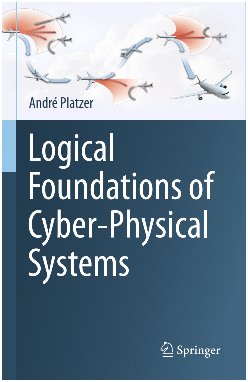
Logical Foundations of Cyber-Physical Systems

01: Cyber-Physical Systems: Overview



Stefan Mitsch

Carnegie Mellon University
Computer Science Department

Outline

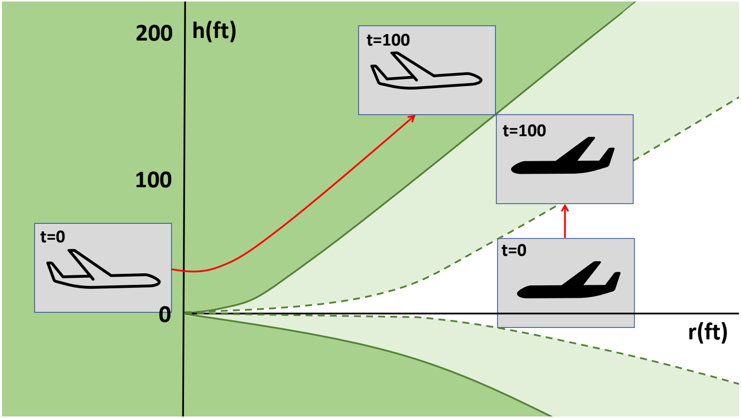
1. CPS: Introduction
   - Hybrid Systems & Cyber-Physical Systems
   - Robot Labs
2. Course: Logical Foundations of Cyber-Physical Systems
   - Educational Approach
   - Objectives
   - Outline
   - Labs
   - Assessment
   - Resources
3. Summary

Outline

1. CPS: Introduction
   - Hybrid Systems & Cyber-Physical Systems
   - Robot Labs
2. Course: Logical Foundations of Cyber-Physical Systems
   - Educational Approach
   - Objectives
   - Outline
   - Labs
   - Assessment
   - Resources
3. Summary

Cyber-Physical Systems Analysis: Aircraft Example

Which control decisions are safe for aircraft collision avoidance?



Cyber-Physical Systems

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

CPSs Promise Transformative Impact!

Prospects: Safe & Efficient

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

Prerequisite: CPSs need to be safe

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

Can you trust a computer to control physics?

Can you trust a computer to control physics?

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

Can you trust a computer to control physics?

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

Course Rationale

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

Can you trust a computer to control physics?

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

Course Rationale

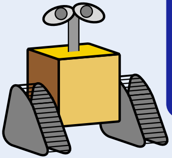
1. Safety guarantees require analytic foundations.
2. A common foundational core helps all application domains.
3. Foundations revolutionized digital computer science & our society.
4. Need even stronger foundations when software reaches out into our physical world.

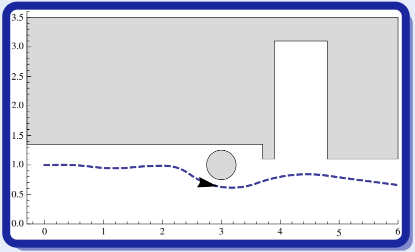
CPSs deserve proofs as safety evidence!

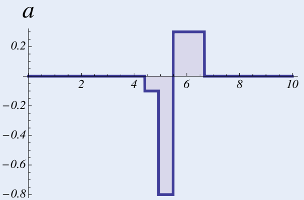
Challenge (CPS)

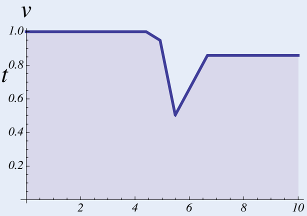
Describe state evolution with both

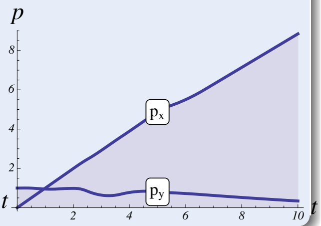
- Discrete dynamics (control decisions)
- Continuous dynamics (differential equations)







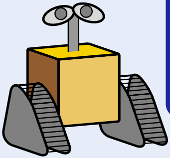


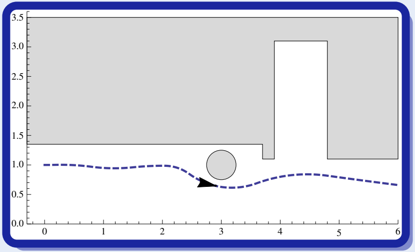


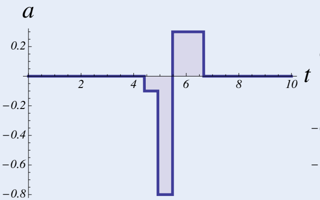
Challenge (CPS)

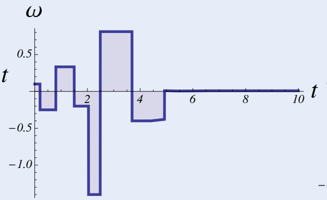
Describe state evolution with both

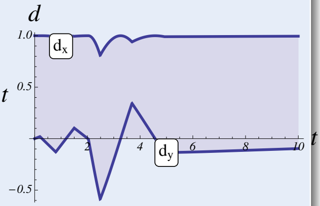
- Discrete dynamics (control decisions)
- Continuous dynamics (differential equations)











Hybrid Systems Versus Cyber-Physical Systems

Technical characteristics:

Definition (Cyber-Physical Systems)

(Distributed networks of) computerized control for physical system
Communication, computation, and control for physics

We will model CPSs as Hybrid Systems

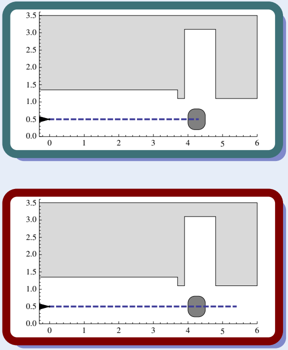
Mathematical model for complex physical systems:

Definition (Hybrid Systems)

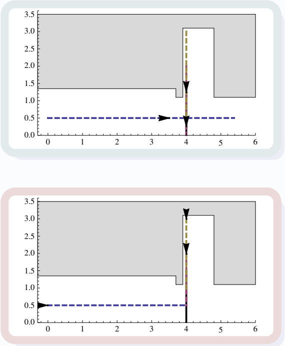
Systems with interacting discrete and continuous dynamics

LFCPS Labs

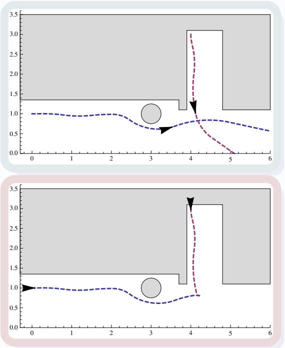
1: Charging Station



2: Follow the Leader



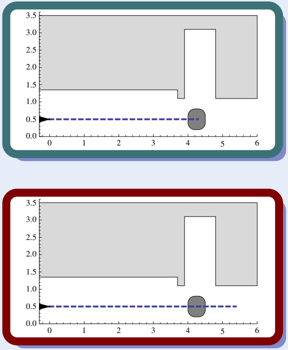
4: Obstacles



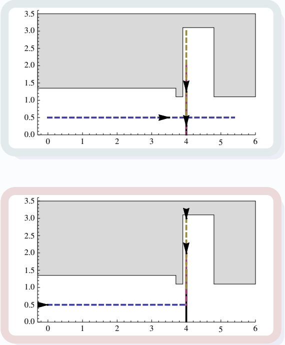
- ✓ Design, model
- ✓ Verify

LFCPS Labs

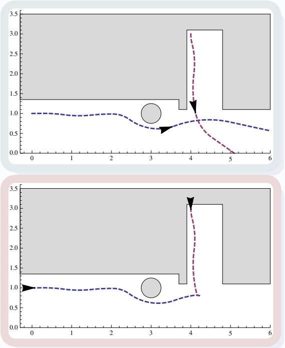
1: Charging Station



2: Follow the Leader

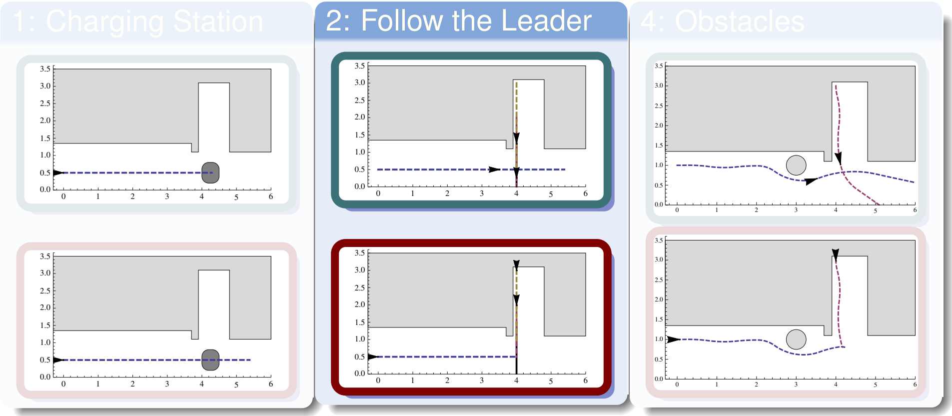


4: Obstacles



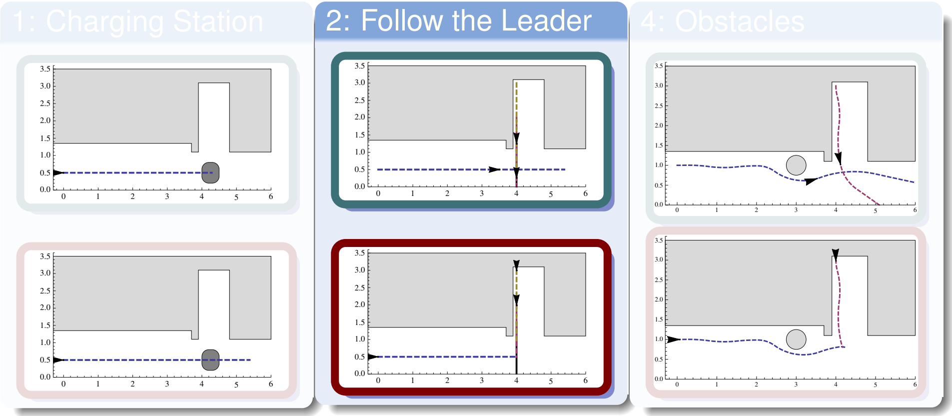
- ✓ Design, model
- ✓ Verify

LFCPS Labs



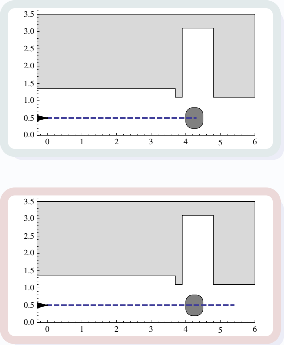
- ✓ Design, model
- ✓ Verify

LFCPS Labs

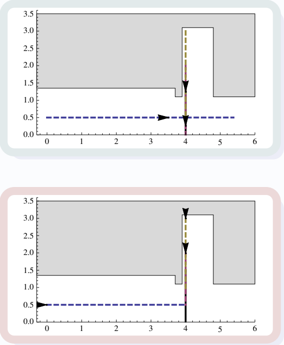


- ✓ Design, model
- ✓ Verify

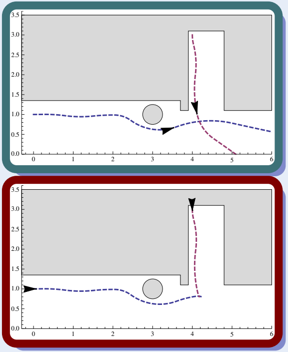
1: Charging Station



2: Follow the Leader



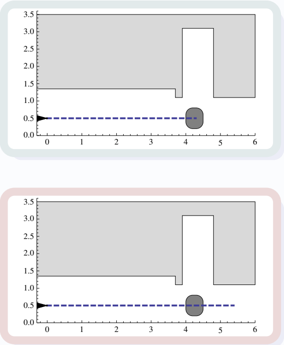
4: Obstacles



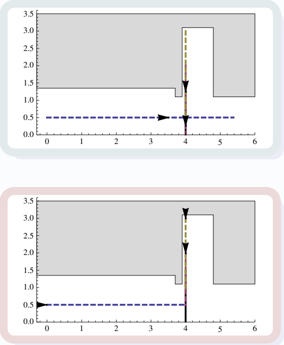
- ✓ Design, model
- ✓ Verify

LFCPS Labs

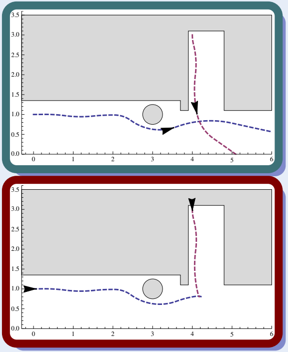
1: Charging Station



2: Follow the Leader



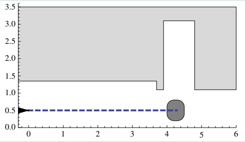
4: Obstacles

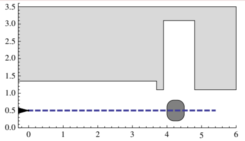


- ✓ Design, model
- ✓ Verify

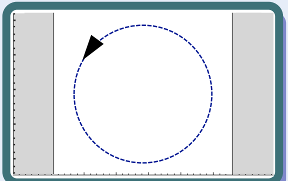
LFCPS Labs

1: Charging Station

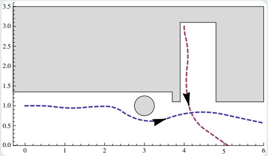


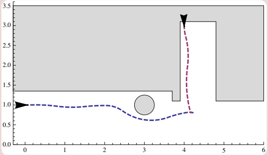


3: Racetrack



4: Obstacles

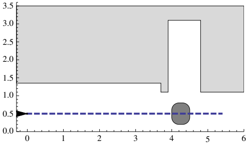


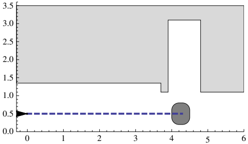


- ✓ Design, model
- ✓ Verify

LFCPS Labs

What is safety?



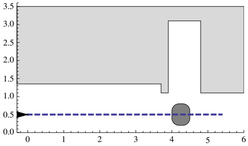


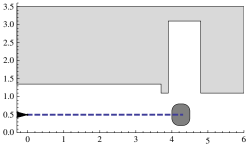
What is safety?

Never drive past the goal?

Positive distance to all obstacles always?

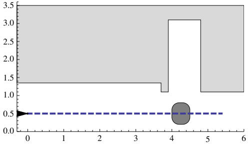
What if they are moving?



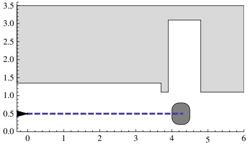


What is safety?

Never drive past the goal?
Positive distance to all obstacles always?
What if they are moving?

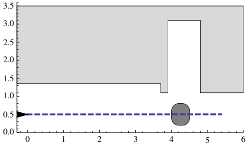


How to balance safety with achieving goals?



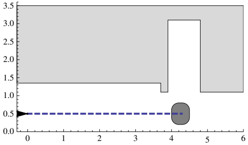
What is safety?

Never drive past the goal?
Positive distance to all obstacles always?
What if they are moving?



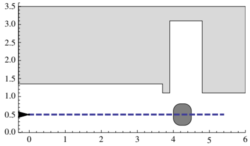
How to balance safety with achieving goals?

What if staying put is safe but not useful?
What if there are conflicting goals?



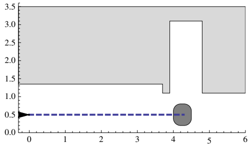
What is safety?

Never drive past the goal?
Positive distance to all obstacles always?
What if they are moving?



How to balance safety with achieving goals?

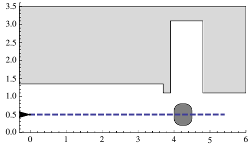
What if staying put is safe but not useful?
What if there are conflicting goals?



Findings of formal models relate to reinforcement learning!

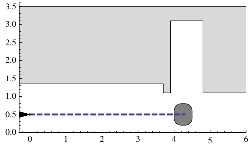
What is safety?

Never drive past the goal?
Positive distance to all obstacles always?
What if they are moving?



How to balance safety with achieving goals?

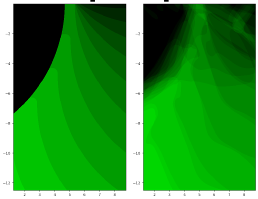
What if staying put is safe but not useful?
What if there are conflicting goals?



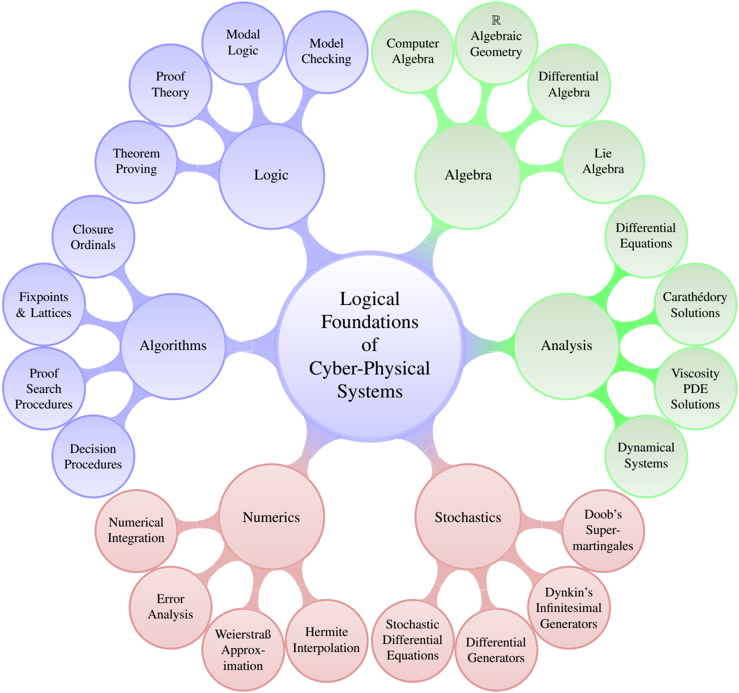
Findings of formal models relate to reinforcement learning!

Reward functions and reward shaping

[FM'21]



Outline


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 Learn Cyber-Physical Systems Foundations?

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

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

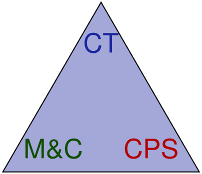
1. CPSs are so easy to get wrong.
2. Retrofitting CPSs for safety is not possible.
3. These logical aspects are an integral part of CPS design.
4. Critical to your understanding of the intricate complexities of CPS.
5. Tame complexity by a simple programming language for core aspects.

About Logical Foundations of Cyber-Physical Systems

- 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 in system design.
  3. Express pre- and postconditions for CPS models.
  4. Use design-by-invariant.
  5. Reason rigorously about CPS models.
  6. Verify CPS models of appropriate scale.
- CPS Skills
  1. Understand the semantics of a CPS model.
  2. Develop an intuition for operational effects.
  3. Identify control constraints.
  4. Understand opportunities and challenges in CPS and verification.
- Byproducts
  1. Well-motivated exposure to numerous math and science areas in action.

Learning Objectives

identify safety specifications for CPS
rigorous reasoning about CPS
understand abstraction & architectures
programming languages for CPS
verify CPS models at scale



cyber+physics models
core principles of CPS
relate discrete+continuous

semantics of CPS models
operational effects
identify control constraints
opportunities and challenges

Textbook and Course Outline

I **Part: Elementary Cyber-Physical Systems**

2. Differential Equations & Domains
3. Choice & Control
4. Safety & Contracts
5. Dynamical Systems & Dynamic Axioms
6. Truth & Proof
7. Control Loops & Invariants
8. Events & Responses
9. Reactions & Delays

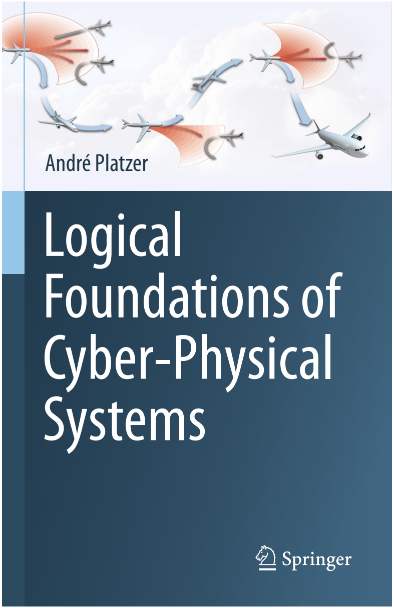
II **Part: Differential Equations Analysis**

10. Differential Equations & Differential Invariants
11. Differential Equations & Proofs
12. Ghosts & Differential Ghosts
13. Differential Invariants & Proof Theory

III **Part: Adversarial Cyber-Physical Systems**

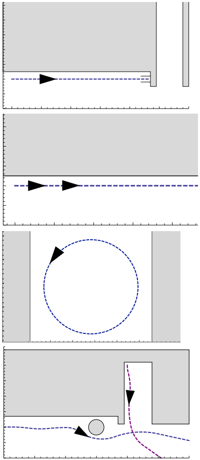
-17. Hybrid Systems & Hybrid Games

IV **Part: Comprehensive CPS Correctness**



Robot Model Labs

1. Robot on Rails
   a. Autobots, Roll Out
   b. Charging Station
2. Robot on Highways: Follow the Leader
   a. with event-triggered control
   b. with time-triggered control
3. Robot on Racetracks
   a. stay on the circular racetrack
   b. slow down to avoid collisions
4. Robot in a Plane
   a. with obstacle avoidance
   b. Robot vs. Roguebot: don't collide with moving obstacles
5. Robot in Star-lab: self-defined final project
6. Final project presentation



Assessment

- TODO: Read Course Policies ▸ Syllabus
- ≈5% Theory assignments, ≈22% quizzes — Due at midnight
- ≈29% Labs, ≈22% final project
  1. Betabot in first week — Due at **beginning** of lecture
  2. Veribot in second week — Due at midnight
- Whitepaper — For final project
- Proposal — For final project
- Term paper — Due with final project
- Final project presentation — Fri Dec 9
- ≈11% Midterm I — In class
- ≈11% Midterm II — In class
- Partner allowed for labs only and only starting in lab 2

Resources

Prerequisites

15-122 Principles of Imperative Computation — if-then-else
21-120 Differential and Integral Calculus — x'
(21-241 Matrix algebra **or**
15-251 Great Theoretical Ideas in Computer Science **or** — Math proofs
18-202 Mathematical Foundations of Electrical Engineering)
Substitutes: 21-242 Matrix theory **or** 21-341 Linear algebra I for 21-241

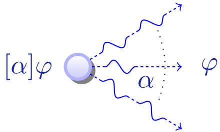
- You are expected to follow extra material in the textbook.
- Further reading and background material on the course web page
- Check course web page periodically
  https://www.cs.cmu.edu/~smitsch/courses/lfcps22
- KeYmaera X: aXiomatic Tactical Theorem Prover for Hybrid Systems
- Diderot, Office Hours, Ask!

Outline

Logical foundations make a big difference for CPS, and vice versa

differential dynamic logic

$\text{dL} = \text{DL} + \text{HP}$



Course content

- Analytic foundations
- Practical reasoning
- Significant applications
- Catalyze many science areas

Skills

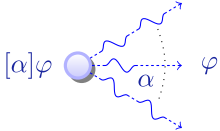
1. Model dynamical systems
2. Combine simple dynamics
3. Tame complexity
4. Verification and validation

Numerous wonders remain to be discovered!

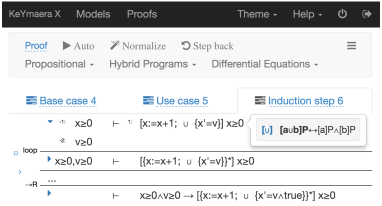
Logical foundations make a big difference for CPS, and vice versa

differential dynamic logic

$$\mathsf{dL} = \mathsf{DL} + \mathsf{HP}$$



KeYmaera X



Course content

- Analytic foundations
- Practical reasoning
- Significant applications
- Catalyze many science areas

Numerous wonders remain to be discovered!