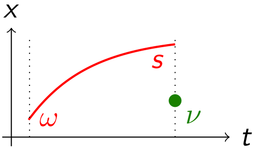
no change if $\omega \in [\![Q]\!]$
otherwise no transition

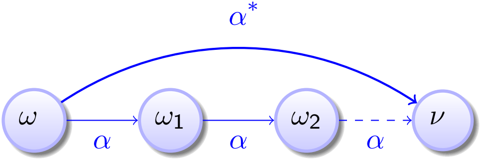
Differential Dynamic Logic d$\mathcal{L}$: Transition Semantics

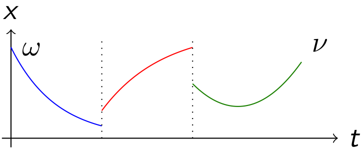




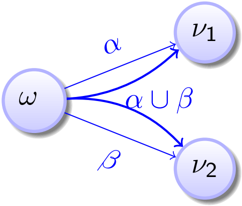


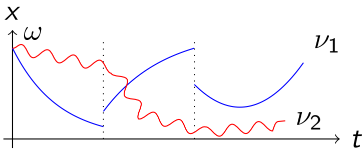


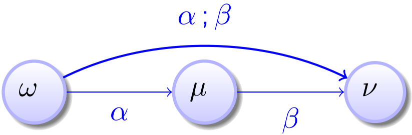


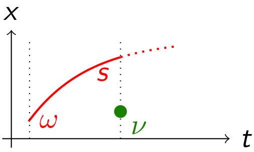


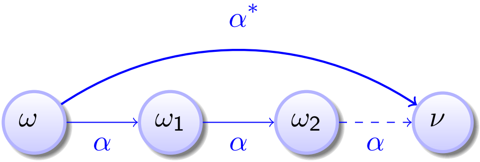
Differential Dynamic Logic d$\mathcal{L}$: Transition Semantics

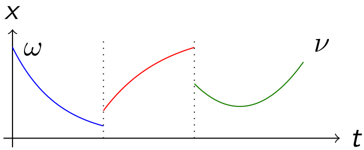




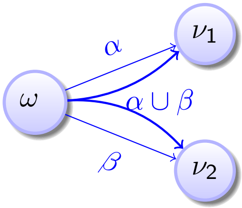


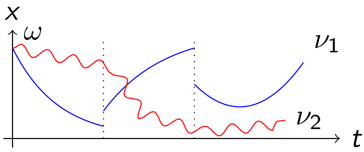


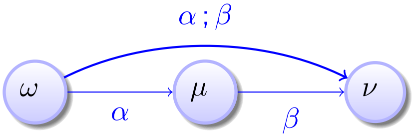


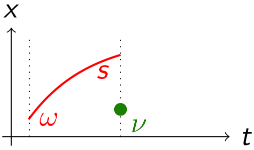


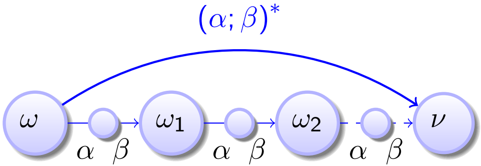
Differential Dynamic Logic d$\mathcal{L}$: Transition Semantics

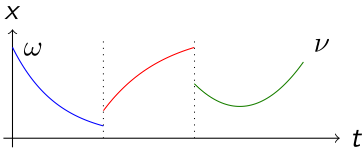




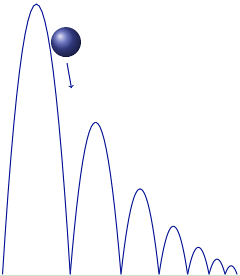








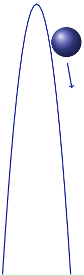
Conjecture: Quantum the Acrophobic Bouncing Ball



Example (Quantum the Bouncing Ball))

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

Conjecture: Quantum the Acrophobic Bouncing Ball

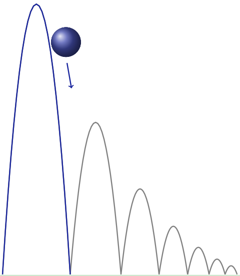


Example (Quantum the Bouncing Ball) (Single-hop)

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

Removing the repetition grotesquely changes the behavior to a single hop

Conjecture: Quantum the Acrophobic Bouncing Ball



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

$$0 \le x \land x = H \land v = 0 \land g > 0 \land 1 \ge c \ge 0 \rightarrow$$
$$\left[\; x' = v, v' = -g \,\&\, x \ge 0; (?x = 0; v := -cv \cup ?x \ne 0) \;\right] (0 \le x \land x \le H)$$

Removing the repetition grotesquely changes the behavior to a single hop

A Proof of a Short Single-hop Bouncing Ball

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

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

$$B(x,v) \overset{\text{def}}{\equiv} 0 \leq x \land x \leq H$$

$$(x'' = -g) \overset{\text{def}}{\equiv} (x' = v, v' = -g)$$

A Proof of a Short Single-hop Bouncing Ball

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

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

$$B(x,v) \overset{\text{def}}{\equiv} 0 \leq x \land x \leq H$$

$$(x''=-g) \overset{\text{def}}{\equiv} (x'=v, v'=-g)$$

A Proof of a Short Single-hop Bouncing Ball

$$
\text{[;]}\;\dfrac{\text{[}\cup\text{]}\;\dfrac{\text{[;]}\;\dfrac{}{A \vdash [x''=-g]\big([?x=0;\, v:=-cv]B(x,v) \land [?x \geq 0]B(x,v)\big)}}{A \vdash [x''=-g][?x=0;\, v:=-cv \cup ?x \geq 0]B(x,v)}}{A \vdash [x''=-g;\, (?x=0;\, v:=-cv \cup ?x \geq 0)]B(x,v)}
$$

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

$$B(x,v) \overset{\text{def}}{\equiv} 0 \leq x \land x \leq H$$

$$(x''=-g) \overset{\text{def}}{\equiv} (x'=v, v'=-g)$$

A Proof of a Short Single-hop Bouncing Ball

$$\begin{array}{rl}
\text{[?],[?]} & \overline{A \vdash [x'' = -g]\big([?x = 0][v := -cv]B(x,v) \land [?x \geq 0]B(x,v)\big)} \\
\text{[;]} & \overline{A \vdash [x'' = -g]\big([?x = 0; v := -cv]B(x,v) \land [?x \geq 0]B(x,v)\big)} \\
\text{[}\cup\text{]} & \overline{A \vdash [x'' = -g][?x = 0; v := -cv \cup ?x \geq 0]B(x,v)} \\
\text{[;]} & \overline{A \vdash [x'' = -g; (?x = 0; v := -cv \cup ?x \geq 0)]B(x,v)}
\end{array}$$

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

$$B(x,v) \overset{\text{def}}{\equiv} 0 \leq x \land x \leq H$$

$$(x'' = -g) \overset{\text{def}}{\equiv} (x' = v, v' = -g)$$

A Proof of a Short Single-hop Bouncing Ball

$$\begin{array}{rl}
{[:=]} & \overline{A \vdash [x'' = -g]\big((x = 0 \to [v := -cv]B_{(x,v)}) \land (x \geq 0 \to B_{(x,v)})\big)} \\
{[?],[?]} & \overline{A \vdash [x'' = -g]\big([?x = 0][v := -cv]B_{(x,v)} \land [?x \geq 0]B_{(x,v)}\big)} \\
{[;]} & \overline{A \vdash [x'' = -g]\big([?x = 0; v := -cv]B_{(x,v)} \land [?x \geq 0]B_{(x,v)}\big)} \\
{[\cup]} & \overline{A \vdash [x'' = -g][?x = 0; v := -cv \cup ?x \geq 0]B_{(x,v)}} \\
{[;]} & \overline{A \vdash [x'' = -g; (?x = 0; v := -cv \cup ?x \geq 0)]B_{(x,v)}}
\end{array}$$

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

$$B_{(x,v)} \overset{\text{def}}{\equiv} 0 \leq x \land x \leq H$$

$$(x'' = -g) \overset{\text{def}}{\equiv} (x' = v, v' = -g)$$

A Proof of a Short Single-hop Bouncing Ball

$$
\begin{array}{rl}
\hline
[{}'] & A \vdash [x''=-g]\big((x=0 \to B_{(x,-cv)}) \land (x \geq 0 \to B_{(x,v)})\big) \\ \hline
[:=] & A \vdash [x''=-g]\big((x=0 \to [v:=-cv]B_{(x,v)}) \land (x \geq 0 \to B_{(x,v)})\big) \\ \hline
[?],[?] & A \vdash [x''=-g]\big([?x=0][v:=-cv]B_{(x,v)} \land [?x \geq 0]B_{(x,v)}\big) \\ \hline
[;] & A \vdash [x''=-g]\big([?x=0;v:=-cv]B_{(x,v)} \land [?x \geq 0]B_{(x,v)}\big) \\ \hline
[\cup] & A \vdash [x''=-g][?x=0;v:=-cv \cup ?x \geq 0]B_{(x,v)} \\ \hline
[;] & A \vdash [x''=-g;(?x=0;v:=-cv \cup ?x \geq 0)]B_{(x,v)}
\end{array}
$$

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

$$B_{(x,v)} \overset{\text{def}}{\equiv} 0 \leq x \land x \leq H$$

$$(x''=-g) \overset{\text{def}}{\equiv} (x'=v, v'=-g)$$

A Proof of a Short Single-hop Bouncing Ball

$$\begin{array}{ll}
\text{[;]} & \overline{A \vdash \forall t{\geq}0\, [x := H - \tfrac{g}{2}t^2; v := -gt]\big((x{=}0 \to B_{(x,-cv)}) \land (x{\geq}0 \to B_{(x,v)})} \\
\text{[$'$]} & \overline{A \vdash [x'' = -g]\big((x = 0 \to B_{(x,-cv)}) \land (x \geq 0 \to B_{(x,v)})\big)} \\
\text{[:=]} & \overline{A \vdash [x'' = -g]\big((x = 0 \to [v := -cv]B_{(x,v)}) \land (x \geq 0 \to B_{(x,v)})\big)} \\
\text{[?],[?]} & \overline{A \vdash [x'' = -g]\big([?x = 0][v := -cv]B_{(x,v)} \land [?x \geq 0]B_{(x,v)}\big)} \\
\text{[;]} & \overline{A \vdash [x'' = -g]\big([?x = 0; v := -cv]B_{(x,v)} \land [?x \geq 0]B_{(x,v)}\big)} \\
\text{[$\cup$]} & \overline{A \vdash [x'' = -g][?x = 0; v := -cv \cup ?x \geq 0]B_{(x,v)}} \\
\text{[;]} & \overline{A \vdash [x'' = -g; (?x = 0; v := -cv \cup ?x \geq 0)]B_{(x,v)}}
\end{array}$$

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

$$B_{(x,v)} \overset{\text{def}}{\equiv} 0 \leq x \land x \leq H$$

$$(x'' = -g) \overset{\text{def}}{\equiv} (x' = v, v' = -g)$$

A Proof of a Short Single-hop Bouncing Ball

$$\begin{array}{rl}
[:=] & \overline{A \vdash \forall t{\geq}0\,[x := H - \frac{g}{2}t^2][v := -gt]\big((x{=}0 \to B_{(x,-cv)}) \land (x{\geq}0 \to B_{(x,v)})} \\
[;] & \overline{A \vdash \forall t{\geq}0\,[x := H - \frac{g}{2}t^2;\, v := -gt]\big((x{=}0 \to B_{(x,-cv)}) \land (x{\geq}0 \to B_{(x,v)})} \\
['] & \overline{A \vdash [x'' = -g]\big((x = 0 \to B_{(x,-cv)}) \land (x \geq 0 \to B_{(x,v)})\big)} \\
[:=] & \overline{A \vdash [x'' = -g]\big((x = 0 \to [v := -cv]B_{(x,v)}) \land (x \geq 0 \to B_{(x,v)})\big)} \\
[?],[?] & \overline{A \vdash [x'' = -g]\big([?x = 0][v := -cv]B_{(x,v)} \land [?x \geq 0]B_{(x,v)}\big)} \\
[;] & \overline{A \vdash [x'' = -g]\big([?x = 0; v := -cv]B_{(x,v)} \land [?x \geq 0]B_{(x,v)}\big)} \\
[\cup] & \overline{A \vdash [x'' = -g][?x = 0; v := -cv \cup ?x \geq 0]B_{(x,v)}} \\
[;] & \overline{A \vdash [x'' = -g; (?x = 0; v := -cv \cup ?x \geq 0)]B_{(x,v)}}
\end{array}$$

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

$$B_{(x,v)} \overset{\text{def}}{\equiv} 0 \leq x \land x \leq H$$

$$(x'' = -g) \overset{\text{def}}{\equiv} (x' = v, v' = -g)$$

A Proof of a Short Single-hop Bouncing Ball

$$
\begin{array}{rl}
\text{[:=]} & \overline{A \vdash \forall t{\geq}0\,[x := H - \tfrac{g}{2}t^2]\big((x{=}0 \to B(x,-c(-gt))) \land (x{\geq}0 \to B(x,-gt))\big)} \\
\text{[:=]} & \overline{A \vdash \forall t{\geq}0\,[x := H - \tfrac{g}{2}t^2][v := -gt]\big((x{=}0 \to B(x,-cv)) \land (x{\geq}0 \to B(x,v))} \\
\text{[;]} & \overline{A \vdash \forall t{\geq}0\,[x := H - \tfrac{g}{2}t^2; v := -gt]\big((x{=}0 \to B(x,-cv)) \land (x{\geq}0 \to B(x,v))} \\
\text{[$'$]} & \overline{A \vdash [x'' = -g]\big((x = 0 \to B(x,-cv)) \land (x \geq 0 \to B(x,v))\big)} \\
\text{[:=]} & \overline{A \vdash [x'' = -g]\big((x = 0 \to [v := -cv]B(x,v)) \land (x \geq 0 \to B(x,v))\big)} \\
\text{[?],[?]} & \overline{A \vdash [x'' = -g]\big([?x = 0][v := -cv]B(x,v) \land [?x \geq 0]B(x,v)\big)} \\
\text{[;]} & \overline{A \vdash [x'' = -g]\big([?x = 0; v := -cv]B(x,v) \land [?x \geq 0]B(x,v)\big)} \\
\text{[$\cup$]} & \overline{A \vdash [x'' = -g][?x = 0; v := -cv \cup ?x \geq 0]B(x,v)} \\
\text{[;]} & A \vdash [x'' = -g; (?x = 0; v := -cv \cup ?x \geq 0)]B(x,v)
\end{array}
$$

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

$$B(x,v) \overset{\text{def}}{\equiv} 0 \leq x \land x \leq H$$

$$(x'' = -g) \overset{\text{def}}{\equiv} (x' = v, v' = -g)$$

A Proof of a Short Single-hop Bouncing Ball

$$\begin{array}{rl}
 & A \vdash \forall t{\geq}0\, \big((H{-}\tfrac{g}{2}t^2{=}0{\rightarrow}B_{(H-\frac{g}{2}t^2,-c(-gt))}\big) \land \big(H{-}\tfrac{g}{2}t^2{\geq}0{\rightarrow}B_{(H-\frac{g}{2}t^2,-gt)} \\
\hline
[:=] & A \vdash \forall t{\geq}0\, [x := H - \tfrac{g}{2}t^2]\big((x{=}0 \rightarrow B_{(x,-c(-gt))}) \land (x{\geq}0 \rightarrow B_{(x,-gt)})\big) \\
\hline
[:=] & A \vdash \forall t{\geq}0\, [x := H - \tfrac{g}{2}t^2][v := -gt]\big((x{=}0 \rightarrow B_{(x,-cv)}) \land (x{\geq}0 \rightarrow B_{(x,v)}) \\
\hline
[;] & A \vdash \forall t{\geq}0\, [x := H - \tfrac{g}{2}t^2; v := -gt]\big((x{=}0 \rightarrow B_{(x,-cv)}) \land (x{\geq}0 \rightarrow B_{(x,v)}) \\
\hline
['] & A \vdash [x'' = -g]\big((x = 0 \rightarrow B_{(x,-cv)}) \land (x \geq 0 \rightarrow B_{(x,v)})\big) \\
\hline
[:=] & A \vdash [x'' = -g]\big((x = 0 \rightarrow [v := -cv]B_{(x,v)}) \land (x \geq 0 \rightarrow B_{(x,v)})\big) \\
\hline
[?],[?] & A \vdash [x'' = -g]\big([?x = 0][v := -cv]B_{(x,v)} \land [?x \geq 0]B_{(x,v)}\big) \\
\hline
[;] & A \vdash [x'' = -g]\big([?x = 0; v := -cv]B_{(x,v)} \land [?x \geq 0]B_{(x,v)}\big) \\
\hline
[\cup] & A \vdash [x'' = -g][?x = 0; v := -cv \cup ?x \geq 0]B_{(x,v)} \\
\hline
[;] & A \vdash [x'' = -g; (?x = 0; v := -cv \cup ?x \geq 0)]B_{(x,v)}
\end{array}$$

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

$$B_{(x,v)} \overset{\text{def}}{\equiv} 0 \leq x \land x \leq H$$

$$(x'' = -g) \overset{\text{def}}{\equiv} (x' = v, v' = -g)$$

A Proof of a Short Single-hop Bouncing Ball

$$\begin{array}{rl}
 & A \vdash \forall t{\geq}0\, \big((H{-}\frac{g}{2}t^2{=}0{\to}B_{(H-\frac{g}{2}t^2,-c(-gt))}\big) \land \big(H{-}\frac{g}{2}t^2{\geq}0{\to}B_{(H-\frac{g}{2}t^2,-gt)} \\ \hline
[:=] & A \vdash \forall t{\geq}0\, [x := H - \frac{g}{2}t^2]\big((x{=}0 \to B_{(x,-c(-gt))}) \land (x{\geq}0 \to B_{(x,-gt)})\big) \\ \hline
[:=] & A \vdash \forall t{\geq}0\, [x := H - \frac{g}{2}t^2][v := -gt]\big((x{=}0 \to B_{(x,-cv)}) \land (x{\geq}0 \to B_{(x,v)}) \\ \hline
[;] & A \vdash \forall t{\geq}0\, [x := H - \frac{g}{2}t^2;\, v := -gt]\big((x{=}0 \to B_{(x,-cv)}) \land (x{\geq}0 \to B_{(x,v)}) \\ \hline
['] & A \vdash [x'' = -g]\big((x = 0 \to B_{(x,-cv)}) \land (x \geq 0 \to B_{(x,v)})\big) \\ \hline
[:=] & A \vdash [x'' = -g]\big((x = 0 \to [v := -cv]B_{(x,v)}) \land (x \geq 0 \to B_{(x,v)})\big) \\ \hline
[?],[?] & A \vdash [x'' = -g]\big([?x = 0][v := -cv]B_{(x,v)} \land [?x \geq 0]B_{(x,v)}\big) \\ \hline
[;] & A \vdash [x'' = -g]\big([?x = 0;\, v := -cv]B_{(x,v)} \land [?x \geq 0]B_{(x,v)}\big) \\ \hline
[\cup] & A \vdash [x'' = -g][?x = 0;\, v := -cv \cup ?x \geq 0]B_{(x,v)} \\ \hline
[;] & A \vdash [x'' = -g;\, (?x = 0;\, v := -cv \cup ?x \geq 0)]B_{(x,v)}
\end{array}$$

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

$$B_{(x,v)} \overset{\text{def}}{\equiv} 0 \leq x \land x \leq H$$

$$(x'' = -g) \overset{\text{def}}{\equiv} (x' = v, v' = -g)$$

A Proof of a Short Single-hop Bouncing Ball

Resolving abbreviations at the premise yields:

$$
\begin{aligned}
&0 \leq x \land x = H \land v = 0 \land g > 0 \land 1 \geq c \geq 0 \rightarrow \\
&\qquad \forall t{\geq}0 \left((H - \frac{g}{2}t^2 = 0 \rightarrow 0 \leq H - \frac{g}{2}t^2 \land H - \frac{g}{2}t^2 \leq H)\right. \\
&\qquad\qquad \left.\land (H - \frac{g}{2}t^2 \geq 0 \rightarrow 0 \leq H - \frac{g}{2}t^2 \land H - \frac{g}{2}t^2 \leq H)\right)
\end{aligned}
$$

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

A Proof of a Short Single-hop Bouncing Ball

Resolving abbreviations at the premise yields:

$$
\begin{aligned}
&0 \leq x \land x = H \land v = 0 \land g > 0 \land 1 \geq c \geq 0 \rightarrow \\
&\qquad \forall t{\geq}0 \left(\left(H - \frac{g}{2}t^2 = 0 \rightarrow 0 \leq H - \frac{g}{2}t^2 \land H - \frac{g}{2}t^2 \leq H\right) \right. \\
&\qquad\qquad \left. \land \left({\color{red}H - \frac{g}{2}t^2 \geq 0} \rightarrow 0 \leq H - \frac{g}{2}t^2 \land H - \frac{g}{2}t^2 \leq H\right) \right)
\end{aligned}
$$

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

Real arithmetic is decidable

Let φ be a first-order formula using addition and multiplication (possibly with $\forall/\exists$).

Real arithmetic is decidable

Let φ be a first-order formula using addition and multiplication (possibly with $\forall/\exists$).

Reminder:

$\mathbb{N} \models \varphi$ is not decidable, not even recursive enumerable (Gödel).

Real arithmetic is decidable

Let φ be a first-order formula using addition and multiplication (possibly with $\forall/\exists$).

Reminder:

$\mathbb{N} \models \varphi$ is not decidable, not even recursive enumerable (Gödel).

Tarski-Seidenberg theorem (c. 1948)

$\mathbb{R} \models \varphi$ **is** decidable.
Complexity is double exponential (c. 1988).

Real arithmetic is decidable

Let φ be a first-order formula using addition and multiplication (possibly with $\forall/\exists$).

Reminder:

$\mathbb{N} \models \varphi$ is not decidable, not even recursive enumerable (Gödel).

Tarski-Seidenberg theorem (c. 1948)

$\mathbb{R} \models \varphi$ **is** decidable.
Complexity is double exponential (c. 1988).

Idea: *Quantifier elimination*

Find formula ψ such that $(\exists x.\varphi(x, y)) \leftrightarrow \psi(y)$.
Computer algebra systems do this: REDLOG, Mathematica, (Z3)

Semialgebraic sets

Semialgebraic set

$S \subseteq \mathbb{R}^n$ is called *semialgebraic* if it is a boolean combination of sets of the shape $\{\bar{x} \in \mathbb{R}^n \mid p(\bar{x}) > 0\}$ for polynomials $p \in \mathbb{Z}[\bar{x}]$.

Semialgebraic sets

Semialgebraic set

$S \subseteq \mathbb{R}^n$ is called *semialgebraic* if it is a boolean combination of sets of the shape $\{\bar{x} \in \mathbb{R}^n \mid p(\bar{x}) > 0\}$ for polynomials $p \in \mathbb{Z}[\bar{x}]$.

S is semialgebaric iff there is a quantifier-free FOL-formula $\varphi(S)$ with n free variables $x_1, \ldots, x_n$ such that

$$(s_1, \ldots, s_n) \in S \iff \mathbb{R}, [x_1 \mapsto s_1, \ldots, x_n \mapsto s_n] \models \varphi(S)$$

Tarski-Seidenberg Theorem

Definition: *Projection* $\pi_n : \mathbb{R}^n \to \mathbb{R}^{n-1}$

Tarski-Seidenberg Theorem

Definition: *Projection* $\pi_n : \mathbb{R}^n \to \mathbb{R}^{n-1}$

$$\pi_n((s_1, ..., s_n)) := (s_1, ..., s_{n-1})$$

$$\pi_n(S) := \{\pi_n(\bar{s}) \mid \bar{s} \in S\} \qquad \text{(extended to } 2^{\mathbb{R}}\text{)}$$

Tarski-Seidenberg Theorem

Definition: *Projection* $\pi_n : \mathbb{R}^n \to \mathbb{R}^{n-1}$

$$\pi_n((s_1, \ldots, s_n)) := (s_1, \ldots, s_{n-1})$$

$$\pi_n(S) := \{\pi_n(\bar{s}) \mid \bar{s} \in S\} \qquad \text{(extended to } 2^{\mathbb{R}}\text{)}$$

$$(s_1, \ldots, s_{n-1}) \in \pi_n(S) \iff \mathbb{R}, [x_1 \mapsto s_1, \ldots, x_{n-1} \mapsto s_{n-1}] \models \exists x_n.\, \varphi(S)$$

Tarski-Seidenberg Theorem

Definition: *Projection* $\pi_n : \mathbb{R}^n \to \mathbb{R}^{n-1}$

$$\pi_n((s_1, \dots, s_n)) := (s_1, \dots, s_{n-1})$$

$$\pi_n(S) := \{\pi_n(\bar{s}) \mid \bar{s} \in S\} \qquad \text{(extended to } 2^{\mathbb{R}}\text{)}$$

$$(s_1, \dots, s_{n-1}) \in \pi_n(S) \iff \mathbb{R}, [x_1 \mapsto s_1, \dots, x_{n-1} \mapsto s_{n-1}] \models \exists x_n.\, \varphi(S)$$

Tarski-Seidenberg Theorem (*Projektionssatz*)

Let $S \subseteq \mathbb{R}^n$ be semialgebraic.
Then $\pi_n(S) \in \mathbb{R}^{n-1}$ is also semialgebraic.

Example

Single variable, single quadratic equation

Let S_{quad} be the solutions of $ax^2 + bx + c = 0$.
(is semialgebraic: $ax^2 + bx + c \in \mathbb{R}[a, b, c, x]$)

Example

Single variable, single quadratic equation

Let S_{quad} be the solutions of $ax^2 + bx + c = 0$.
(is semialgebraic: $ax^2 + bx + c \in \mathbb{R}[a, b, c, x]$)

Due to Tarski-Seidenberg, there must be an equiv. quantifier-free formula $\varphi(\pi_4(S_{quad}))$ with free variables a, b, c.

$$\exists x. ax^2 + bx + c = 0$$

$$\Longleftrightarrow$$

Example

Single variable, single quadratic equation

Let S_{quad} be the solutions of $ax^2 + bx + c = 0$.
(is semialgebraic: $ax^2 + bx + c \in \mathbb{R}[a, b, c, x]$)

Due to Tarski-Seidenberg, there must be an equiv. quantifier-free formula $\varphi(\pi_4(S_{quad}))$ with free variables a, b, c.

$$\exists x. ax^2 + bx + c = 0$$

$$\iff$$

$$\begin{gathered}(a \neq 0 \wedge b^2 - 4ac \geq 0) \\ \vee (a = 0 \wedge (b = 0 \rightarrow c = 0))\end{gathered}$$

Example

Single variable, single quadratic equation

Let S_{quad} be the solutions of $ax^2 + bx + c = 0$.
(is semialgebraic: $ax^2 + bx + c \in \mathbb{R}[a, b, c, x]$)

Due to Tarski-Seidenberg, there must be an equiv. quantifier-free formula $\varphi(\pi_4(S_{quad}))$ with free variables a, b, c.

$$\exists x. ax^2 + bx + c = 0$$

$$\Longleftrightarrow$$

$$\begin{gathered}(a \neq 0 \land b^2 - 4ac \geq 0) \\ \lor (a = 0 \land (b = 0 \to c = 0))\end{gathered}$$

$\big(\exists x. x^3 + a_2x^2 + a_1x + a_0 = 0$ is trivally equivalent to true.$\big)$

Quantifier Elimination – Algorithm

① Sufficient to look at $\exists x. \bigwedge_i \phi_i(\bar{y}, x)$ for atomic ϕ_i. → Why?

Quantifier Elimination – Algorithm

1. Sufficient to look at $\exists x. \bigwedge_i \phi_i(\bar{y}, x)$ for atomic ϕ_i. → Why?
2. Sufficient to consider ϕ_i of shape $p(\bar{y}, x) \left\{ \begin{smallmatrix} < \\ > \\ = \end{smallmatrix} \right\} 0$ for $p \in \mathbb{R}[\bar{y}][x]$ → Why?

Quantifier Elimination – Algorithm

1. Sufficient to look at $\exists x. \bigwedge_i \phi_i(\bar{y}, x)$ for atomic ϕ_i. → Why?
2. Sufficient to consider ϕ_i of shape $p(\bar{y}, x) \left\{\begin{matrix} < \\ > \\ = \end{matrix}\right\} 0$ for $p \in \mathbb{R}[\bar{y}][x]$ → Why?
3. Every polynomial $p \in R[x]$ has finitely many connected regions with same sign. → Board
   Choose a set *Rep* of representatives.

Quantifier Elimination – Algorithm

1. Sufficient to look at $\exists x. \bigwedge_i \phi_i(\bar{y}, x)$ for atomic ϕ_i. → Why?
2. Sufficient to consider ϕ_i of shape $p(\bar{y}, x) \left\{ \begin{matrix} < \\ > \\ = \end{matrix} \right\} 0$ for $p \in \mathbb{R}[\bar{y}][x]$ → Why?
3. Every polynomial $p \in R[x]$ has finitely many connected regions with same sign. → Board
   Choose a set *Rep* of representatives.
4. $\exists x. \bigwedge\limits_i \phi_i(x, \bar{y}) \leftrightarrow \bigvee\limits_{r \in Rep} \bigwedge\limits_i \phi_i(r, \bar{y})$

Quantifier Elimination – Linear Example

In $\mathbb{R}[z, x]$:

$$\psi := \qquad \exists x. x > 2 \land x < 3 \land x > z$$

Quantifier Elimination – Linear Example

In $\mathbb{R}[z, x]$:

$$\psi := \qquad \exists x. x > 2 \land x < 3 \land x > z$$

- Interesting points for x: $I = \{2, 3, z\}$

Quantifier Elimination – Linear Example

In $\mathbb{R}[z, x]$:

$$\psi := \qquad \exists x . x > 2 \land x < 3 \land x > z$$

- Interesting points for x: $I = \{2, 3, z\}$
- Interesting intervals: $(-\infty, 2)$, $(2, 3)$, $(3, \infty)$, $(2, z)$, …

Quantifier Elimination – Linear Example

In $\mathbb{R}[z, x]$:

$$\psi := \qquad \exists x . x > 2 \land x < 3 \land x > z$$

- Interesting points for x: $I = \{2, 3, z\}$
- Interesting intervals: $(-\infty, 2)$, $(2, 3)$, $(3, \infty)$, $(2, z)$, ...
- Representatives:

$$\begin{aligned} Rep &= \left\{2, 3, z, \text{“}-\infty\text{”}, \text{“}+\infty\text{”}, \tfrac{2+3}{2}, \tfrac{2+z}{2}, \tfrac{3+z}{2}\right\} \\ &= \left\{\tfrac{i_1+i_2}{2} \mid i_1, i_2 \in I\right\} \cup \left\{\text{“}-\infty\text{”}, \text{“}+\infty\text{”}\right\} \end{aligned}$$

Quantifier Elimination – Linear Example

In $\mathbb{R}[z, x]$:

$$\psi := \qquad \exists x. x > 2 \land x < 3 \land x > z$$

- Interesting points for x: $I = \{2, 3, z\}$
- Interesting intervals: $(-\infty, 2)$, $(2, 3)$, $(3, \infty)$, $(2, z)$, ...
- Representatives:

$$\begin{aligned} Rep &= \left\{2, 3, z, \text{“}{-\infty}\text{”}, \text{“}{+\infty}\text{”}, \tfrac{2+3}{2}, \tfrac{2+z}{2}, \tfrac{3+z}{2}\right\} \\ &= \left\{\tfrac{i_1+i_2}{2} \mid i_1, i_2 \in I\right\} \cup \left\{\text{“}{-\infty}\text{”}, \text{“}{+\infty}\text{”}\right\} \end{aligned}$$

Quantifier Elimination – Linear Example

In $\mathbb{R}[z,x]$:

$$\psi := \qquad \exists x. x > 2 \land x < 3 \land x > z$$

- Interesting points for x: $I = \{2, 3, z\}$
- Interesting intervals: $(-\infty, 2)$, $(2, 3)$, $(3, \infty)$, $(2, z)$, $\ldots$
- Representatives:

$$\begin{aligned} Rep &= \left\{2, 3, z, \text{“}-\infty\text{”}, \text{“}+\infty\text{”}, \tfrac{2+3}{2}, \tfrac{2+z}{2}, \tfrac{3+z}{2}\right\} \\ &= \left\{\tfrac{i_1+i_2}{2} \mid i_1, i_2 \in I\right\} \cup \{\text{“}-\infty\text{”}, \text{“}+\infty\text{”}\} \end{aligned}$$

For the example:

$$\begin{aligned} \psi &\leftrightarrow \bigvee_{r \in Rep} r > 2 \land r < 3 \land x > z \\ &\leftrightarrow 2.5 > z \lor (z > 2 \land z < 4 \land 2 > z) \lor (z > 1 \land z < 3 \land 3 > z) \\ &\leftrightarrow \end{aligned}$$

Quantifier Elimination – Linear Example

In $\mathbb{R}[z, x]$:

$$\psi := \qquad \exists x. x > 2 \land x < 3 \land x > z$$

- Interesting points for x: $I = \{2, 3, z\}$
- Interesting intervals: $(-\infty, 2)$, $(2, 3)$, $(3, \infty)$, $(2, z)$, …
- Representatives:

$$\begin{aligned} Rep &= \left\{2, 3, z, \text{“}-\infty\text{”}, \text{“}+\infty\text{”}, \tfrac{2+3}{2}, \tfrac{2+z}{2}, \tfrac{3+z}{2}\right\} \\ &= \left\{\tfrac{i_1+i_2}{2} \mid i_1, i_2 \in I\right\} \cup \{\text{“}-\infty\text{”}, \text{“}+\infty\text{”}\} \end{aligned}$$

For the example:

$$\begin{aligned} \psi \quad &\leftrightarrow \quad \bigvee_{r \in Rep} r > 2 \land r < 3 \land x > z \\ &\leftrightarrow \quad 2.5 > z \lor (z > 2 \land z < 4 \land 2 > z) \lor (z > 1 \land z < 3 \land 3 > z) \\ &\leftrightarrow \quad z < 3 \end{aligned}$$

More QE: Presburger Arithmetic

Presburger Arithmetic (1929)

Presburger Arithmetic is the theory of $\mathbb{N}$-valid first order-formulas over the signature which contains symbols $0, 1, +$ (but **not** $\cdot$)

More QE: Presburger Arithmetic

Presburger Arithmetic (1929)

Presburger Arithmetic is the theory of $\mathbb{N}$-valid first order-formulas over the signature which contains symbols $0, 1, +$ (but **not** $\cdot$)

Presburger Arithmetic is axiomatizable:

1. $\forall x.\ x + 0 = 0 \land \neg x + 1 = 0$
2. $\forall x, y.\ x + 1 = y + 1 \rightarrow x = y$
3. $\forall x, y, z.\ (x + y) + z = x + (y + z)$
4. $P(0) \land (\forall x.\ P(x) \rightarrow P(x + 1)) \rightarrow (\forall x.\ P(x))$ for some formula P

More QE: Presburger Arithmetic

Presburger Arithmetic (1929)

Presburger Arithmetic is the theory of $\mathbb{N}$-valid first order-formulas over the signature which contains symbols $0, 1, +$ (but **not** $\cdot$)

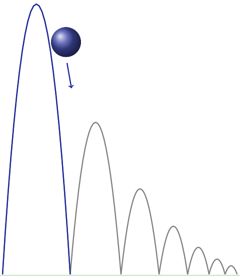
Presburger Arithmetic is axiomatizable:

1. $\forall x.\ x + 0 = 0 \land \neg x + 1 = 0$
2. $\forall x, y.\ x + 1 = y + 1 \rightarrow x = y$
3. $\forall x, y, z.\ (x + y) + z = x + (y + z)$
4. $P(0) \land (\forall x.\ P(x) \rightarrow P(x + 1)) \rightarrow (\forall x.\ P(x))$ for some formula P

Presburger Arithmetic is Decidable

P.A. supports quantifier elimination. (→ Cooper's Algorithm)
(Complexity theoretically double exponential, in practice often better)

Conjecture: Quantum the Acrophobic Bouncing Ball



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

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

Removing the repetition grotesquely changes the behavior to a single hop

Hybrid Programs and Loop Invariants

Repeatedly bouncing ball

$$0 \leq x \land x = H \land v = 0 \land g > 0 \land 0 < c \leq 1 \rightarrow$$
$$[(x'' = -g \,\&\, x \geq 0 \,;\, \text{if } x = 0 \text{ then } v := -c \cdot v)^*](0 \leq x \leq H)$$

Use discrete invariant rules from DL to prove hybrid proof obligation.

Sequent Calculus Rules

$$\text{loop}\ \frac{\Gamma \vdash \mathit{INV}, \Delta \qquad \mathit{INV} \vdash [\alpha]\mathit{INV} \qquad \mathit{INV} \vdash \mathit{SAFE}}{\Gamma \vdash [\alpha^*]\mathit{SAFE}, \Delta}$$

Sequent Calculus Rules

$$\text{loop}\,\frac{\Gamma \vdash \mathit{INV}, \Delta \qquad \mathit{INV} \vdash [\alpha]\mathit{INV} \qquad \mathit{INV} \vdash \mathit{SAFE}}{\Gamma \vdash [\alpha^*]\mathit{SAFE}, \Delta}$$

$$\text{MR}\,\frac{\Gamma \vdash [\alpha]\Phi, \Delta \qquad \Phi \vdash [\beta]\mathit{SAFE}}{\Gamma \vdash [\alpha\ ;\ \beta]\mathit{SAFE}, \Delta}$$

Sequent Calculus Rules

$$\text{loop}\ \frac{\Gamma \vdash \mathit{INV}, \Delta \qquad \mathit{INV} \vdash [\alpha]\mathit{INV} \qquad \mathit{INV} \vdash \mathit{SAFE}}{\Gamma \vdash [\alpha^*]\mathit{SAFE}, \Delta}$$

$$\text{MR}\ \frac{\Gamma \vdash [\alpha]\Phi, \Delta \qquad \Phi \vdash [\beta]\mathit{SAFE}}{\Gamma \vdash [\alpha\ ;\ \beta]\mathit{SAFE}, \Delta}$$

$$[']\ \frac{\Gamma \vdash \forall t \geq 0.([x := X(t)]\phi), \Delta}{\Gamma \vdash [x' = t\ \&\ Q(x)]\phi, \Delta}$$

Sequent Calculus Rules

$$\text{loop}\,\frac{\Gamma \vdash \mathit{INV}, \Delta \qquad \mathit{INV} \vdash [\alpha]\mathit{INV} \qquad \mathit{INV} \vdash \mathit{SAFE}}{\Gamma \vdash [\alpha^*]\mathit{SAFE}, \Delta}$$

$$\text{MR}\,\frac{\Gamma \vdash [\alpha]\Phi, \Delta \qquad \Phi \vdash [\beta]\mathit{SAFE}}{\Gamma \vdash [\alpha\ ;\ \beta]\mathit{SAFE}, \Delta}$$

$$[']\,\frac{\Gamma \vdash \forall t \geq 0.((\forall t'.0 \leq t' \leq t \rightarrow Q(t')) \rightarrow [x := X(t)]\phi), \Delta}{\Gamma \vdash [x' = t\ \&\ Q(x)]\phi, \Delta}$$

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

$$\frac{}{j(x,v) \vdash [x''=;\,(?x=0;\,v:=-cv \cup ?x\neq0]j(x,v)}$$

$$\text{loop}\ \frac{A \vdash j(x,v) \qquad [;]\,\dfrac{}{j(x,v) \vdash [x''=;\,(?x=0;\,v:=-cv \cup ?x\neq0]j(x,v)} \qquad j(x,v) \vdash B(x,v)}{A \vdash \big[\big(x''=;\,(?x=0;\,v:=-cv \cup ?x\neq0)\big)^{*}\big]B(x,v)}$$

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

$$\text{[;]}\,\dfrac{\text{MR}\,\dfrac{j(x,v) \vdash [x''=]j(x,v) \qquad \dfrac{}{j(x,v) \vdash [?x=0;\, v:=-cv \cup ?x\neq0]j(x,v)}}{j(x,v) \vdash [x''=][?x=0;\, v:=-cv \cup ?x\neq0]j(x,v)}}{j(x,v) \vdash [x''=;\, (?x=0;\, v:=-cv \cup ?x\neq0]j(x,v)}$$

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

$$\text{[;]}\,\dfrac{\text{MR}\,\dfrac{j(x,v) \vdash [x''=]j(x,v) \qquad \text{[}\cup\text{]}\,\dfrac{\wedge\text{R}\,\dfrac{\dfrac{}{j(x,v) \vdash [?x=0;\, v:=-cv]j(x,v)} \qquad \dfrac{}{j(x,v) \vdash [?x\neq0]j(x,v)}}{j(x,v) \vdash [?x=0;\, v:=-cv]j(x,v) \wedge [?x\neq0]j(x,v)}}{j(x,v) \vdash [?x=0;\, v:=-cv \cup ?x\neq0]j(x,v)}}{j(x,v) \vdash [x''=][?x=0;\, v:=-cv \cup ?x\neq0]j(x,v)}}{j(x,v) \vdash [x''=;\, (?x=0;\, v:=-cv \cup ?x\neq0]j(x,v)}$$

$$\text{loop}\,\dfrac{A \vdash j(x,v) \qquad \text{[;]}\,\dfrac{}{j(x,v) \vdash [x''=;\, (?x=0;\, v:=-cv \cup ?x\neq0]j(x,v)} \qquad j(x,v) \vdash B(x,v)}{A \vdash \left[\big(x''=;\, (?x=0;\, v:=-cv \cup ?x\neq0)\big)^*\right]B(x,v)}$$

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

$$
\text{MR}\;\text{[;]}\dfrac{\text{MR}\dfrac{j(x,v) \vdash [x''=]j(x,v) \quad \text{[}\cup\text{]}\dfrac{\wedge\text{R}\dfrac{\text{[;]}\dfrac{\text{[?]}\dfrac{\text{[:=]}\dfrac{j(x,v), x=0 \vdash j(x,-cv)}{j(x,v), x=0 \vdash [v:=-cv]j(x,v)}}{j(x,v) \vdash [?x=0][v:=-cv]j(x,v)}}{j(x,v) \vdash [?x=0; v:=-cv]j(x,v)} \qquad \dfrac{}{j(x,v) \vdash [?x\neq0]j(x,v)}}{j(x,v) \vdash [?x=0; v:=-cv]j(x,v) \wedge [?x\neq0]j(x,v)}}{j(x,v) \vdash [?x=0; v:=-cv \cup ?x\neq0]j(x,v)}}{j(x,v) \vdash [x''=][?x=0; v:=-cv \cup ?x\neq0]j(x,v)}}{j(x,v) \vdash [x''=; (?x=0; v:=-cv \cup ?x\neq0]j(x,v)}
$$

$$
\text{loop}\dfrac{A \vdash j(x,v) \quad \text{[;]}\dfrac{}{j(x,v) \vdash [x''=; (?x=0; v:=-cv \cup ?x\neq0]j(x,v)} \quad j(x,v) \vdash B(x,v)}{A \vdash [\big(x''=; (?x=0; v:=-cv \cup ?x\neq0)\big)^*]B(x,v)}
$$

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

$A \vdash j(x,v)$
$j(x,v) \vdash [x''=](j(x,v))$
$j(x,v), x=0 \vdash j(x,(-cv))$
$j(x,v), x\neq 0 \vdash j(x,v)$
$j(x,v) \vdash B(x,v)$

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

2. $j(x,v) \equiv 0 \le x \land x \le H$

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

1. $j(x,v) \equiv x \ge 0$ weaker: fails postcondition if $x > H$
2. $j(x,v) \equiv 0 \le x \land x \le H$ weak: fails ODE if $v \gg 0$

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

$j(x,v) \vdash [\{x'=v, v'=-g \,\&\, x\ge0\}](j(x,v))$

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

$j(x,v), x\ne0 \vdash j(x,v)$

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

$$2gx{=}2gH{-}v^2 \land x{\ge}0, x{=}0 \vdash 2gx{=}2gH{-}({-}cv)^2 \land x{\ge}0$$

$$2gx{=}2gH{-}v^2 \land x{\ge}0, x{\ne}0 \vdash 2gx{=}2gH{-}v^2 \land x{\ge}0$$

$$2gx{=}2gH{-}v^2 \land x{\ge}0 \vdash 0 \le x \land x \le H$$

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

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

Proving Quantum the Acrophobic Bouncing Ball

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

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

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

Quantum the Provably Safe Bouncing Ball

Proposition (Quantum can bounce around safely)

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

$\texttt{@requires}(0 \le x \land x = H \land v = 0)$

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

$\texttt{@ensures}(0 \le x \land x \le H)$

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

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

Invariant Contracts

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

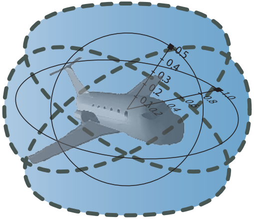
Note: constants $c = 1 \land g > 0$ that never change are often elided

10: Differential Equations & Differential Invariants

15-424: Foundations of Cyber-Physical Systems

André Platzer

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



Solutions more complicated than ODE

ODE	Solution
$x' = 1, x(0) = x_0$	$x(t) = x_0 + t$
$x' = 5, x(0) = x_0$	$x(t) = x_0 + 5t$
$x' = x, x(0) = x_0$	$x(t) = x_0 e^t$
$x' = x^2, x(0) = x_0$	$x(t) = \frac{x_0}{1-tx_0}$
$x' = \frac{1}{x}, x(0) = 1$	$x(t) = \sqrt{1+2t} \dots$
$y'(x) = -2xy, y(0) = 1$	$y(x) = e^{-x^2}$
$x'(t) = tx, x(0) = x_0$	$x(t) = x_0 e^{\frac{t^2}{2}}$
$x' = \sqrt{x}, x(0) = x_0$	$x(t) = \frac{t^2}{4} \pm t\sqrt{x_0} + x_0$
$x' = y, y' = -x, x(0) = 0, y(0) = 1$	$x(t) = \sin t, y(t) = \cos t$
$x' = 1 + x^2, x(0) = 0$	$x(t) = \tan t$
$x'(t) = \frac{2}{t^3} x(t)$	$x(t) = e^{-\frac{1}{t^2}}$ non-analytic
$x' = x^2 + x^4$	???
$x'(t) = e^{t^2}$	non-elementary

Global Descriptive Power of Local Differential Equations

Descriptive power of differential equations

1. Simple differential equations can describe quite complicated physical processes.
2. Solution is a global description of the system evolution.
3. ODE is a local characterization.
4. Complexity difference between local description and global behavior
5. Let's exploit that phenomenon for proofs!

Differential Equations vs. Loops

Lemma (Differential equations are their own loop)

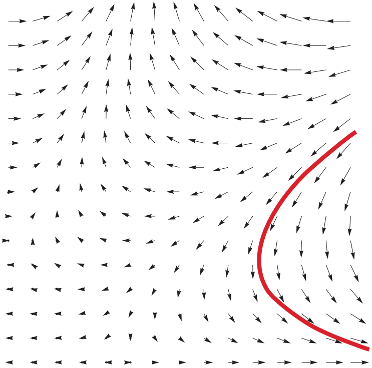
$$[\![(x' = f(x))^*]\!] = [\![x' = f(x)]\!]$$

loop α^*	ODE $x' = f(x)$
repeat any number $n \in \mathbb{N}$ of times	evolve for any duration $r \in \mathbb{R}$
can repeat 0 times	can evolve for duration 0
effect depends on previous loop iteratior	effect depends on the past solution
local generator α	local generator $x' = f(x)$
full global execution trace	global solution $\varphi : [0, r] \to \mathcal{S}$
unwinding proof by iteration $[*]$	proof by global solution with $[']$
inductive proof with loop invariant	proof with differential invariant

Intuition for Differential Invariants

Differential Invariant

$$\frac{\Gamma \vdash F, \Delta \quad F \vdash ???F \quad F \vdash P}{\Gamma \vdash [x' = f(x)]P, \Delta}$$

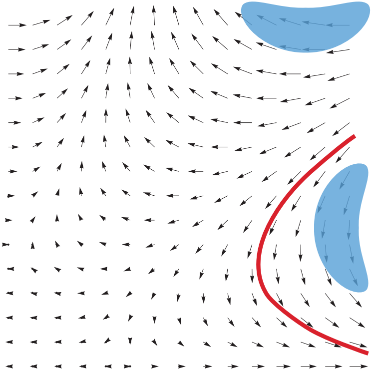


$$[{}'] \ [x' = f(x)]P \leftrightarrow \forall t{\geq}0\, [x := y(t)]P \qquad \text{(y' =f(y), y(0)=x)}$$

Intuition for Differential Invariants

Differential Invariant

$$\frac{\Gamma \vdash F, \Delta \quad F \vdash ???F \quad F \vdash P}{\Gamma \vdash [x' = f(x)]P, \Delta}$$



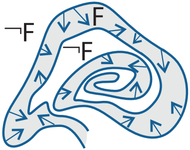
$$['] \; [x' = f(x)]P \leftrightarrow \forall t{\geq}0\, [x := y(t)]P \qquad (y' = f(y),\ y(0)=x)$$

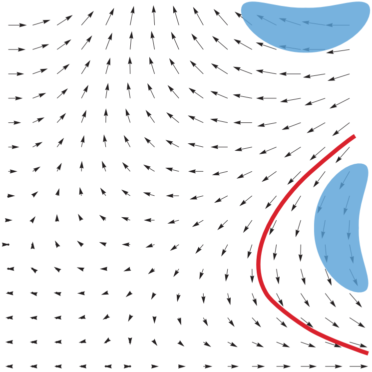
Intuition for Differential Invariants

Differential Invariant

$$\frac{\Gamma \vdash F, \Delta \quad F \vdash {\color{red}???}F \quad F \vdash P}{\Gamma \vdash [x' = f(x)]P, \Delta}$$

Want: F remains true in the direction of the dynamics





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

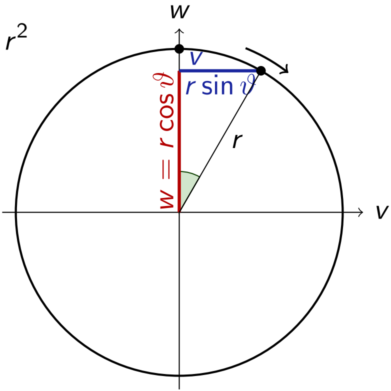
Don't need to know where exactly the system evolves to. Just that it remains somewhere in F.
Show: only evolves into directions in which formula F stays true.

Guiding Example

$$v^2+w^2 = r^2 \rightarrow [v' = w, w' = -v]v^2+w^2 = r^2$$

Guiding Example: Rotational Dynamics

$$v^2+w^2 = r^2 \rightarrow [v' = w, w' = -v]v^2+w^2 = r^2$$



Guiding Example: Rotational Dynamics

$$v^2+w^2=r^2 \rightarrow [v'=w, w'=-v]v^2+w^2=r^2$$

$$\rightarrow\text{R}\,\frac{}{\vdash v^2+w^2-r^2=0 \rightarrow [v'=w, w'=-v]v^2+w^2-r^2=0}$$

Derivatives for a Change

Syntax $e ::= x \mid c \mid e + k \mid e - k \mid e \cdot k \mid e/k$

Derivatives for a Change

Syntax $e ::= x \mid c \mid e + k \mid e - k \mid e \cdot k \mid e/k$

Derivatives

$$\begin{aligned}
(e + k)' &= (e)' + (k)' \\
(e - k)' &= (e)' - (k)' \\
(e \cdot k)' &= (e)' \cdot k + e \cdot (k)' \\
(e/k)' &= \big((e)' \cdot k - e \cdot (k)'\big)/k^2 \\
(c())' &= 0 \qquad \text{for constants/numbers } c()
\end{aligned}$$

Augmented states

For every variable x used in a differential equation, we add new variable x'.

Augmented states

For every variable x used in a differential equation, we add new variable x'.

Semantics of diff. eq.

$(s_1, s_2) \in \rho(x' = e \,\&\, Q)$

$\iff$

ex. $t > 0$ and $X : [0, t] \to \mathbb{R}$ with

1. $X(0) = s_1(x)$
2. $X'(u) = val_{s[x \mapsto X(u)]}(e)$ for all $0 \geq u \leq t$
3. $X(t) = s_2(x)$
4. $s_1[x \mapsto X(u)] \models Q$ for all $0 \geq u \leq t$
5. $s_1(y) = s_2(y)$ for all other variables y.

Augmented states

For every variable x used in a differential equation, we add new variable x'.

Semantics of diff. eq.

$(s_1, s_2) \in \rho(x' = e \mathbin{\&} Q)$

$\iff$

ex. $t > 0$ and $X : [0, t] \to \mathbb{R}$ with

1. $X(0) = s_1(x)$
2. $X'(u) = val_{s[x \mapsto X(u)]}(e)$ for all $0 \geq u \leq t$
3. $X(t) = s_2(x)$ and $X'(t) = s_2(x')$
4. $s_1[x \mapsto X(u)] \models Q$ for all $0 \geq u \leq t$
5. $s_1(y) = s_2(y)$ for all other variables y.

Derivatives for a Change

Syntax $e ::= x \mid c \mid e + k \mid e - k \mid e \cdot k \mid e/k \mid (e)'$

internalize primes into d$\mathcal{L}$ syntax

Derivatives

$$\begin{aligned}
(e + k)' &= (e)' + (k)' \\
(e - k)' &= (e)' - (k)' \\
(e \cdot k)' &= (e)' \cdot k + e \cdot (k)' \\
(e/k)' &= \big((e)' \cdot k - e \cdot (k)'\big)/k^2 && \text{same singularities} \\
(c())' &= 0 && \text{for constants/numbers } c()
\end{aligned}$$

. . . What do these primes mean? . . .

Differential Substitution Lemmas

Lemma (Differential lemma) (Differential value vs. Time-derivative)

If $\varphi \models x' = f(x) \land Q$ *for duration* $r > 0$*, then for all* $0 \leq z \leq r$*:*

Syntactic

$$[\![(e)']\!]\varphi(z) = \frac{\mathrm{d}[\![e]\!]\varphi(t)}{\mathrm{d}t}(z)$$

Analytic

Lemma (Differential assignment) (Effect on Differentials)

If $\varphi \models x' = f(x) \land Q$ *then* $\varphi \models P \leftrightarrow [x' := f(x)]P$

Lemma (Derivations) (Equations of Differentials)

$$\begin{aligned}
(e + k)' &= (e)' + (k)' \\
(e \cdot k)' &= (e)' \cdot k + e \cdot (k)' \\
(c())' &= 0 && \textit{for constants/numbers } c() \\
(x)' &= x' && \textit{for variables } x \in \mathcal{V}
\end{aligned}$$

Differential Substitution Lemmas

Lemma (Differential lemma) (Differential value vs. Time-derivative)

If $\varphi \models x' = f(x) \land Q$ *for duration* $r > 0$, *then for all* $0 \leq z \leq r$*:*

$$[\![(e)']\!]\varphi(z) = \frac{\mathrm{d}[\![e]\!]\varphi(t)}{\mathrm{d}t}(z)$$

Lemma (Differential assignment) (Effect on Differentials)

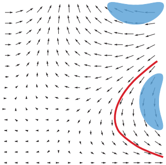
If $\varphi \models x' = f(x) \land Q$ *then* $\varphi \models P \leftrightarrow [x' := f(x)]P$

Axiomatics

$$\text{DE}\ [x' = f(x)\,\&\,Q]P \leftrightarrow [x' = f(x)\,\&\,Q][x' := f(x)]P$$

$$\text{DI}\ \frac{\vdash [x' = f(x)\,\&\,Q](e)' = 0}{e = 0 \vdash [x' = f(x)\,\&\,Q]e = 0}$$

Differential Invariants for Differential Equations

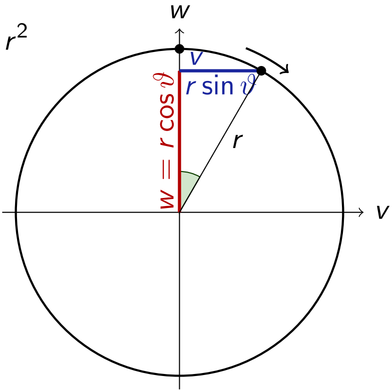


Differential Invariant

$$\mathrm{DI}_{=0}\ \frac{\vdash [x' := f(x)](e)' = 0}{e = 0 \vdash [x' = f(x)]e = 0}$$

Guiding Example: Rotational Dynamics

$$v^2 + w^2 = r^2 \rightarrow [v' = w, w' = -v] v^2 + w^2 = r^2$$



Guiding Example: Rotational Dynamics

$$v^2+w^2 = r^2 \rightarrow [v' = w, w' = -v]v^2+w^2 = r^2$$

$$\rightarrow\text{R}\ \frac{}{\vdash v^2+w^2-r^2=0 \rightarrow [v' = w, w' = -v]v^2+w^2-r^2=0}$$

Guiding Example: Rotational Dynamics

$$v^2+w^2 = r^2 \to [v' = w, w' = -v]v^2+w^2 = r^2$$

$$\dfrac{\mathrm{DI}_{=0}\;\dfrac{}{v^2+w^2-r^2=0 \vdash [v' = w, w' = -v]v^2 + w^2 - r^2 = 0}}{\vdash v^2+w^2-r^2=0 \to [v' = w, w' = -v]v^2+w^2-r^2=0}\;{\to}\mathrm{R}$$

Guiding Example: Rotational Dynamics

$$v^2+w^2 = r^2 \to [v' = w, w' = -v]v^2+w^2 = r^2$$

$$
\begin{array}{ll}
[{}'{:=}] & \overline{ \vdash [v'{:=}w][w'{:=}-v]2vv' + 2ww' - r' = 0} \\
\text{DI}_{=0} & \overline{v^2+w^2-r^2=0 \vdash [v' = w, w' = -v]v^2 + w^2 - r^2 = 0} \\
\to\text{R} & \overline{ \vdash v^2+w^2-r^2=0 \to [v' = w, w' = -v]v^2+w^2-r^2=0}
\end{array}
$$

Guiding Example: Rotational Dynamics

$$v^2+w^2 = r^2 \to [v' = w, w' = -v]v^2+w^2 = r^2$$

$$\begin{array}{l|r}
\mathbb{R} & \hline \vdash 2v(w) + 2w(-v) = 0 \\
[{}':=] & \hline \vdash [v':=w][w':=-v]2vv' + 2ww' - r' = 0 \\
\mathrm{DI}_{=0} & \hline v^2+w^2-r^2=0 \vdash [v' = w, w' = -v]v^2 + w^2 - r^2 = 0 \\
\to\mathrm{R} & \hline \vdash v^2+w^2-r^2=0 \to [v' = w, w' = -v]v^2+w^2-r^2=0
\end{array}$$

Guiding Example: Rotational Dynamics

$$v^2+w^2 = r^2 \to [v' = w, w' = -v]v^2+w^2 = r^2$$

$$
\begin{array}{lrl}
 & & \quad * \\
\cline{2-3}
\mathbb{R} & & \vdash 2v(w) + 2w(-v) = 0 \\
\cline{2-3}
[' {:=}] & & \vdash [v' {:=} w][w' {:=} -v]2vv' + 2ww' - r' = 0 \\
\cline{2-3}
\mathrm{DI}_{=0} & v^2+w^2-r^2=0 & \vdash [v' = w, w' = -v]v^2 + w^2 - r^2 = 0 \\
\cline{2-3}
\to\mathrm{R} & & \vdash v^2+w^2-r^2=0 \to [v' = w, w' = -v]v^2+w^2-r^2=0
\end{array}
$$

Guiding Example: Rotational Dynamics

$$v^2+w^2 = r^2 \rightarrow [v' = w, w' = -v]v^2+w^2 = r^2$$

$$
{\scriptstyle \rightarrow\mathrm{R}}\;\dfrac{{\scriptstyle \mathrm{DI}_{=0}}\;\dfrac{{\scriptstyle [':=]}\;\dfrac{{\scriptstyle \mathbb{R}}\;\dfrac{*}{\vdash 2v(w) + 2w(-v) = 0}}{\vdash [v':=w][w':=-v]2vv' + 2ww' - r' = 0}}{v^2+w^2-r^2=0 \vdash [v' = w, w' = -v]v^2 + w^2 - r^2 = 0}}{\vdash v^2+w^2-r^2=0 \rightarrow [v' = w, w' = -v]v^2+w^2-r^2=0}
$$

Simple proof without solving ODE

Strengthening Induction Hypotheses

Stronger Induction Hypotheses

1. As usual in math and in proofs with loops:
2. Inductive proofs may need stronger induction hypotheses to succeed.
3. Differentially inductive proofs may need a stronger differential inductive structure to succeed.
4. Even if $\{(x,y) \in \mathbb{R}^2 \ : \ x^2 + y^2 = 0\} = \{\{(x,y) \in \mathbb{R}^2 \ : \ x^4 + y^4 = 0\}$ have the same solutions, they have different differential structure.