Karlsruhe Institute of Technology

# Formale Systeme II: Theorie

SS 2018

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

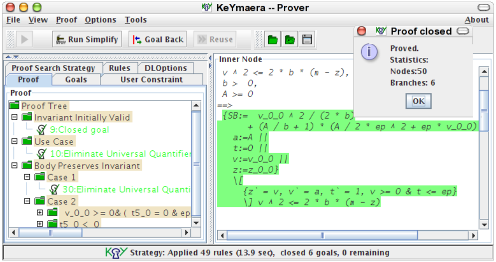
## Overview – a family of logics

$$\begin{tikzcd}
 & \text{Modal Logics} \arrow[d] & \\
 & \text{Propositional Dynamic Logic} \arrow[d] & \\
 & \text{Dynamic Logic} \arrow[dl] \arrow[dr] & \\
\text{Hybrid DL} & & \text{Java DL}
\end{tikzcd}$$

# Goals

- differential equations
- hybrid automata
- hybrid dynamic logic
- differential invariants

# A. Platzer, KeYmaera




http://www.symbolaris.com

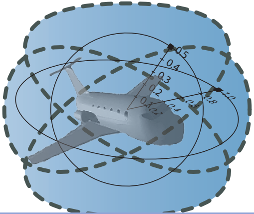
# 15-424/15-624: Foundations of Cyber-Physical Systems

## 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?

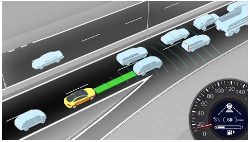
# CPSs Promise Transformative Impact!

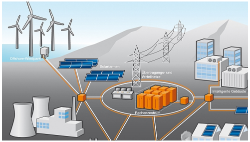
## Prospects: Safe & Efficient

Driver assistance
Autonomous cars

Pilot decision support
Autopilots / UAVs

Train protection
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

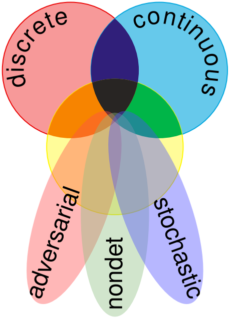
## Cyber-physical Systems

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:

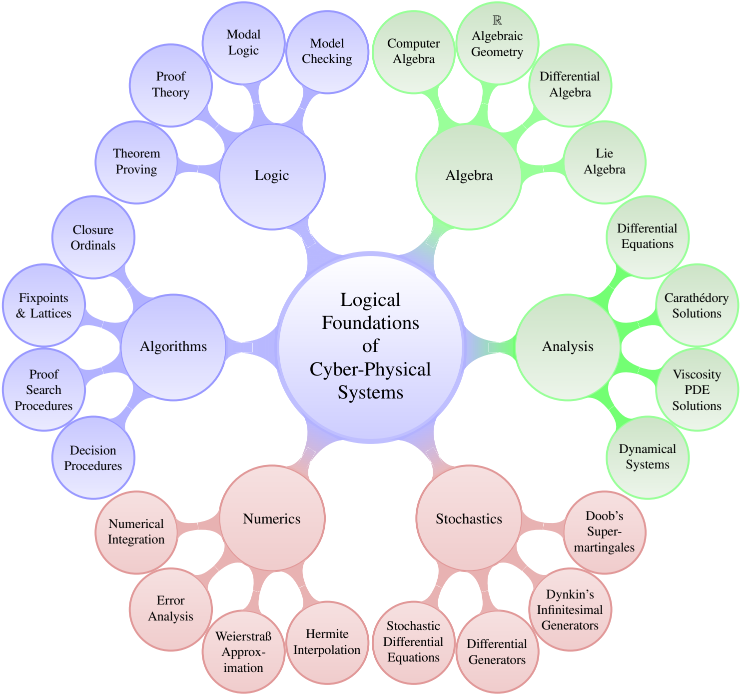
**Definition (Hybrid Systems)**

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

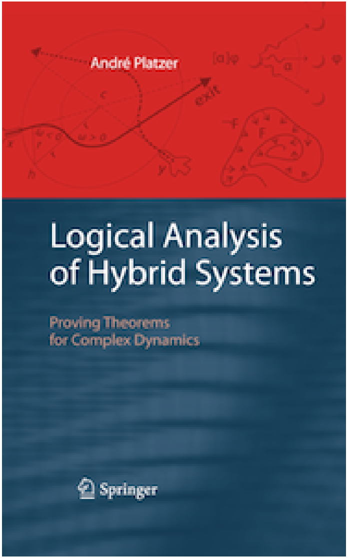


Logical Foundations of Cyber-Physical Systems
Logic
Modal Logic
Model Checking
Proof Theory
Theorem Proving
Algebra
Computer Algebra
ℝ Algebraic Geometry
Differential Algebra
Lie Algebra
Algorithms
Closure Ordinals
Fixpoints & Lattices
Proof Search Procedures
Decision Procedures
Analysis
Differential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

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`

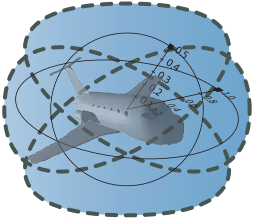
- André Platzer.
  *Logical Analysis of Hybrid Systems*.
  Springer, 426p., 2010.
  DOI 10.1007/978-3-642-14509-4
  `http://symbolaris.com/lahs/`
  CMU library e-book

# 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

# Differential Equations as Models of Continuous Processes

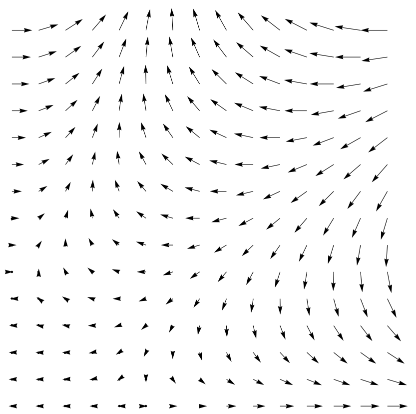
**Example (Vector field and one solution of a differential equation)**

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

Intuition:

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

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

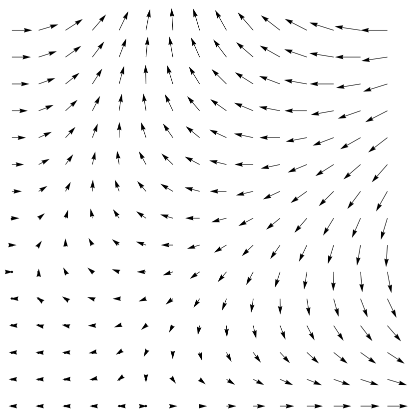


Intuition:

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

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

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



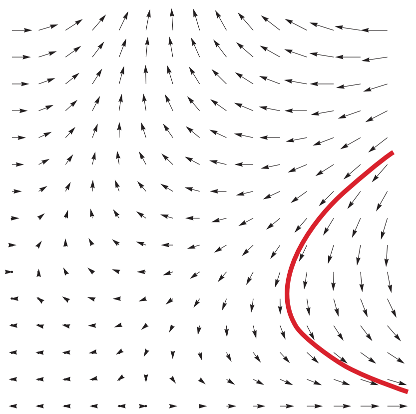
Intuition:

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)

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



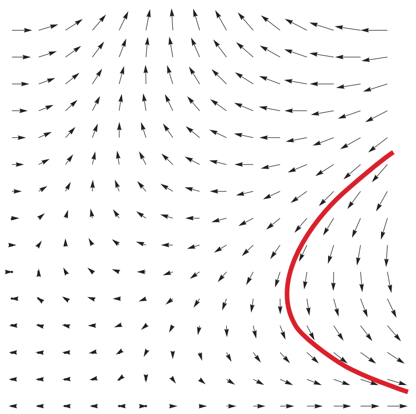
Intuition:

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

# Differential Equations as Models of Continuous Processes

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

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



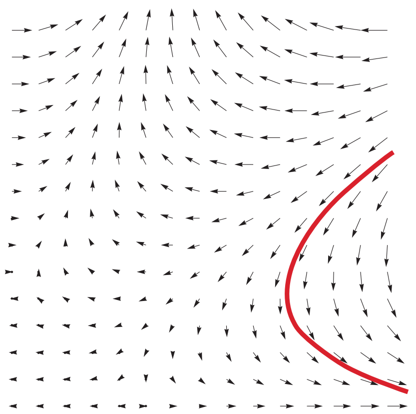
Intuition:

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 . . .

## 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:

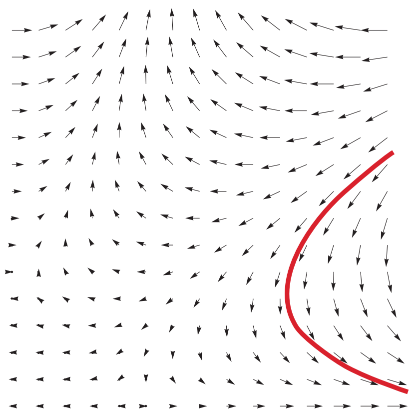
1. At each point in space, plot the value of $f(t,y)$ as a vector
2. Start at initial state $y_0$ at initial time $t_0$
3. Follow the direction of the vector

↯ The diagram should show infinitely many vectors ...

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

## 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 $x' = v, v' = a$

Well it's a wee bit more complicated

# Outline

# 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)

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

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)

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

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)

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

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

# 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

# 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 $x(t) = 5t + 2$

# Example: A Constant Differential Equation

## Example (Initial value problem)

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

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

## Check by inserting solution into ODE+IVP.

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

□

# 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)**

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

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

# 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 $x(t) = e^{\frac{t}{4}}$

**Check by inserting solution into ODE+IVP.**

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

$\square$

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

# ODE Examples

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

# ODE Examples

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

# 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 |

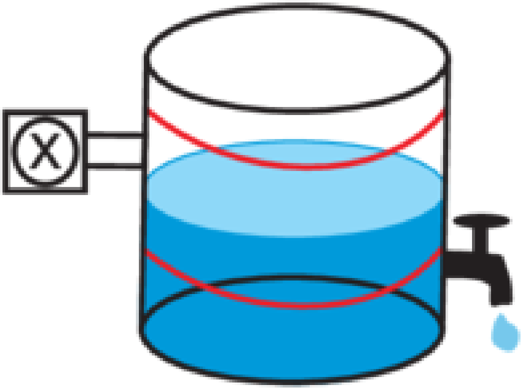
| ODE | Solution |
|---|---|
| $x' = 1, x(0) = x_0$ | $x(t) = x_0 + t$ |
| $x' = 5, x(0) = x_0$ | $x(t) = x_0 + 5t$ |
| $x' = x, x(0) = x_0$ | $x(t) = x_0 e^t$ |
| $x' = x^2, x(0) = x_0$ | $x(t) = \frac{x_0}{1-tx_0}$ |
| $x' = \frac{1}{x}, x(0) = 1$ | $x(t) = \sqrt{1+2t} \dots$ |
| $y'(x) = -2xy, y(0)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

# Takeaway Message

**Descriptive power of differential equations**

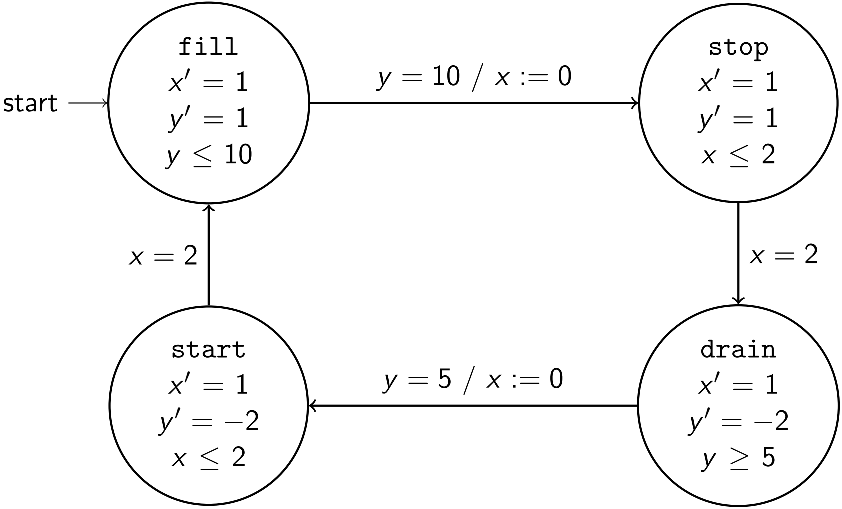
1. Solutions of differential equations can be much more involved than the differential equations themselves.
2. Representational and descriptive power of differential equations!
3. Simple differential equations can describe quite complicated physical processes.
4. Local description as the direction into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

# Hybrid automata – Motivation



© symbolaris.com

# Hybrid automata – Example



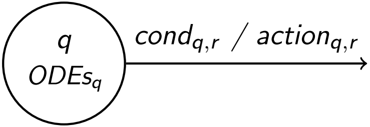
# Hybrid Automata

Extension of Finite State Machines (*Henzinger*, 1990s)

# Hybrid Automata

## Extension of Finite State Machines (*Henzinger*, 1990s)

State $q \in S$ with edge to $r \in S$:

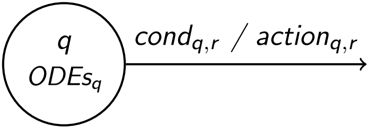



ODEs may have domain constraints

# Hybrid Automata

## Extension of Finite State Machines (*Henzinger*, 1990s)

State $q \in S$ with edge to $r \in S$:




ODEs may have domain constraints

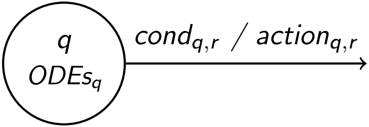
### Semantics (Idea)

1. Sequence of *edge steps* and *time steps (flow)*

# Hybrid Automata

## Extension of Finite State Machines (*Henzinger*, 1990s)

State $q \in S$ with edge to $r \in S$:




ODEs may have domain constraints

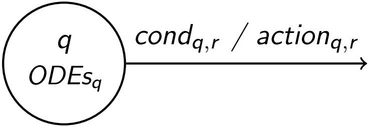
### Semantics (Idea)

1. Sequence of *edge steps* and *time steps (flow)*
2. during flow: variables evolve according to $ODEs_q$

# Hybrid Automata

## Extension of Finite State Machines (*Henzinger*, 1990s)

State $q \in S$ with edge to $r \in S$:




ODEs may have domain constraints

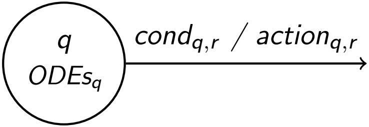
### Semantics (Idea)

1. Sequence of *edge steps* and *time steps (flow)*
2. during flow: variables evolve according to $ODEs_q$
3. discrete state changes at $t_i$ from $q_i$ to $q_{i+1}$:
   $cond_{q_i}$ must hold, $action_{q_i,q_{i+1}}$ is performed

# Hybrid Automata

## Extension of Finite State Machines (*Henzinger*, 1990s)

State $q \in S$ with edge to $r \in S$:




ODEs may have domain constraints

### Semantics (Idea)

1. Sequence of *edge steps* and *time steps (flow)*
2. during flow: variables evolve according to $ODEs_q$
3. discrete state changes at $t_i$ from $q_i$ to $q_{i+1}$:
   $cond_{q_i}$ must hold, $action_{q_i,q_{i+1}}$ is performed
4. edge: condition $cond_{q,r}$ satisfied, $action_{q,r}$ performed discretely, new state is $r$

# Rectangular Hybrid Automata

## Rectangular condition

A rectangular condition on *Var* is a conjunction of atoms of the form $x \leq const$ or $x \geq const$ for variables $x \in Var$.

## Rectangular automata

A hybr. automaton is called *rectangular* if

# Rectangular Hybrid Automata

## Rectangular condition

A rectangular condition on *Var* is a conjunction of atoms of the form $x \leq \mathit{const}$ or $x \geq \mathit{const}$ for variables $x \in \mathit{Var}$.

## Rectangular automata

A hybr. automaton is called *rectangular* if

- every *cond* is a rectangular condition

# Rectangular Hybrid Automata

## Rectangular condition

A rectangular condition on *Var* is a conjunction of atoms of the form $x \leq \mathit{const}$ or $x \geq \mathit{const}$ for variables $x \in \mathit{Var}$.

## Rectangular automata

A hybr. automaton is called *rectangular* if

- every *cond* is a rectangular condition
- every *action* is a sequence of assignments $x := \mathit{const}$

# Rectangular Hybrid Automata

### Rectangular condition

A rectangular condition on *Var* is a conjunction of atoms of the form $x \leq \mathit{const}$ or $x \geq \mathit{const}$ for variables $x \in \mathit{Var}$.

### Rectangular automata

A hybr. automaton is called *rectangular* if

- every *cond* is a rectangular condition
- every *action* is a sequence of assignments $x := \mathit{const}$
- every *ODE* is a rectangular condition on the derivatives $x', \ldots$

# Rectangular Hybrid Automata

## Rectangular condition

A rectangular condition on *Var* is a conjunction of atoms of the form $x \leq const$ or $x \geq const$ for variables $x \in Var$.

## Rectangular automata

A hybr. automaton is called *rectangular* if

- every *cond* is a rectangular condition
- every *action* is a sequence of assignments $x := const$
- every *ODE* is a rectangular condition on the derivatives $x', \ldots$
- every domain constraint is a rectangular condition

# Rectangular Hybrid Automata

**Decidability**

The safety problem for rectangular automata w.r.t. to rectangular safety invariants is decidable (in PSPACE).

["What's Decidable about Hybrid Automata?", Henzinger et al. 1998]

Proof by reduction to *timed automata* $\rightarrow$ lecture FS2: Application

# Rectangular Hybrid Automata

## Decidability

The safety problem for rectangular automata w.r.t. to rectangular safety invariants is decidable (in PSPACE).

["What's Decidable about Hybrid Automata?", Henzinger et al. 1998]

Proof by reduction to *timed automata* $\rightarrow$ lecture FS2: Application

## Undecidablity result

The safety problem is undecidable for hybrid automata with general linear ODEs.

# Differential Dynamic Logic

# Differential Dynamic Logic d$\mathcal{L}$

is an extension of first order dynamic logic

**Programs:** If $\alpha, \beta$ are $d\mathcal{L}$ (regular) programs, then

- $\alpha \,;\, \beta$
- $\alpha \cup \beta$
- $\alpha^*$
- $x := t$ ($x$ a variable, $t$ a term)
- $?\varphi$ ($\varphi$ a formula)

are d$\mathcal{L}$ programs, too.

# Differential Dynamic Logic d$\mathcal{L}$

is an extension of first order dynamic logic

**Programs:** If $\alpha, \beta$ are $d\mathcal{L}$ (regular) programs, then

- $\alpha\,;\,\beta$
- $\alpha \cup \beta$
- $\alpha^*$
- $x := t$ ($x$ a variable, $t$ a term)
- $?\varphi$ ($\varphi$ a formula)
- $x_1' = t_1, \ldots, x_n' = t_n \;\&\; \varphi$ ($x_i$ a variable, $t_i$ a term, $\varphi$ a formula, $i \in [1..n]$)

are d$\mathcal{L}$ programs, too.

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

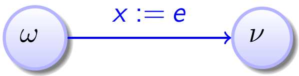
## Definition (Hybrid program semantics) $(\llbracket\cdot\rrbracket : \mathrm{HP} \to \wp(\mathcal{S} \times \mathcal{S}))$

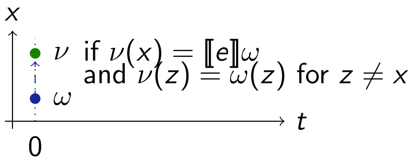
$$
\begin{aligned}
\llbracket x := e \rrbracket &= \{(\omega,\nu) : \nu = \omega \text{ except } \llbracket x \rrbracket\nu = \llbracket e \rrbracket\omega\} \\
\llbracket ?Q \rrbracket &= \{(\omega,\omega) : \omega \in \llbracket Q \rrbracket\} \\
\llbracket x' = f(x) \rrbracket &= \{(\varphi(0),\varphi(r))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

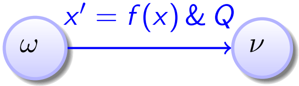
## Definition (d$\mathcal{L}$ semantics) $(\llbracket\cdot\rrbracket : \mathrm{Fml} \to \wp(\mathcal{S}))$

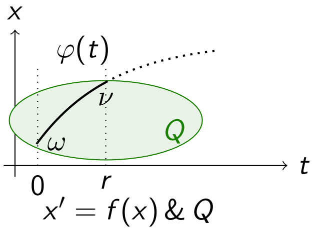
$$
\begin{aligned}
\llbracket \theta \geq \eta \rrbracket &= \{\omega : \llbracket \theta \rrbracket\omega \geq \llbracket \eta \rrbracket\omega\} \\
\llbracket \neg\phi \rrbracket &= (\llbracket \phi \rrbracket)^{\complement} \\
\llbracket \phi \wedge \psi \rrbracket &= \llbracket \phi \rrbracket \cap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

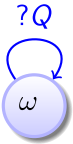
# Differential Dynamic Logic $d\mathcal{L}$: Transition Semantics



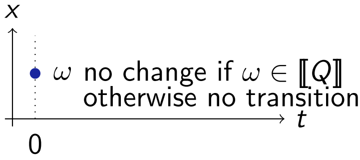



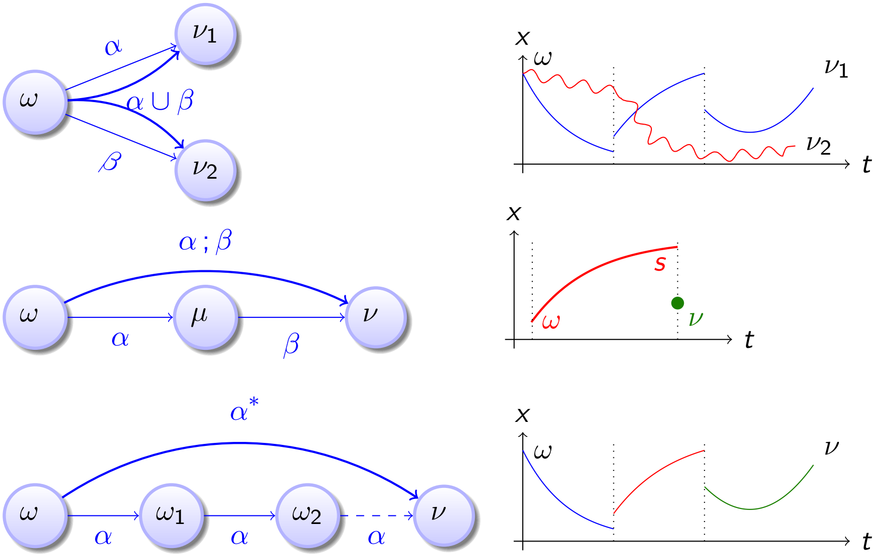



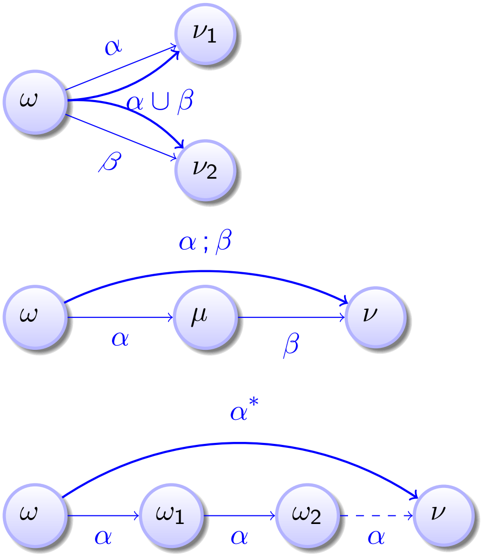




if $\omega \in [\![Q]\!]$

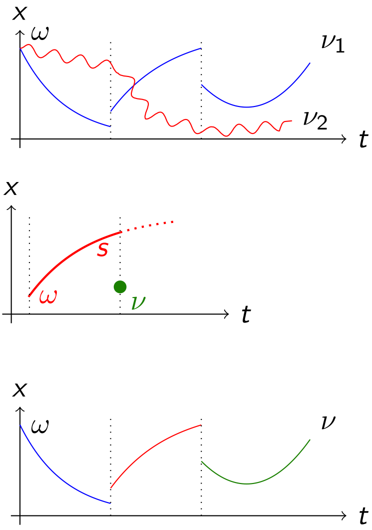


# Differential Dynamic Logic d$\mathcal{L}$: Transition Semantics



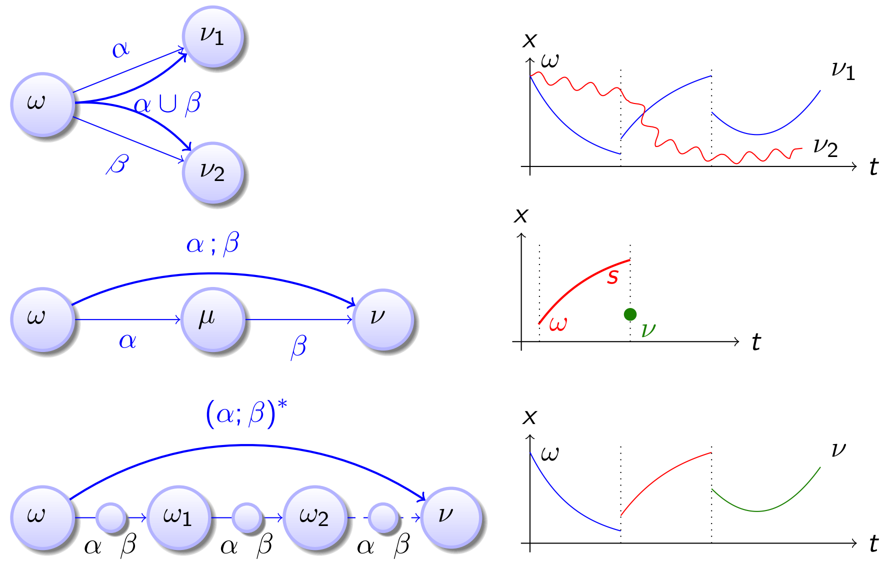


α
ν1
ω
α ∪ β
β
ν2
α ; β
ω
μ
ν
α
β
α*
ω
ω1
ω2
ν
α
α
α

x
ω
ν1
ν2
t
x
s
ω
ν
t
x
ω
ν
t

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

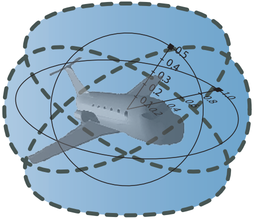


# 04: Safety & Contracts

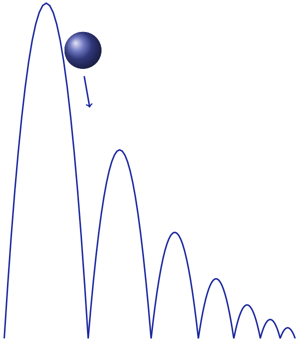
## 15-424: Foundations of Cyber-Physical Systems

André Platzer

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

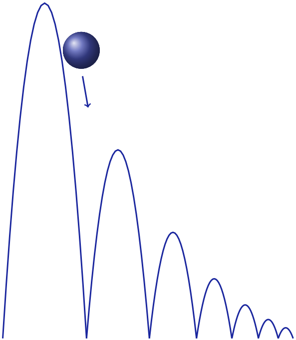


# Quantum the Acrophobic Bouncing Ball



**Example (Quantum the Bouncing Ball)**

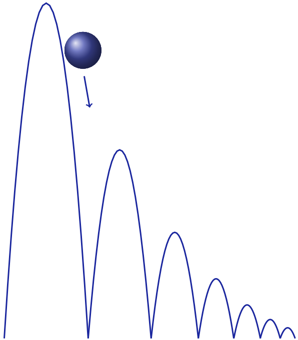
# Quantum the Acrophobic Bouncing Ball



**Example (Quantum the Bouncing Ball)**

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

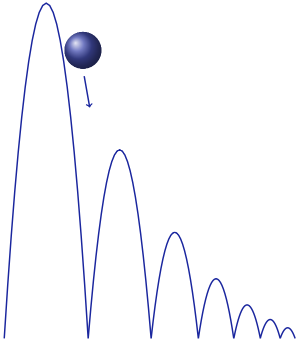
# Quantum the Acrophobic Bouncing Ball



**Example (Quantum the Bouncing Ball)**

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

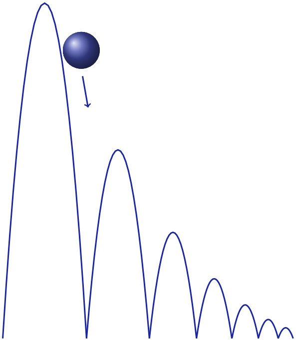
# Quantum the Acrophobic Bouncing Ball



Example (Quantum the Bouncing Ball)

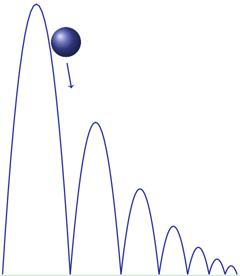
$$\big(x' = v, v' = -g \,\&\, x \geq 0;$$
$$\texttt{if}(x = 0)\, v := -cv\big)^*$$

# Quantum the Acrophobic Bouncing Ball



Example (Quantum the Bouncing Ball)

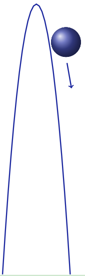
$$\big(x' = v, v' = -g \,\&\, x \geq 0;$$
$$\texttt{if}(x = 0)\, v := -cv\big)^*$$



**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

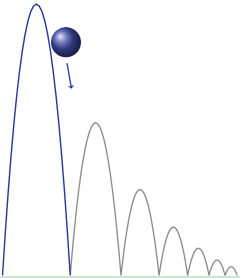


**Example (Quantum the Bouncing Ball)** (Single-hop)

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

Removing the repetition grotesquely changes the behavior to a single hop

# Conjecture: Quantum the Acrophobic Bouncing Ball



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

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

Removing the repetition grotesquely changes the behavior to a single hop

# A Proof of a Short Single-hop Bouncing Ball

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

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

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

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

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

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

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

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

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

# A Proof of a Short Single-hop Bouncing Ball

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

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

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

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

# A Proof of a Short Single-hop Bouncing Ball

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

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

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

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

# A Proof of a Short Single-hop Bouncing Ball

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

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

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

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

# A Proof of a Short Single-hop Bouncing Ball

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

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

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

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

# A Proof of a Short Single-hop Bouncing Ball

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

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

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

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

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

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

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

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

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

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

# A Proof of a Short Single-hop Bouncing Ball

$$[:=]\quad A \vdash \forall t{\geq}0\, [x := H - \tfrac{g}{2}t^2][v := -gt]\big((x{=}0 \to B(x,-cv)) \land (x{\geq}0 \to B(x,v)\big)$$

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

$$[']\quad A \vdash [x'' = -g]\big((x = 0 \to B(x,-cv)) \land (x \geq 0 \to B(x,v))\big)$$

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

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

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

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

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

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

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

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

# A Proof of a Short Single-hop Bouncing Ball

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

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

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

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

# A Proof of a Short Single-hop Bouncing Ball

$$A \vdash \forall t{\geq}0\, \big(\big(H-\tfrac{g}{2}t^2{=}0 \to B(H-\tfrac{g}{2}t^2, -c(-gt))\big) \land \big(H-\tfrac{g}{2}t^2{\geq}0 \to B(H-\tfrac{g}{2}t^2, -gt)$$

[:=] $$A \vdash \forall t{\geq}0\, [x := H - \tfrac{g}{2}t^2]\big(\big(x{=}0 \to B(x, -c(-gt))\big) \land \big(x{\geq}0 \to B(x, -gt)\big)\big)$$

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

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

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

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

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

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

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

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

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

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

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

# A Proof of a Short Single-hop Bouncing Ball

$$A \vdash \forall t{\geq}0\, \big((H{-}\tfrac{g}{2}t^2{=}0{\to}B(H{-}\tfrac{g}{2}t^2,-c(-gt))\big) \land \big(H{-}\tfrac{g}{2}t^2{\geq}0{\to}B(H{-}\tfrac{g}{2}t^2,-gt)\big)$$

$$[:=]\quad A \vdash \forall t{\geq}0\, [x := H - \tfrac{g}{2}t^2]\big((x{=}0 \to B(x,-c(-gt))) \land (x{\geq}0 \to B(x,-gt))\big)$$

$$[:=]\quad A \vdash \forall t{\geq}0\, [x := H - \tfrac{g}{2}t^2][v := -gt]\big((x{=}0 \to B(x,-cv)) \land (x{\geq}0 \to B(x,v))\big)$$

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

$$[']\quad A \vdash [x'' = -g]\big((x = 0 \to B(x,-cv)) \land (x \geq 0 \to B(x,v))\big)$$

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

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

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

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

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

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

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

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

# A Proof of a Short Single-hop Bouncing Ball

Resolving abbreviations at the premise yields:

$$
\begin{aligned}
&0 \le x \land x = H \land v = 0 \land g > 0 \land 1 \ge c \ge 0 \rightarrow \\
&\qquad \forall t{\ge}0 \, \Big( \big(H - \frac{g}{2}t^2 = 0 \rightarrow 0 \le H - \frac{g}{2}t^2 \land H - \frac{g}{2}t^2 \le H\big) \\
&\qquad\qquad \land \big(H - \frac{g}{2}t^2 \ge 0 \rightarrow 0 \le H - \frac{g}{2}t^2 \land H - \frac{g}{2}t^2 \le H\big)\Big)
\end{aligned}
$$

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

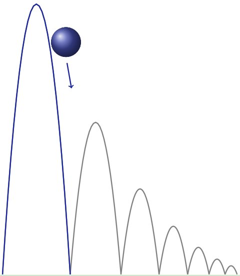
# A Proof of a Short Single-hop Bouncing Ball

Resolving abbreviations at the premise yields:

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

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

# Conjecture: Quantum the Acrophobic Bouncing Ball



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

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

Removing the repetition grotesquely changes the behavior to a single hop

# Hybrid Programs and Loop Invariants

**Repeatedly bouncing ball**

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

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

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

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

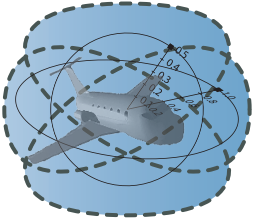
$$[']\ \frac{\Gamma \vdash \forall t \geq 0.((\forall t'.0 \leq t' \leq t \rightarrow Q(t')) \rightarrow [x := X(t)]\phi), \Delta}{\Gamma \vdash [x' = t\ \&\ Q(x)]\phi, \Delta}$$

# 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



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

# Differential Equations vs. Loops

**Lemma (Differential equations are their own loop)**

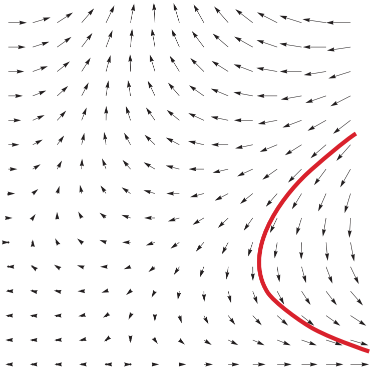
$$[\![(x' = f(x))^*]\!] = [\![x' = f(x)]\!]$$

| loop $\alpha^*$ | 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 $\alpha$ | 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**

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

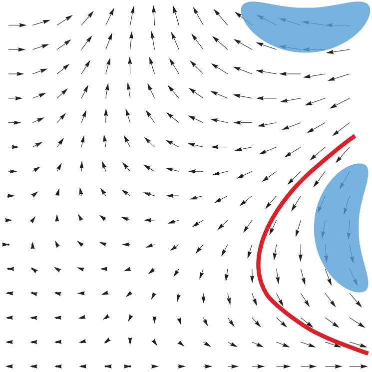


$['] \; [x' = f(x)]P \leftrightarrow \forall t \geq 0 \, [x := y(t)]P$ (y' =f(y), y(0)=x)

# Intuition for Differential Invariants

**Differential Invariant**

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

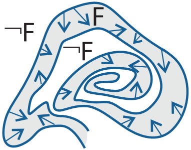


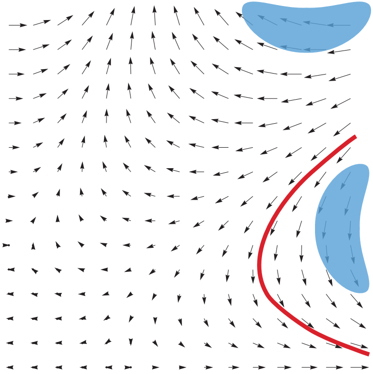
$$['] \; [x' = f(x)]P \leftrightarrow \forall t{\geq}0\, [x := y(t)]P \qquad \text{(y' =f(y), y(0)=x)}$$

**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



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

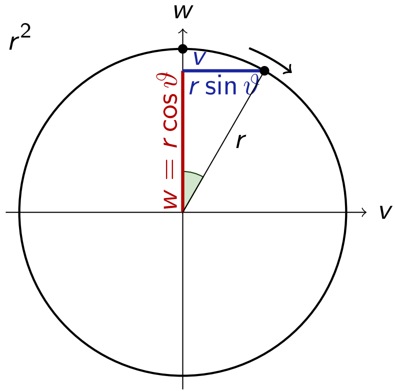
Don't need to know where exactly the system evolves to. Just that it remains somewhere in $F$.
Show: only evolves into directions in which formula $F$ stays true.

# 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

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

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

# 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**

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

# Augmented states

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

Let $x'$ also evolve by differential equations.

# Augmented states

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

Let $x'$ also evolve by differential equations.

## 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 $0 \leq u \leq t$
3. $X(t) = s_2(x)$
4. $s_1[x \mapsto X(u)] \models Q$ for all $0 \leq u \leq t$
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 $x'$.

Let $x'$ also evolve by differential equations.

## 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 $0 \leq u \leq t$
3. $X(t) = s_2(x)$ and $X'(t) = s_2(x')$
4. $s_1[x \mapsto X(u)] \models Q$ for all $0 \leq u \leq t$
5. $s_1(y) = s_2(y)$ for all other variables $y$.

# Notation

Let now $\varphi : [0, r] \to \mathbb{R}^n$ for some duration $r \in \mathbb{R}$ be a solution of $x' = e \mathbin{\&} Q$:

$$(\varphi(0), \varphi(r)) \in \rho(x' = e \mathbin{\&} Q)$$

# 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

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

...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* $0 \leq z \leq r$*:*

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

**Lemma (Differential assignment)** (Effect on Differentials)

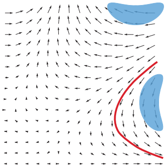
*If* $\varphi \models x' = f(x) \land Q$ *then* $\varphi \models P \leftrightarrow [x' := f(x)]P$

**Axiomatics**

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

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

# Differential Invariants for Differential Equations

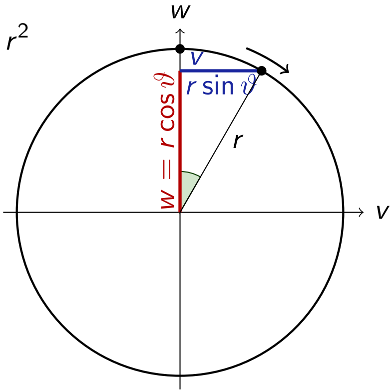


**Differential Invariant**

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

# 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

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

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

# 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

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

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

# Guiding Example: Rotational Dynamics

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

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

# Guiding Example: Rotational Dynamics

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

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

# Guiding Example: Rotational Dynamics

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

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

Simple proof without solving ODE

## 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.