André Platzer

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

http://symbolaris.com/course/fcps13.html
Outline

1. CPS: Introduction
   - Hybrid Systems & Cyber-Physical Systems
   - Applications
   - Robot Labs

2. 15-424: Foundations of Cyber-Physical Systems
   - Objectives
   - Outline
   - Assessment
   - Labs
   - Resources

3. Approach
   - CPS Contracts
   - CPS Logic
   - Differential Dynamic Logic Family

4. Summary
How can we provide people with cyber-physical systems they can bet their lives on?
[Jeannette Wing]
Can you trust a computer to control physics?

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

CPS Foundations: intellectual grand challenge

Research & Industry
**Outline**

1. **CPS: Introduction**
   - Hybrid Systems & Cyber-Physical Systems
   - Applications
   - Robot Labs

   - Objectives
   - Outline
   - Assessment
   - Labs
   - Resources

3. **Approach**
   - CPS Contracts
   - CPS Logic
   - Differential Dynamic Logic Family

4. **Summary**
Train Control

Challenge

Hybrid systems

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)
Challenge

Hybrid systems
- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)
Challenge

Hybrid systems

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)
Challenge

Hybrid systems

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)
Train Control

Challenge

Hybrid systems

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)

More than computers:

no NullPointerException ⇒ safe

More than physics: braking control

$v^2 \leq v^2 + a^2 + \varepsilon^2 + \varepsilon v + \varepsilon^2 + \varepsilon^2$

Joint dynamics requires:

$S_B \geq v^2 + a^2 + \varepsilon^2 + \varepsilon v + \varepsilon^2 + \varepsilon^2$
Train Control

Challenge

Hybrid systems

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)

1. More than computers: no NullPointerException \(\not\Rightarrow\) safe
2. More than physics: braking control \(\sqrt{v^2} \leq 2b(MA - z) \not\Rightarrow\) safe
Train Control

Challenge

Hybrid systems

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)

1. More than computers: no NullPointerException \( \not\Rightarrow \) safe
2. More than physics: braking control \( v^2 \leq 2b(MA - z) \not\Rightarrow \) safe
3. Joint dynamics requires:

\[
SB \geq \frac{v^2}{2b} + \frac{a^2 \varepsilon^2}{2b} + \frac{a}{b} \varepsilon v + \frac{a}{2} \varepsilon^2 + \varepsilon v \ldots
\]

André Platzer (CMU)
Challenge

Hybrid systems

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)
Train Control

Challenge

Hybrid systems

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)
Challenge

Hybrid systems

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)
Challenge

Hybrid systems

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)
Train Control

Challenge

Hybrid systems
- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)
Train Control

Challenge

Hybrid systems

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)

\[ SB \geq \frac{v^2}{2b} + \frac{a^2\varepsilon^2}{2b} + \frac{a}{b} \varepsilon v + \frac{a}{2} \varepsilon^2 + \varepsilon v \]
Challenge

Hybrid systems

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)

∀MA ∃SB “train always safe”
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
What CPS are around us?

What CPS will be around us in the future?

Which CPS do we trust with our lives?
Successful Hybrid Systems Proofs

André Platzer (CMU)

FCPS/01: Overview
Challenge (Hybrid Systems)

Design & verify controller for a robot avoiding obstacles

- Accelerate / brake (discrete dynamics)
- 1D motion (continuous dynamics)
Design & verify controller for a robot avoiding obstacles

- Accelerate / brake (discrete dynamics)
- 1D motion (continuous dynamics)
Challenge (Hybrid Systems)

Design & verify controller for a robot avoiding obstacles

- Accelerate / brake / stop (discrete dynamics)
- 1D motion (continuous dynamics)
Challenge (Hybrid Systems)

Design & verify controller for a robot avoiding obstacles
- Accelerate / brake / stop (discrete dynamics)
- 1D motion (continuous dynamics)
Challenge (Hybrid Systems)

Design & verify controller for a robot avoiding obstacles

- Accelerate / brake (discrete dynamics)
- 1D motion (continuous dynamics)
Challenge (Hybrid Systems)

Design & verify controller for a robot avoiding obstacles

- Accelerate / brake (discrete dynamics)
- 1D motion (continuous dynamics)
Challenge (Hybrid Systems)

Design & verify controller for a robot avoiding obstacles
- Accel / brake / steer (discrete dynamics)
- 2D motion (continuous dynamics)
Challenge (Hybrid Systems)

Design & verify controller for a robot avoiding obstacles

- Accel / brake / steer (discrete dynamics)
- 2D motion (continuous dynamics)
Challenge (Hybrid Systems)

Design & verify controller for a robot avoiding obstacles

- Dynamic obstacles (other agents)
- Avoid collisions (define safety)
Challenge (Hybrid Systems)

Design & verify controller for a robot avoiding obstacles

- Dynamic obstacles (other agents)
- Avoid collisions (define safety)
Challenge (Hybrid Systems)

Design & verify controller for a robot avoiding obstacles

- Control robot (respect delays)
- Environment interaction (obstacles, agents, uncertainty)
Challenge (Hybrid Systems)

Design & verify controller for a robot avoiding obstacles

- Control robot (respect delays)
- Environment interaction (obstacles, agents, uncertainty)
Outline

1. CPS: Introduction
   - Hybrid Systems & Cyber-Physical Systems
   - Applications
   - Robot Labs

2. 15-424: Foundations of Cyber-Physical Systems
   - Objectives
   - Outline
   - Assessment
   - Labs
   - Resources

3. Approach
   - CPS Contracts
   - CPS Logic
   - Differential Dynamic Logic Family

4. Summary
Foundations!

Modeling & Control
1. Understand the core principles behind CPSs.
2. Develop models and controls.
3. Identify the relevant dynamical aspects.

Computational Thinking
1. Identify safety specifications and critical properties of CPSs.
2. Understand abstraction and system architectures.
3. Learn how to design by invariant.
4. Reason rigorously about CPS models.
5. Verify CPS models of appropriate scale.

CPS Skills
1. Understand the semantics of a CPS model.
2. Develop an intuition for operational effects.
3. Use higher-level model-predictive control.
Course Outline

1. Cyber-physical systems: introduction
2. Differential equations & domains
3. Choice & control
4. Safety & contracts
5. Dynamical systems & Kripke models
6. Truth & proof
7. Control loops & invariants
8. Events & delays
9. Differential equations & invariants
10. Differential equations & proofs
11. Dynamic logic & dynamical systems: differential dynamic logic
12. Dynamical systems: discrete & continuous & hybrid
13. Differential variance & invariance
14. Robots & applications
15. Railway control & applications
16. Air traffic control & applications
17. Car control & applications
Assessment

- Read Academic Integrity Policy
- \(\approx 20\%\) Theory homework Due at \textit{beginning} of lecture
- \(\approx 50\%\) Labs
- Term paper
- \(\approx 10\%\) Midterm
- \(\approx 20\%\) Final

Due at \textbf{beginning} of lecture
Due at 23:59
Due with Lab 6
Robot on Rails
- Autobots, Roll Out
- Charging Station

Robot on Highways
- with event-driven control
- with time-triggered control

Robot on Racetracks
- stay on the circular racetrack
- slow down to avoid collisions

Robot in a Plane
- free motion
- with obstacle avoidance

Robot vs. Roguebot
- avoid collisions with moving obstacles

Robot in Star-lab
## Prerequisites

15-122 Principles of Imperative Computation  
15-251 Great Theoretical Ideas in Computer Science  
21-122 Integration, Differential Equations, and Approximation

- You will be expected to follow extra background reading material as needed.
- Further reading and background material on the course web page
- Check course web page periodically
- Piazza
- Autolab
- KeYmaera
- Ask!
André Platzer.
*Logical Analysis of Hybrid Systems.*
DOI 10.1007/978-3-642-14509-4
http://symbolaris.com/lahs/
CMU library e-book

André Platzer.
*Foundations of Cyber-Physical Systems.*
Lecture notes.
Do not cover everything!
Outline

1. CPS: Introduction
   - Hybrid Systems & Cyber-Physical Systems
   - Applications
   - Robot Labs

2. 15-424: Foundations of Cyber-Physical Systems
   - Objectives
   - Outline
   - Assessment
   - Labs
   - Resources

3. Approach
   - CPS Contracts
   - CPS Logic
   - Differential Dynamic Logic Family

4. Summary
@requires \( v^2 \leq 2b(m-x) \)

@requires \( v \geq 0 \) & \( A \geq 0 \) & \( b > 0 \)

@ensures \( x \leq m \)

\[
\begin{cases} 
\text{if } (v^2 \leq 2b(m-x) - (A+b)(A+2v)) \{ \\
\quad a := A; \\
\text{else } \{ \\
\quad a := -b; \\
\} \\
\} \\
\end{cases}
\]

\[
t := 0; \\
\{x' = v, v' = a, t' = 1, v \geq 0 \text{ and } t \leq 1\}
\]

* @invariant \( v^2 \leq 2b(m-x) \)
v^2 \leq 2 \cdot b \cdot (m-x) \\
& v \geq 0 & A \geq 0 & b > 0 \\
\rightarrow \\
[ \\
\quad \text{if } (v^2 \leq 2 \cdot b \cdot (m-x) - (A+b) \cdot (A+2 \cdot v)) \{ \\
\quad \quad a := A; \\
\quad \} \text{ else } \{ \\
\quad \quad a := -b; \\
\quad \} \\
\quad t := 0; \\
\quad \{x' = v, \ v' = a, \ t' = 1, \ v \geq 0 & t \leq 1\} \\
\} \text{ @invariant } (v^2 \leq 2 \cdot b \cdot (m-x)) \\
] (x \leq m)
Family of Differential Dynamic Logics

discrete  continuous
adversarial
stochastic
nondet
Family of Differential Dynamic Logics

- **Differential dynamic logic**: $d\mathcal{L} = DL + HP$
- **Differential game logic**: $d\mathcal{GL} = GL + HG$
- **Stochastic differential DL**: $Sd\mathcal{L} = DL + SHP$
- **Quantified differential DL**: $Qd\mathcal{L} = FOL + DL + QHP$
Outline

1 CPS: Introduction
   - Hybrid Systems & Cyber-Physical Systems
   - Applications
   - Robot Labs

2 15-424: Foundations of Cyber-Physical Systems
   - Objectives
   - Outline
   - Assessment
   - Labs
   - Resources

3 Approach
   - CPS Contracts
   - CPS Logic
   - Differential Dynamic Logic Family

4 Summary
Can you trust a computer to control physics?

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

CPS Foundations: intellectual grand challenge

Research & Industry
André Platzer.
Logics of dynamical systems.

André Platzer.
*Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics.*

André Platzer.
Differential dynamic logic for hybrid systems.

André Platzer.
Differential dynamic logic for verifying parametric hybrid systems.