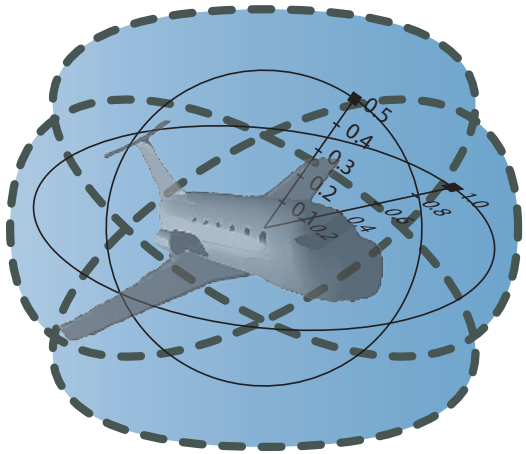
15-424/15-624: Foundations of Cyber-Physical Systems

01: Overview

André Platzer

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

http://symbolaris.com/course/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

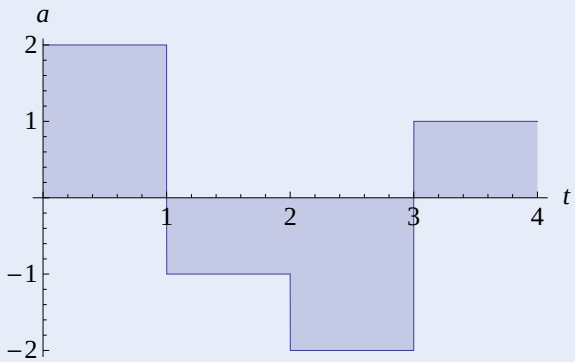
Outline

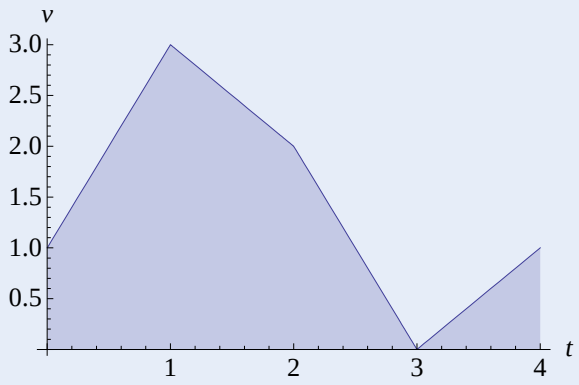
1. CPS: Introduction
   - Hybrid Systems & Cyber-Physical Systems
   - Applications
   - Robot Labs
2. 15-424: Foundations of Cyber-Physical Systems
   - Objectives
   - Outline
   - Assessment
   - Labs
   - Resources
3. Approach
   - CPS Contracts
   - CPS Logic
   - Differential Dynamic Logic Family
4. Summary

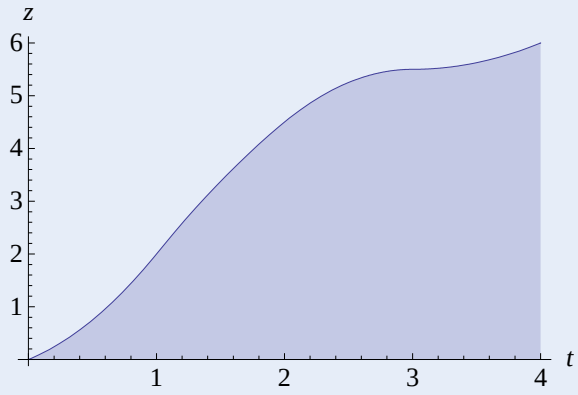
Challenge

Hybrid systems

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



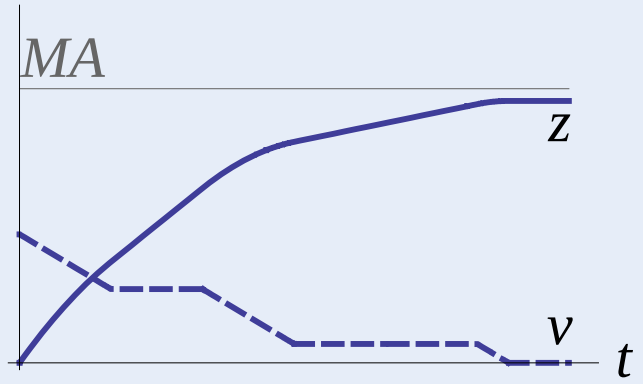




Challenge

Hybrid systems

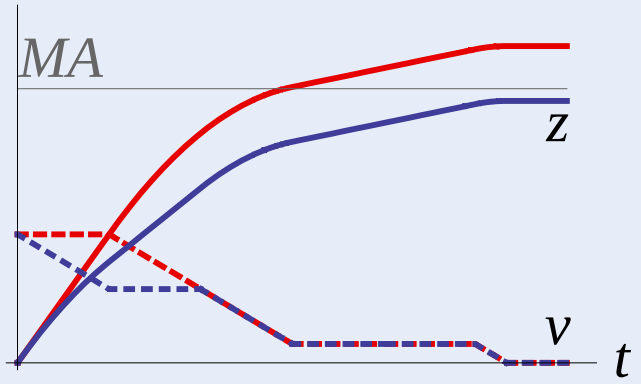
- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)



Challenge

Hybrid systems

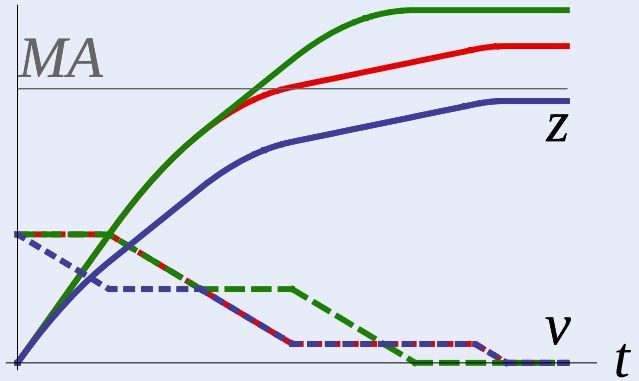
- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)



Challenge

Hybrid systems

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



Train Control

Challenge

Hybrid systems

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

1. More than computers: no `NullPointerException` $\not\Rightarrow$ 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

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:

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

Challenge

Hybrid systems

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

Train Control

Challenge

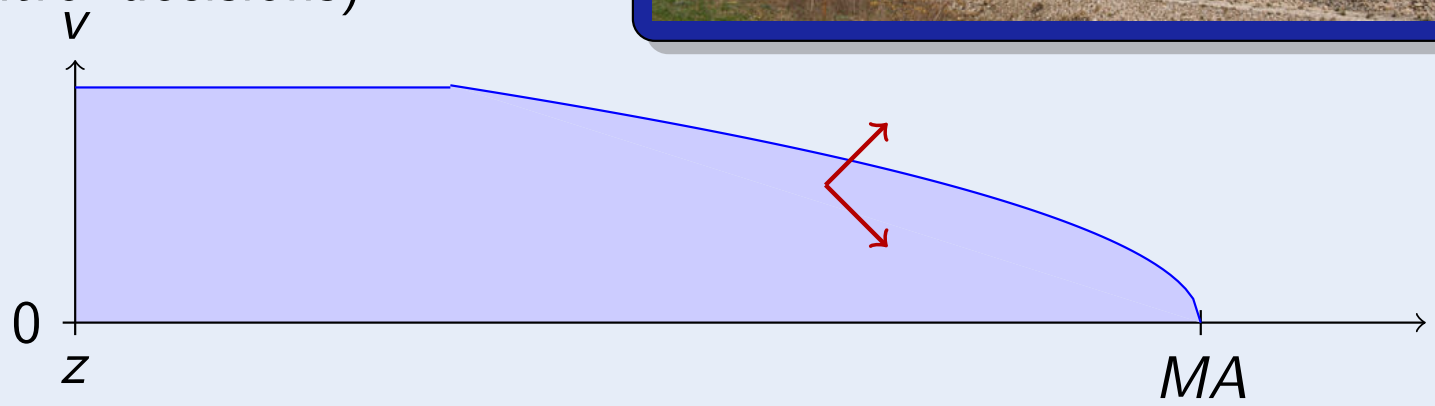
Hybrid systems

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

Challenge

Hybrid systems

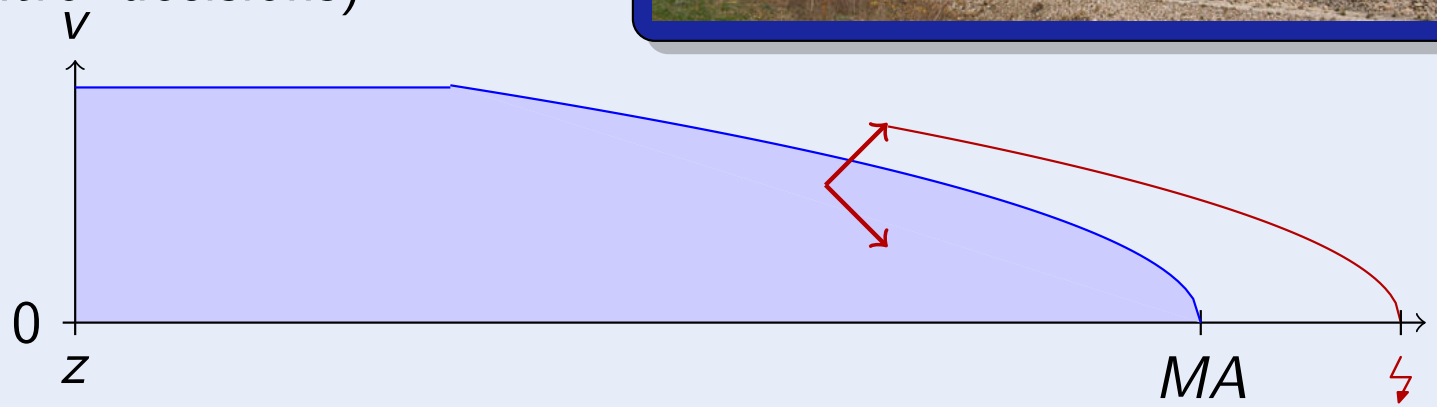
- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)



Challenge

Hybrid systems

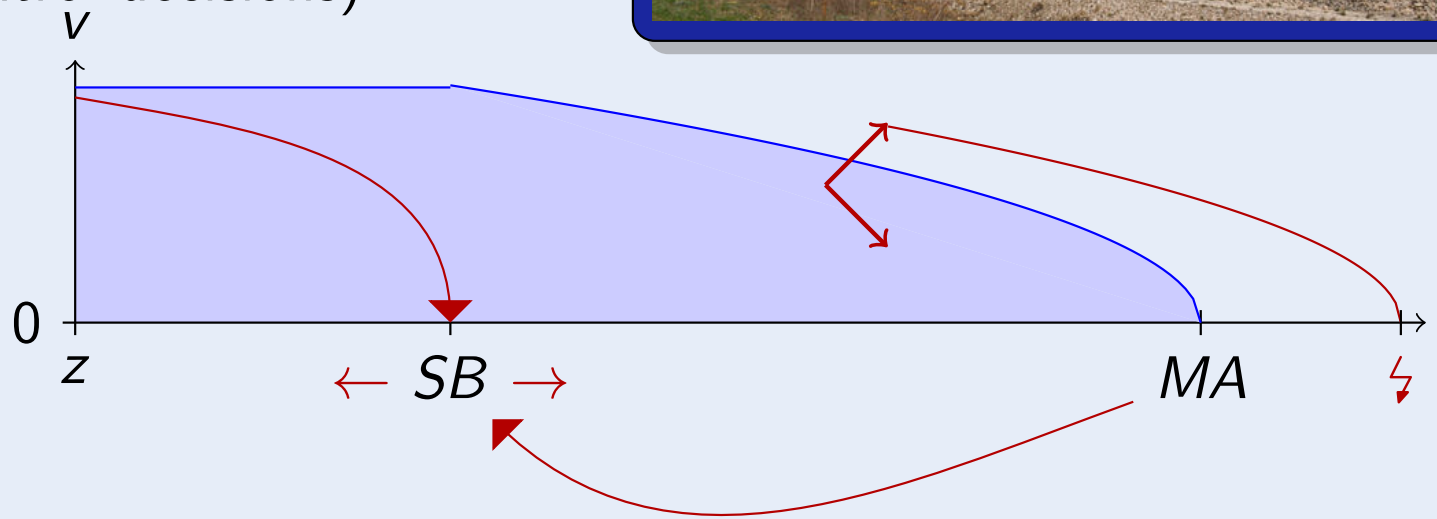
- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)



Challenge

Hybrid systems

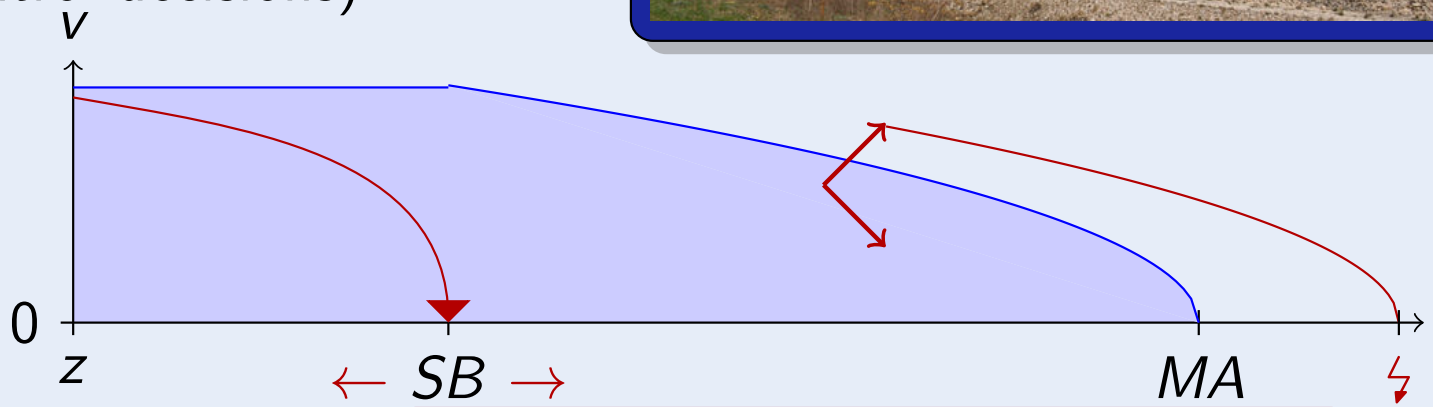
- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)



Challenge

Hybrid systems

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

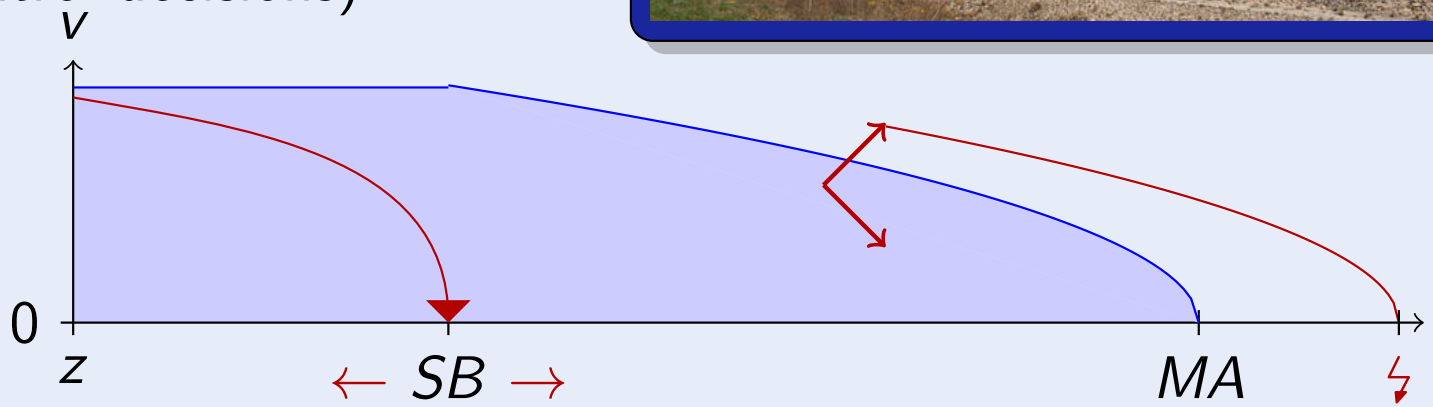


$$SB \geq \frac{v^2}{2b} + \frac{a^2\varepsilon^2}{2b} + \frac{a}{b}\varepsilon v + \frac{a}{2}\varepsilon^2 + \varepsilon v$$

Challenge

Hybrid systems

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



$\forall MA\, \exists SB$ "train always safe"

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)

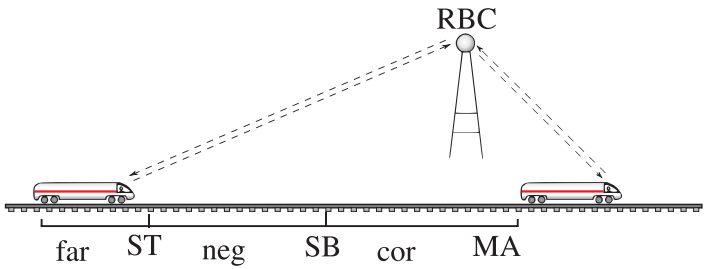
(Distributed network of) computerized control for physical system

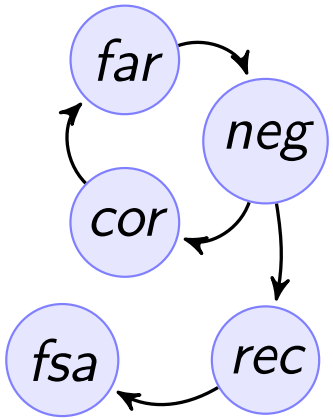
What CPS are around us?

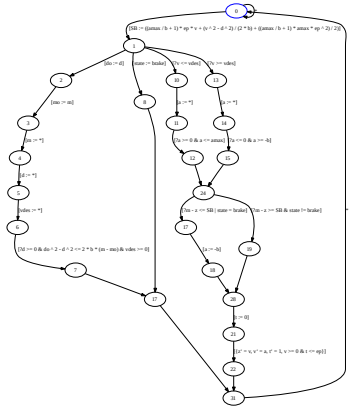
What CPS will be around us in the future?

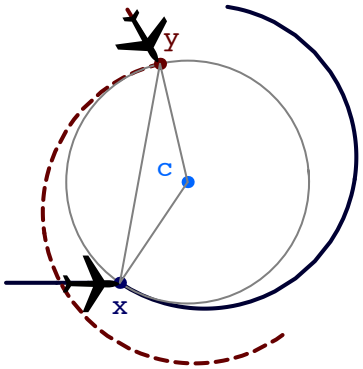
Which CPS do we trust with our lives?

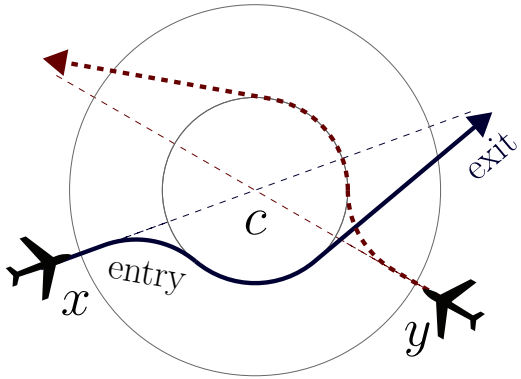
Successful Hybrid Systems Proofs

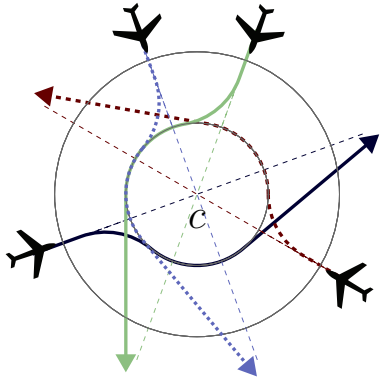


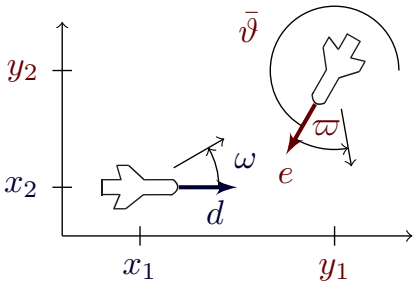


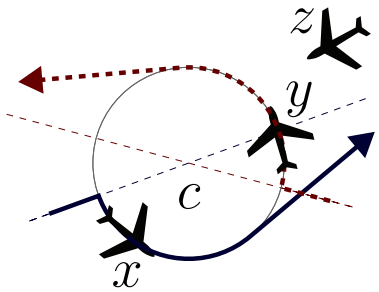


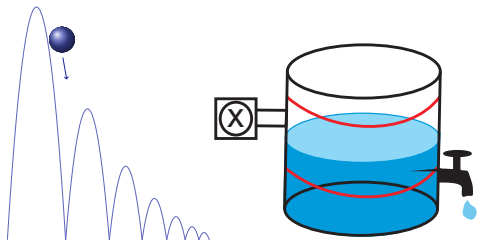




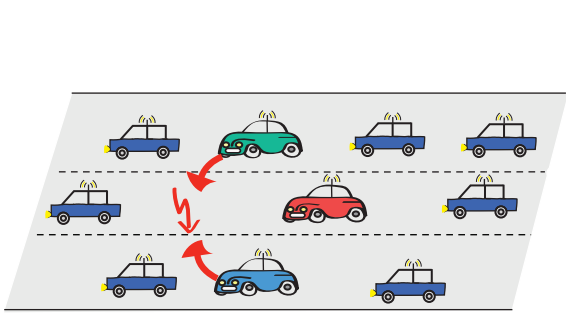


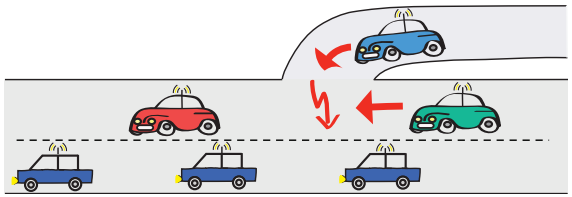


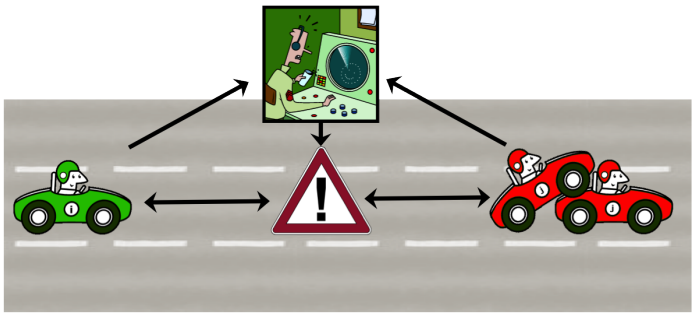


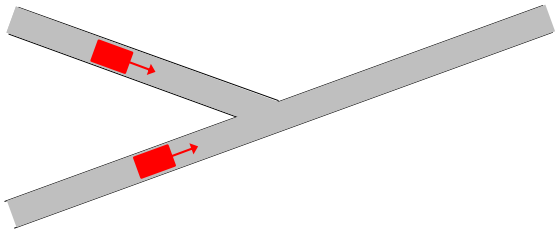


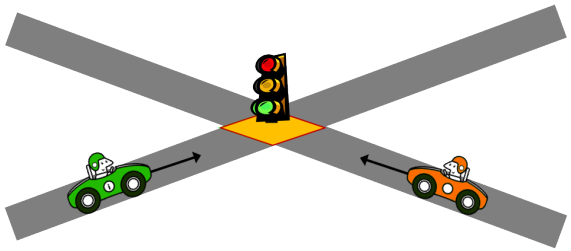
Successful Hybrid Systems Proofs

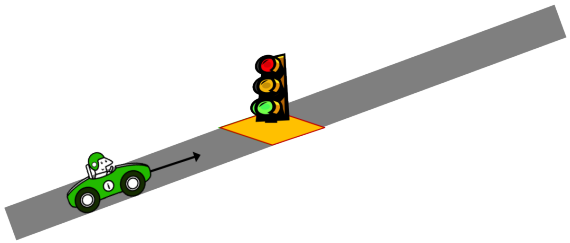


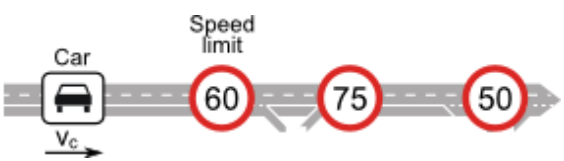


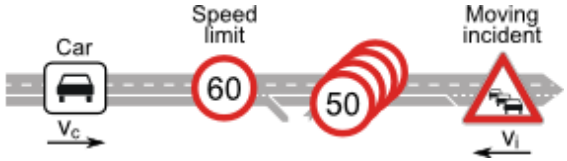


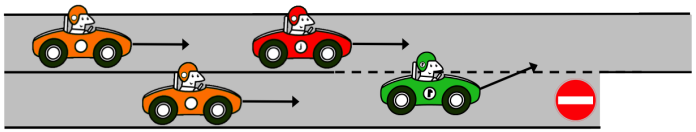


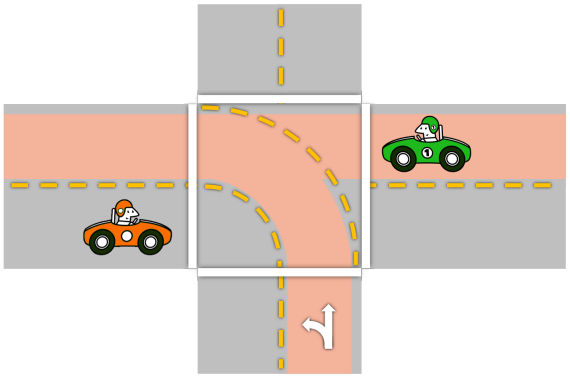


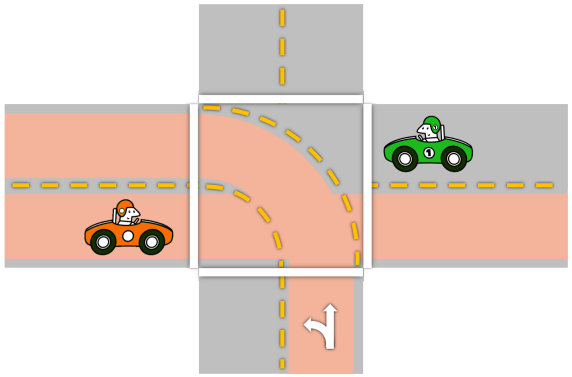


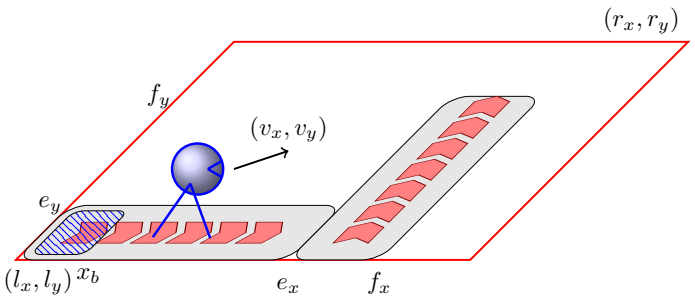




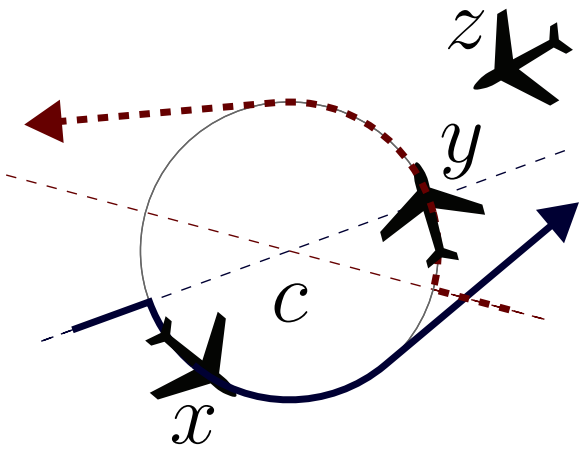


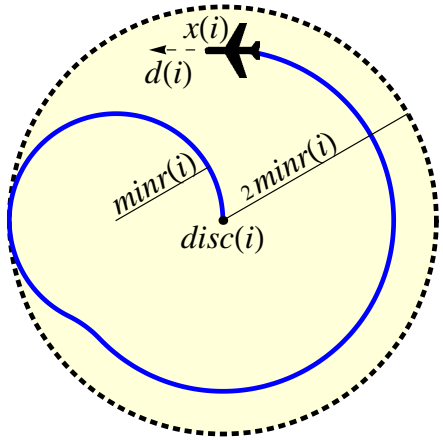


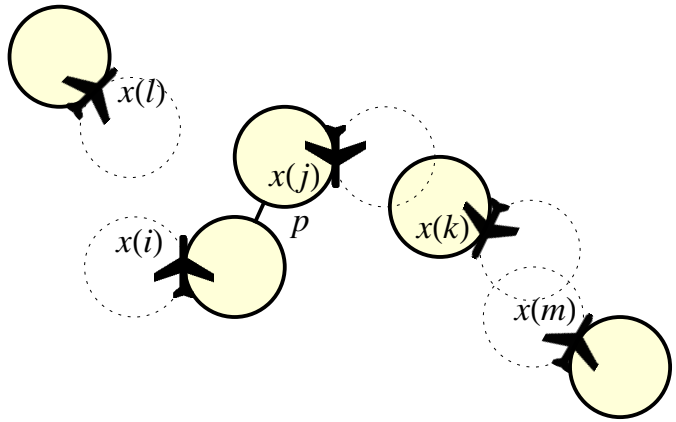


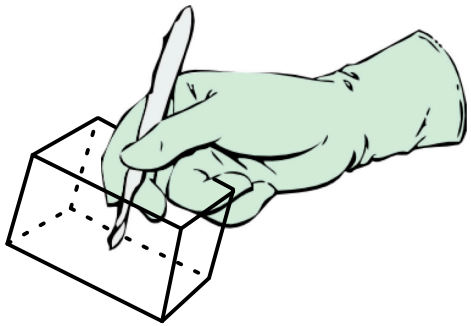


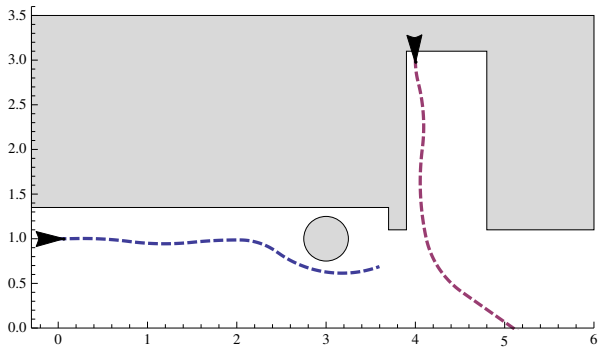
Successful Hybrid Systems Proofs

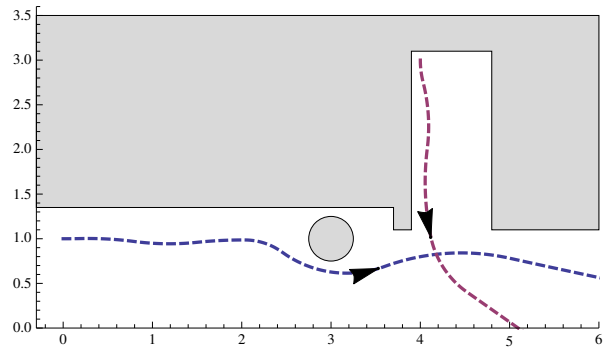


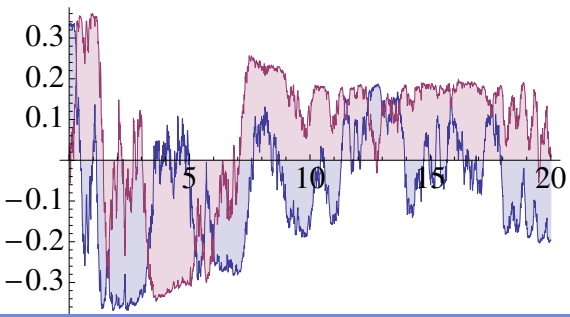


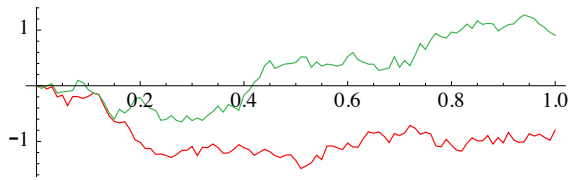


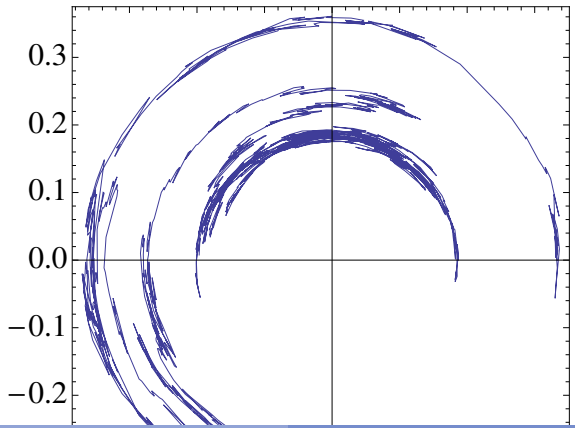








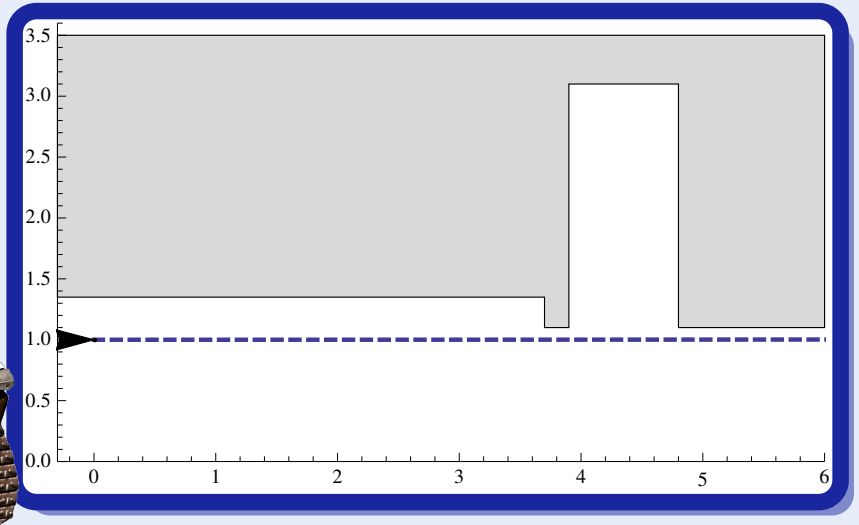


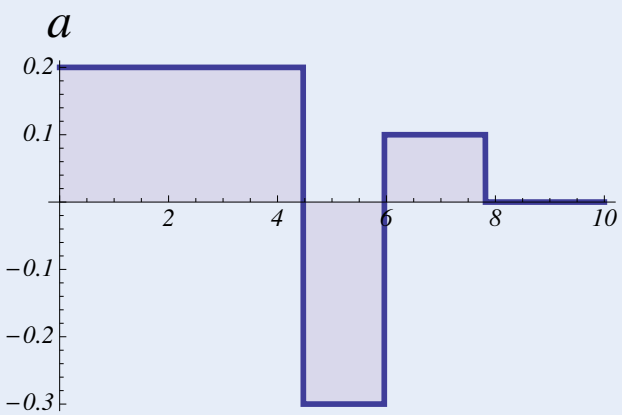


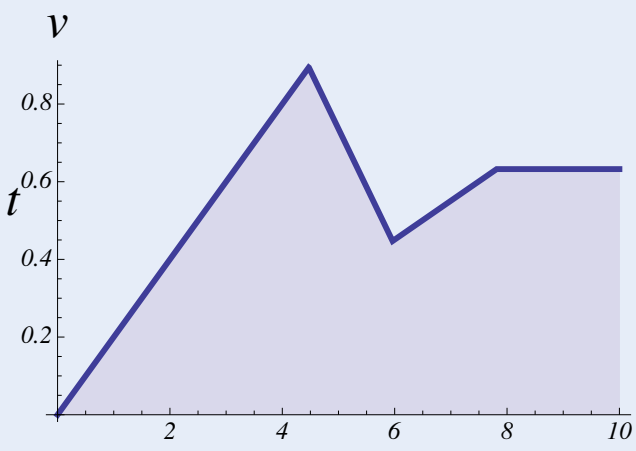
Challenge (Hybrid Systems)

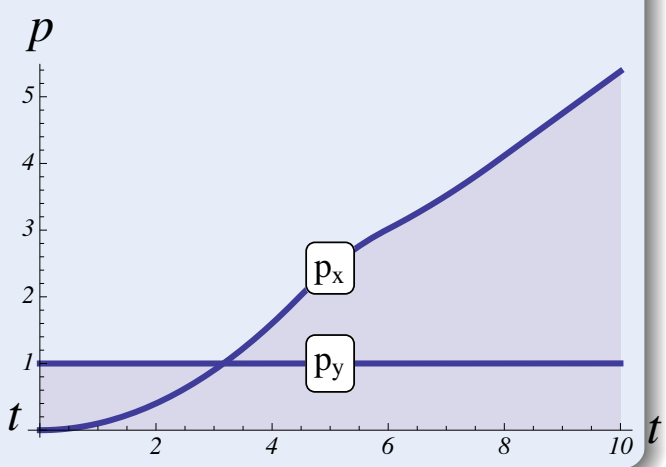
Design & verify controller for a robot avoiding obstacles

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





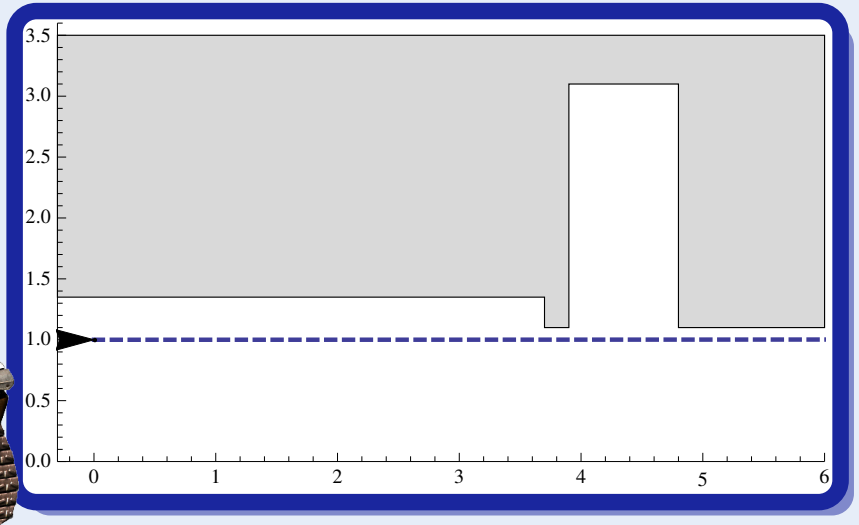


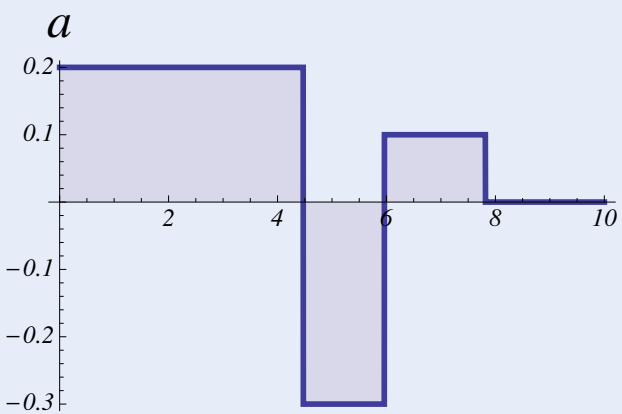


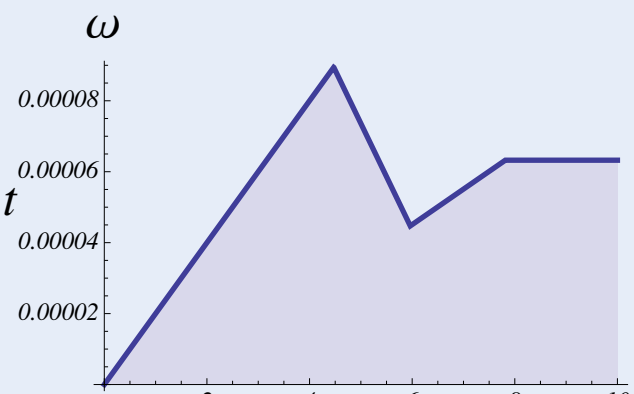
Challenge (Hybrid Systems)

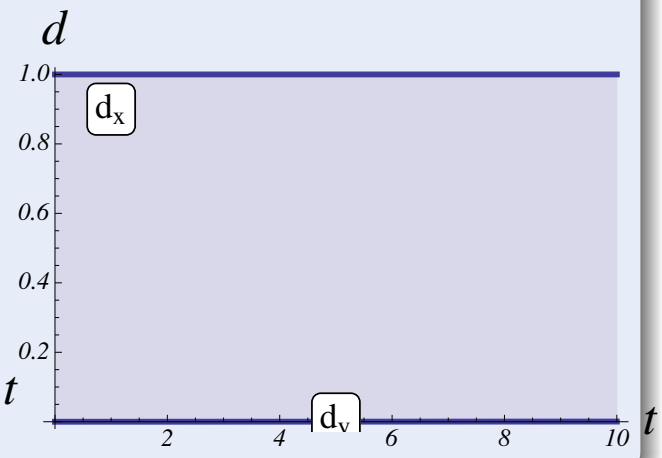
Design & verify controller for a robot avoiding obstacles

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





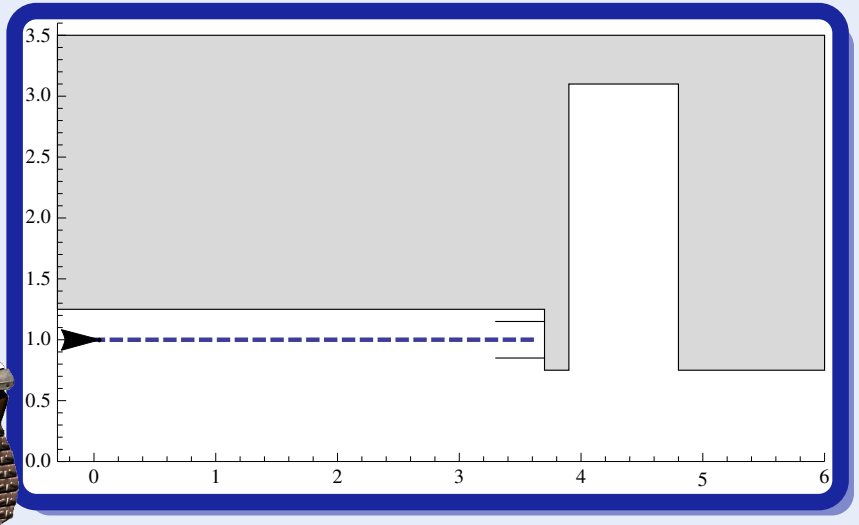


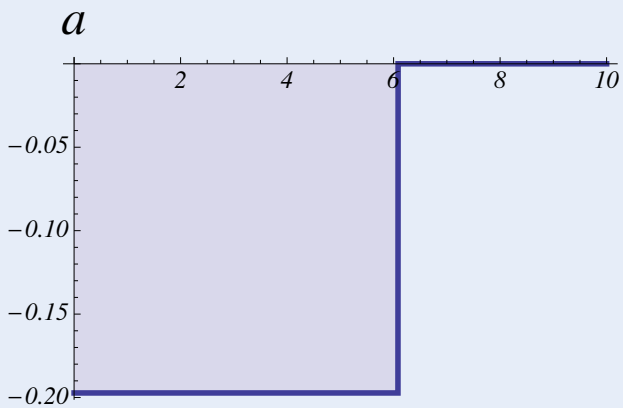


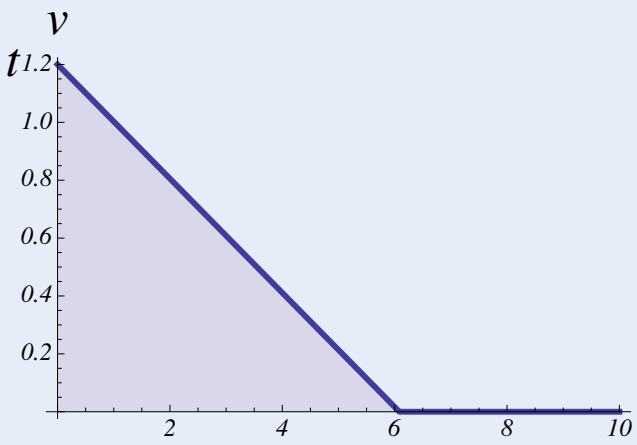
Challenge (Hybrid Systems)

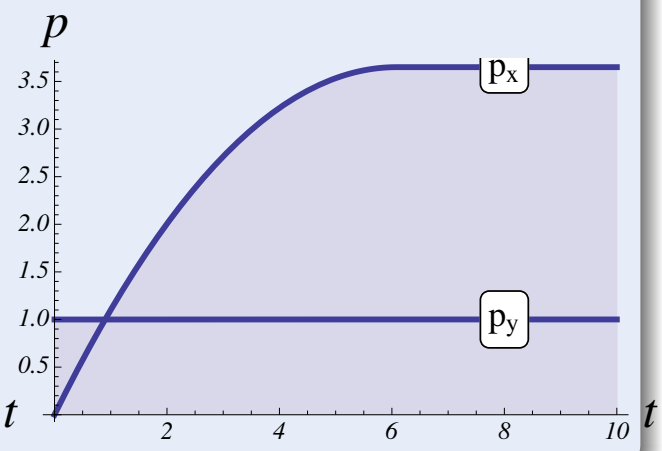
Design & verify controller for a robot avoiding obstacles

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





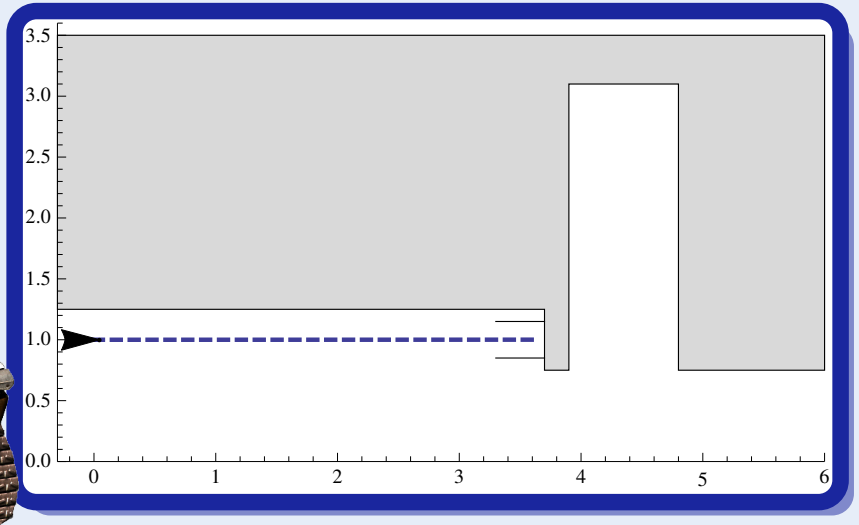


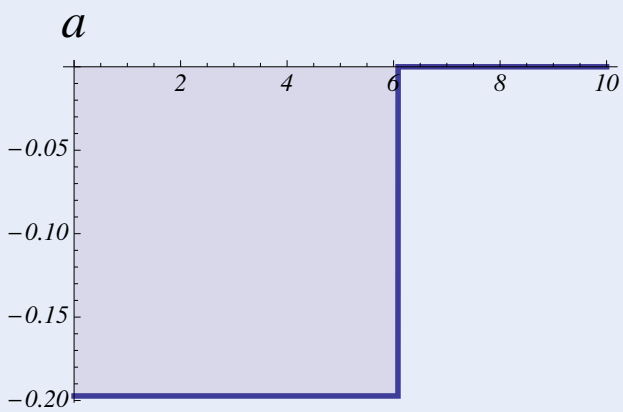


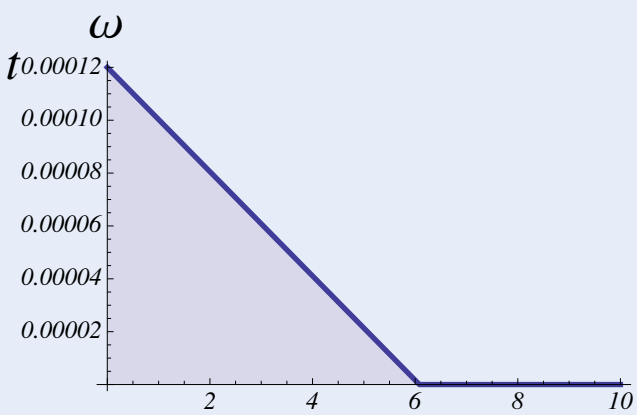
Challenge (Hybrid Systems)

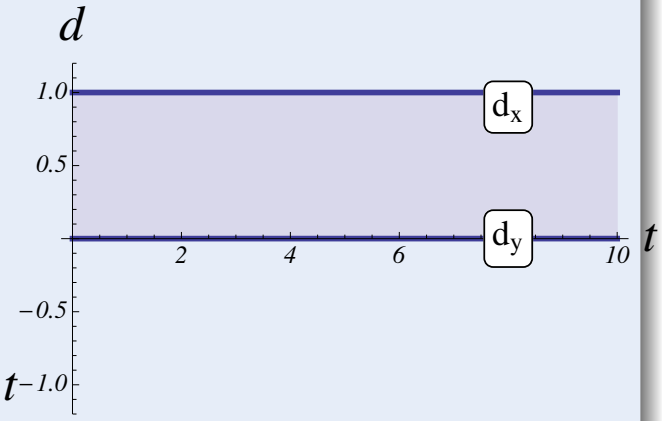
Design & verify controller for a robot avoiding obstacles

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





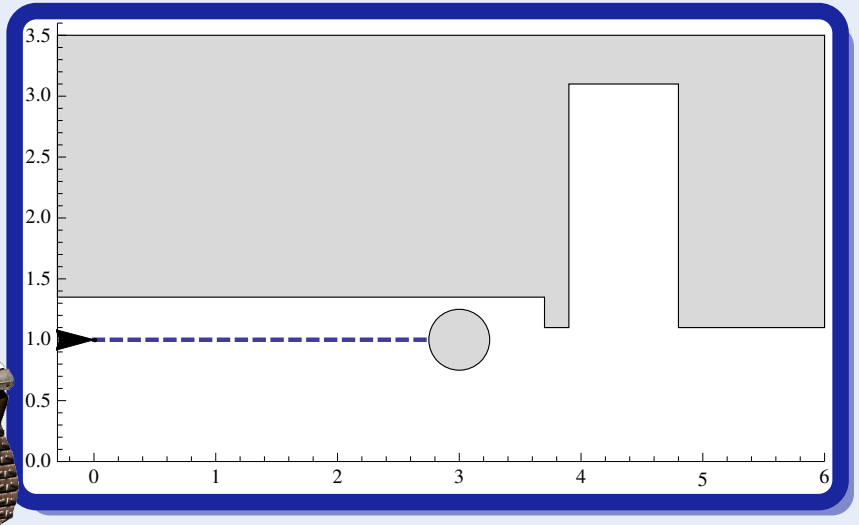


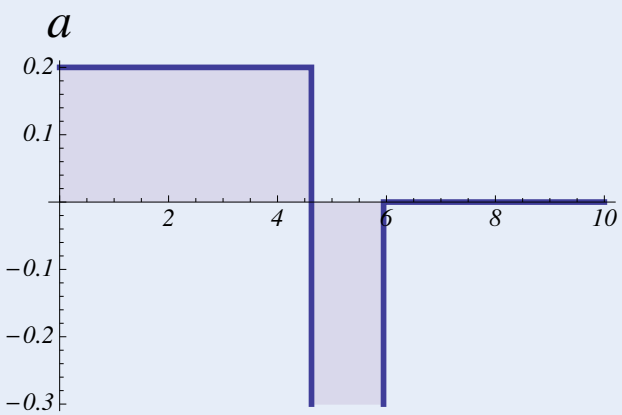


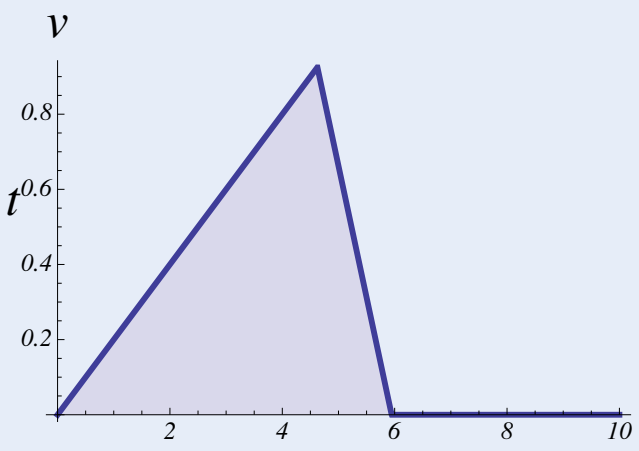
Challenge (Hybrid Systems)

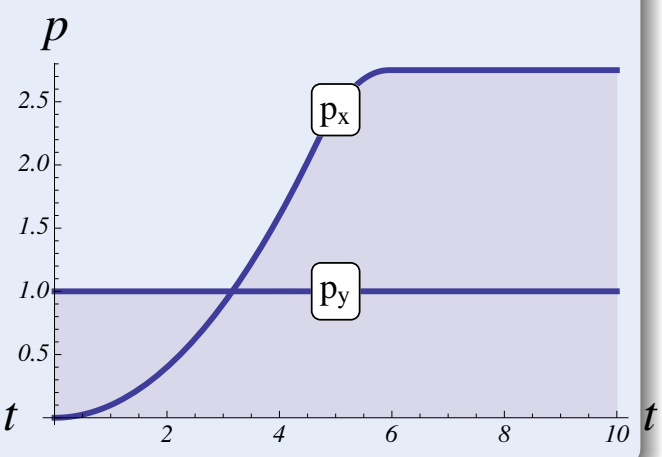
Design & verify controller for a robot avoiding obstacles

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





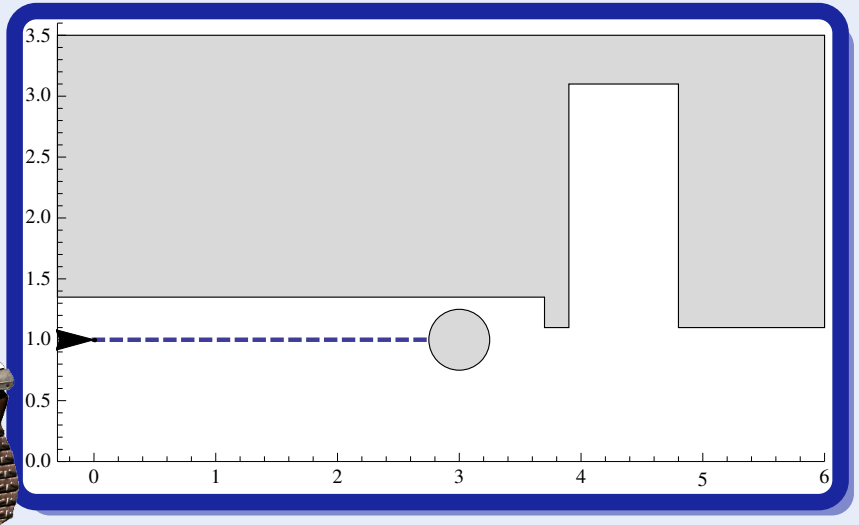


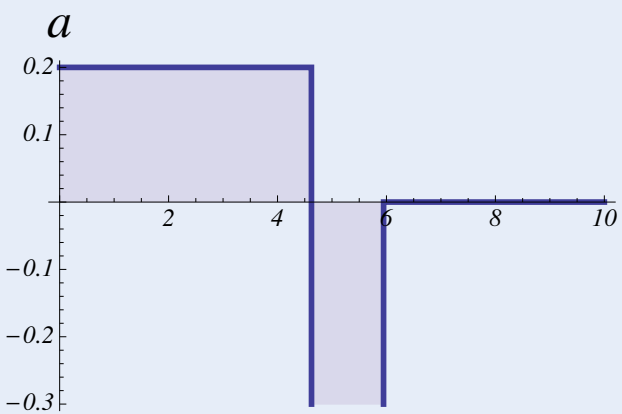


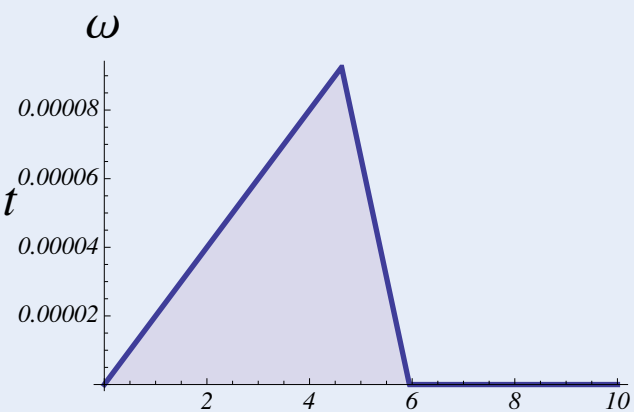
Challenge (Hybrid Systems)

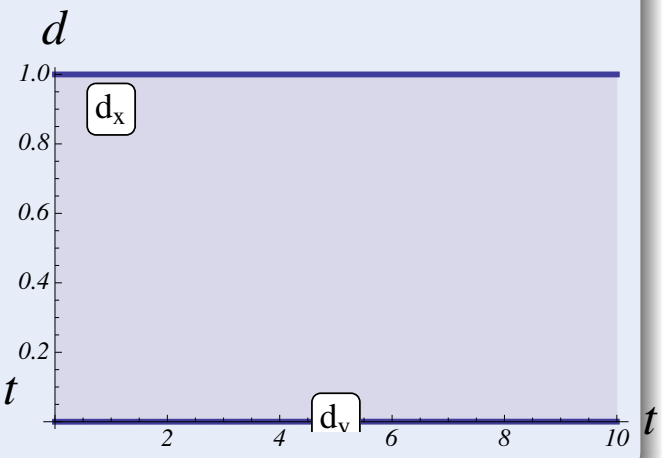
Design & verify controller for a robot avoiding obstacles

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





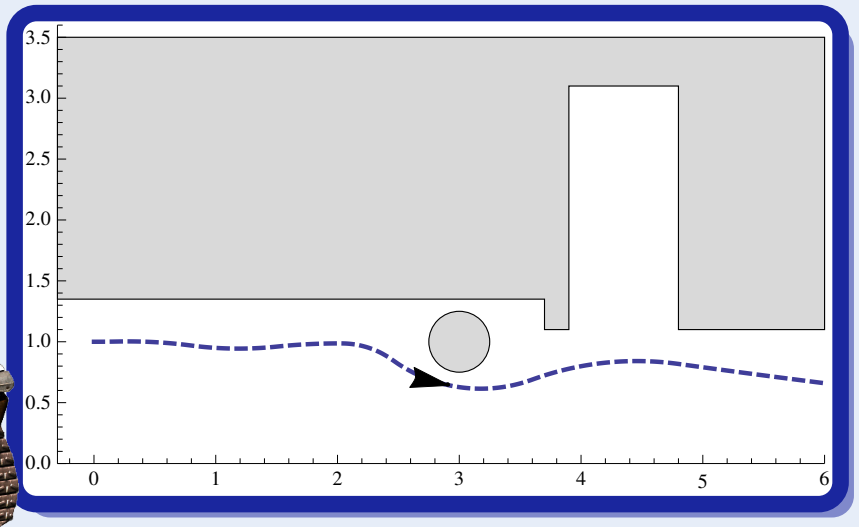


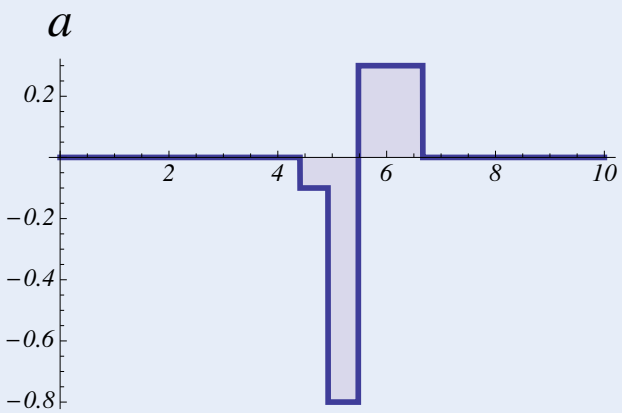


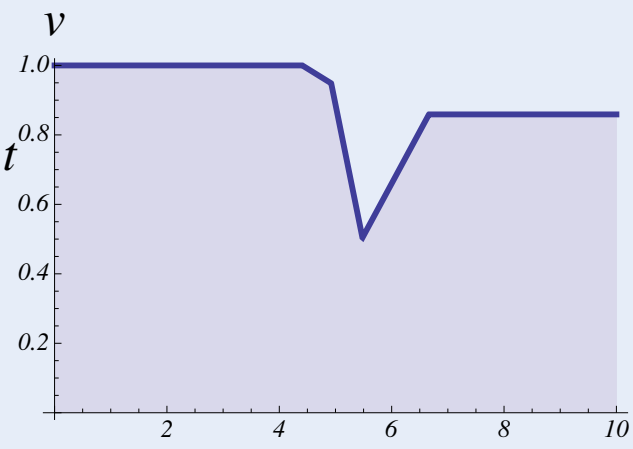
Challenge (Hybrid Systems)

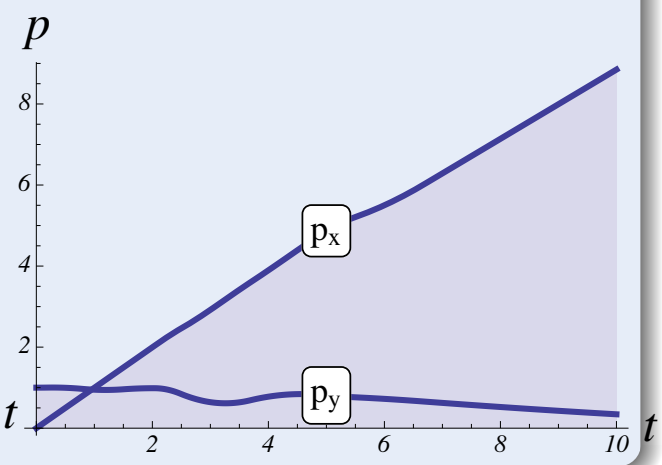
Design & verify controller for a robot avoiding obstacles

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





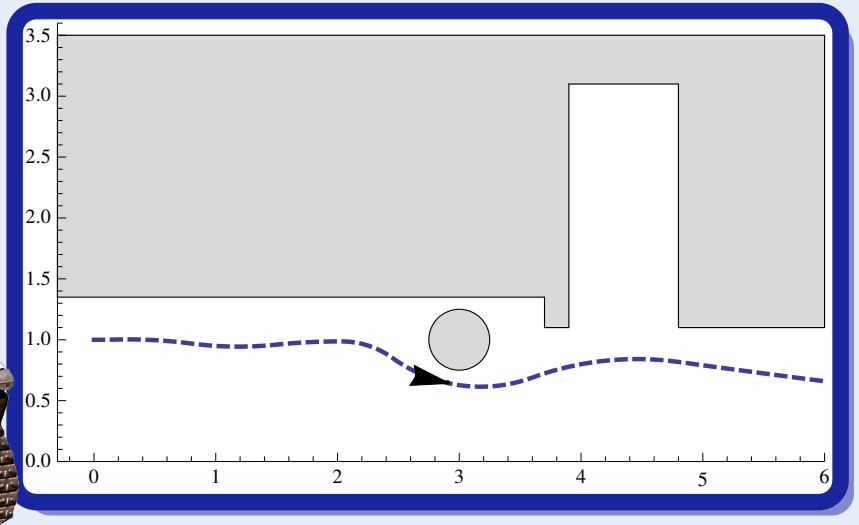


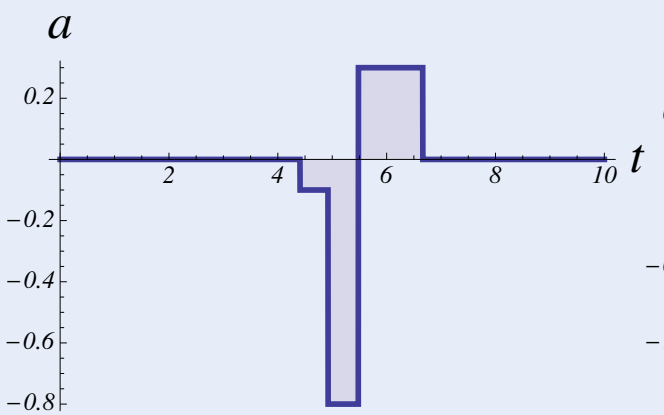


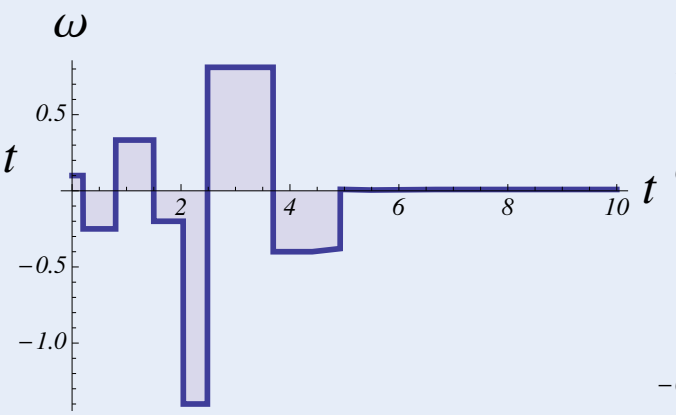
Challenge (Hybrid Systems)

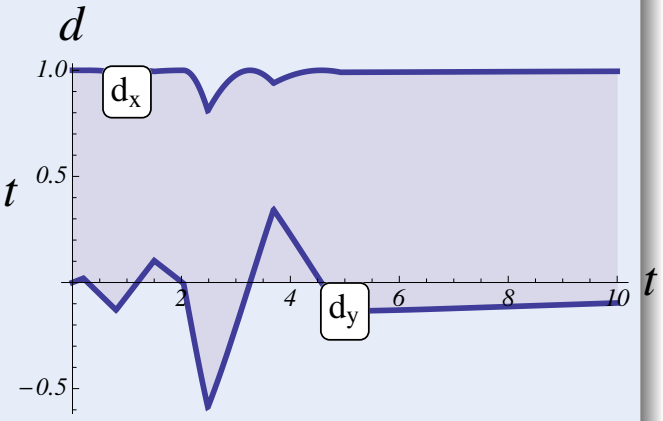
Design & verify controller for a robot avoiding obstacles

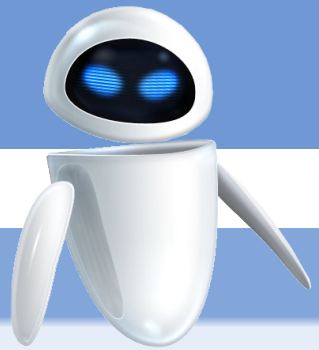
- Accel / brake / steer (discrete dynamics)
- 2D motion (continuous dynamics)







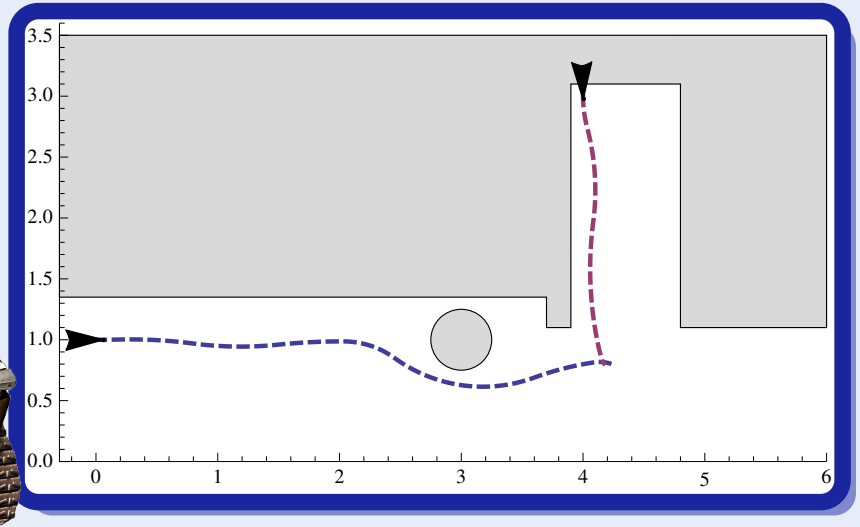


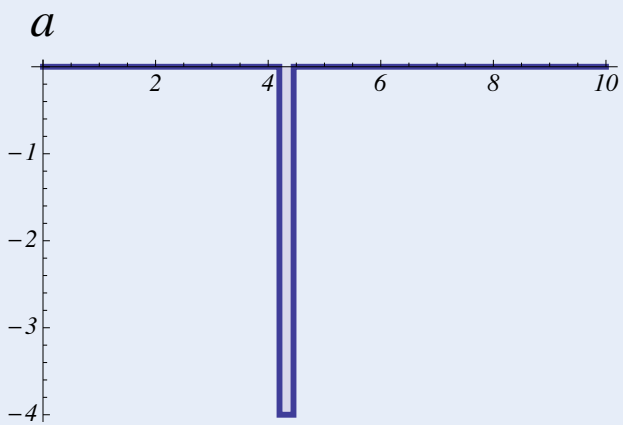


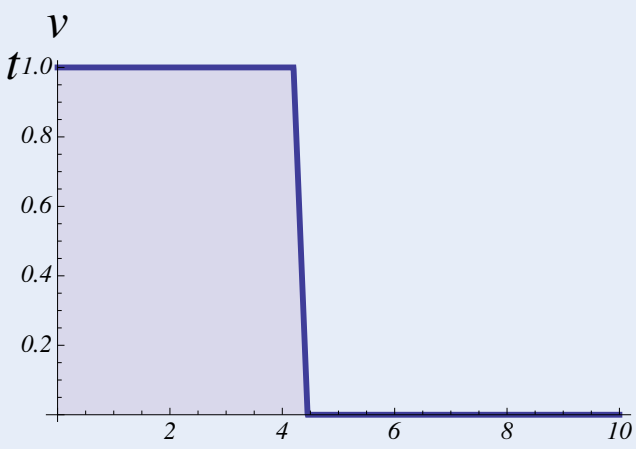
Challenge (Hybrid Systems)

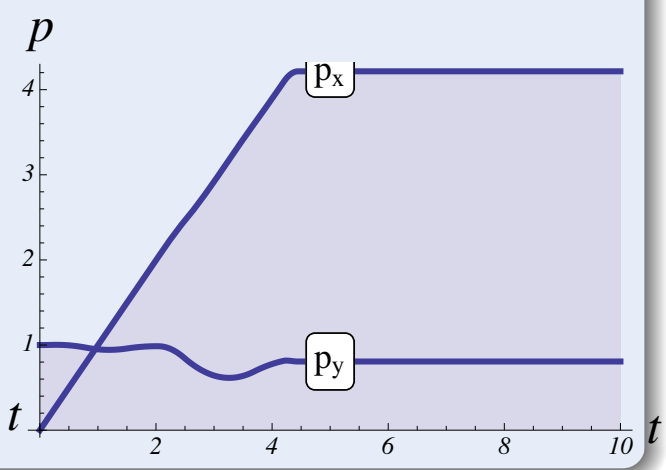
Design & verify controller for a robot avoiding obstacles

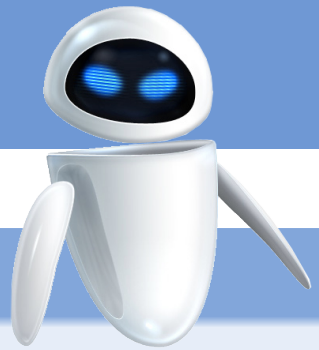
- Dynamic obstacles (other agents)
- Avoid collisions (define safety)







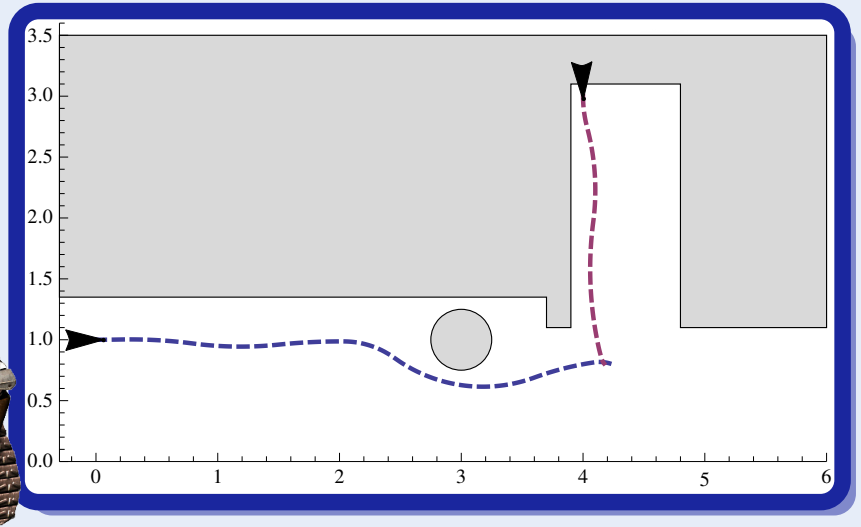


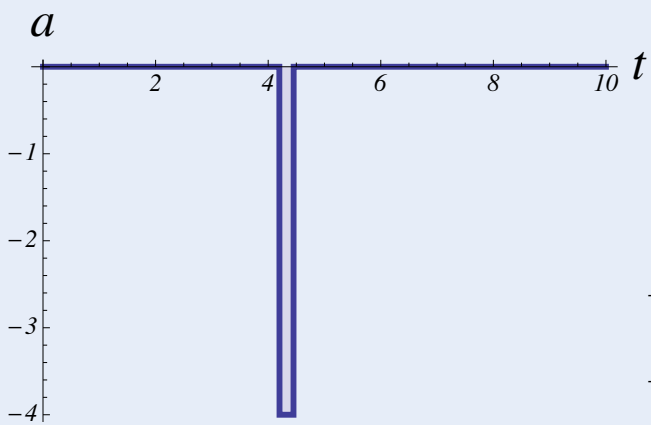


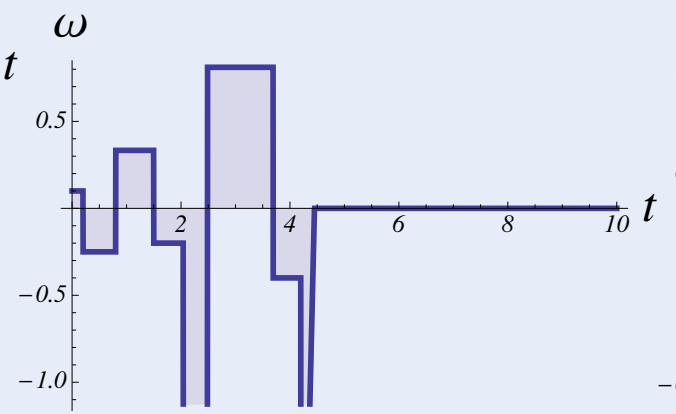
Challenge (Hybrid Systems)

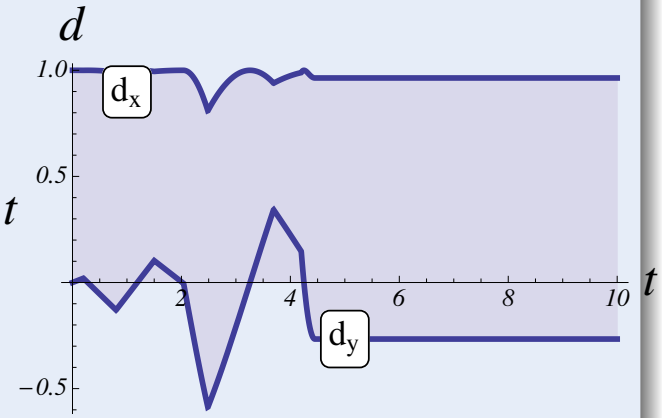
Design & verify controller for a robot avoiding obstacles

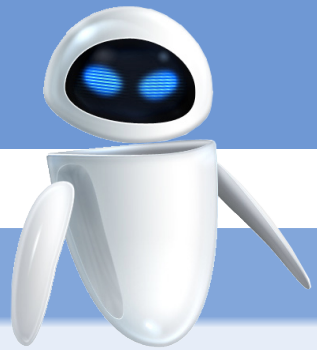
- Dynamic obstacles (other agents)
- Avoid collisions (define safety)







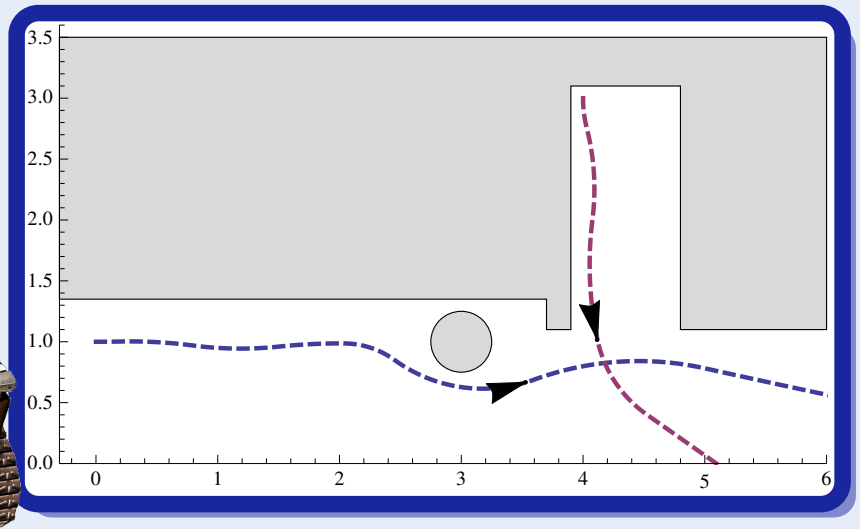


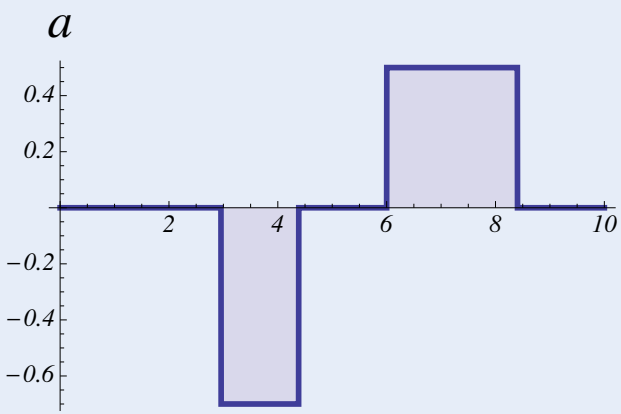


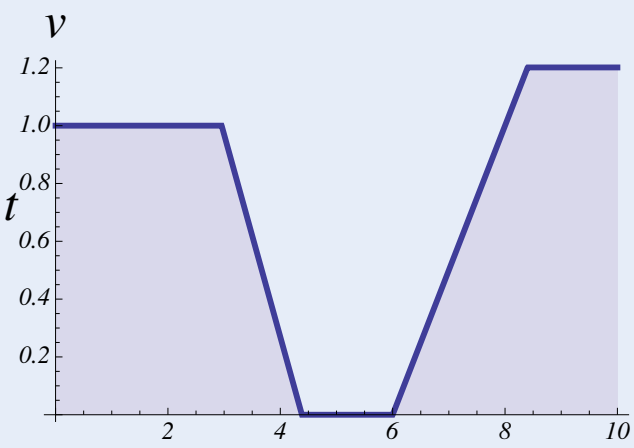
Challenge (Hybrid Systems)

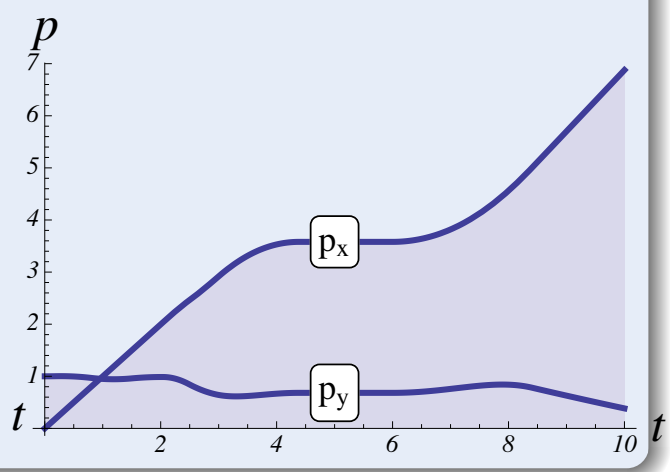
Design & verify controller for a robot avoiding obstacles

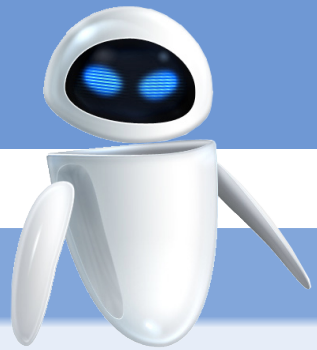
- Control robot (respect delays)
- Environment interaction (obstacles, agents, uncertainty)







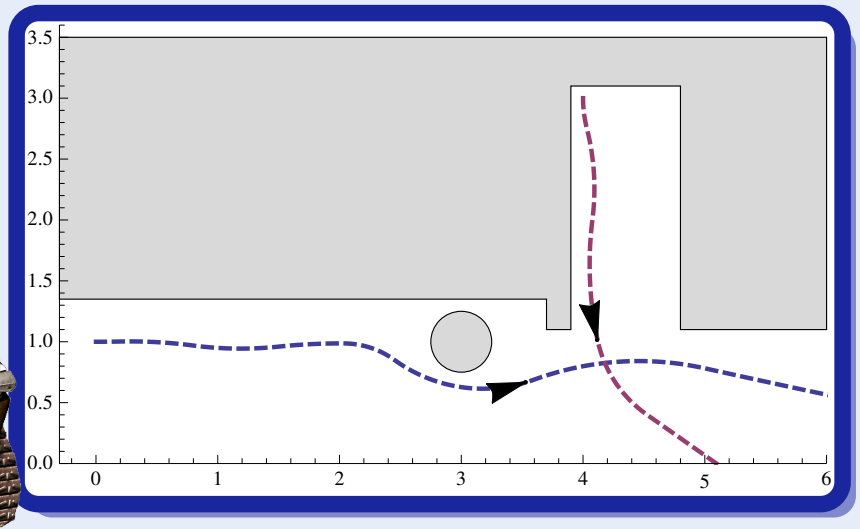


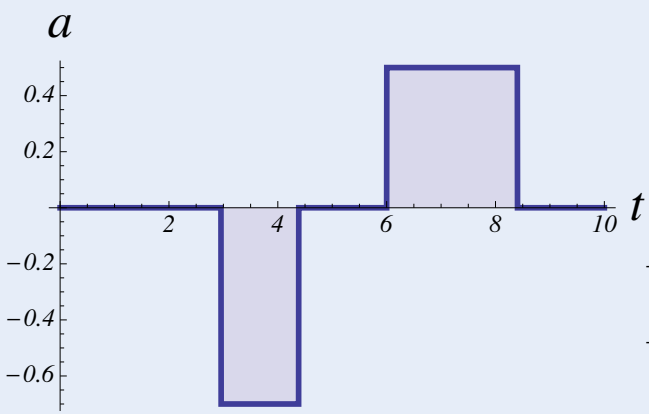


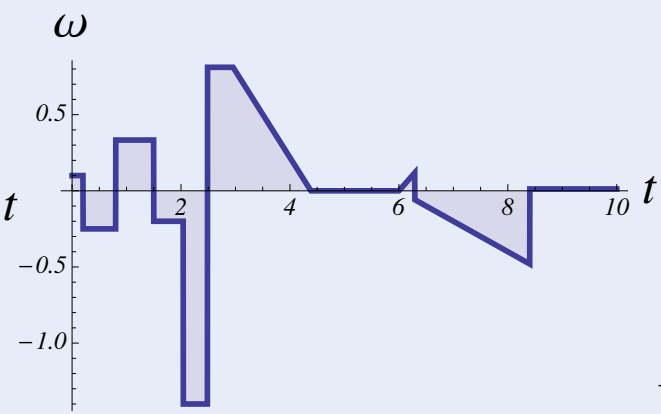
Challenge (Hybrid Systems)

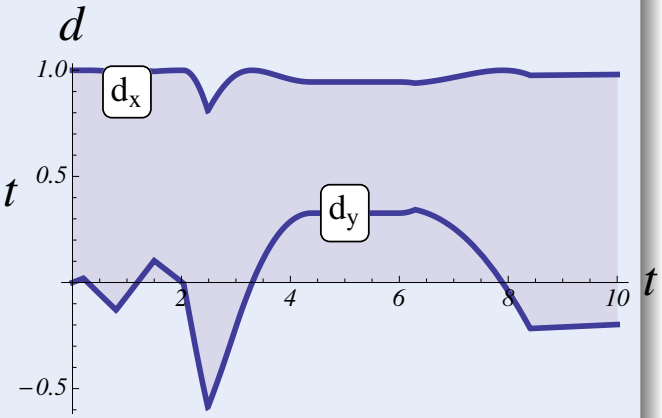
Design & verify controller for a robot avoiding obstacles

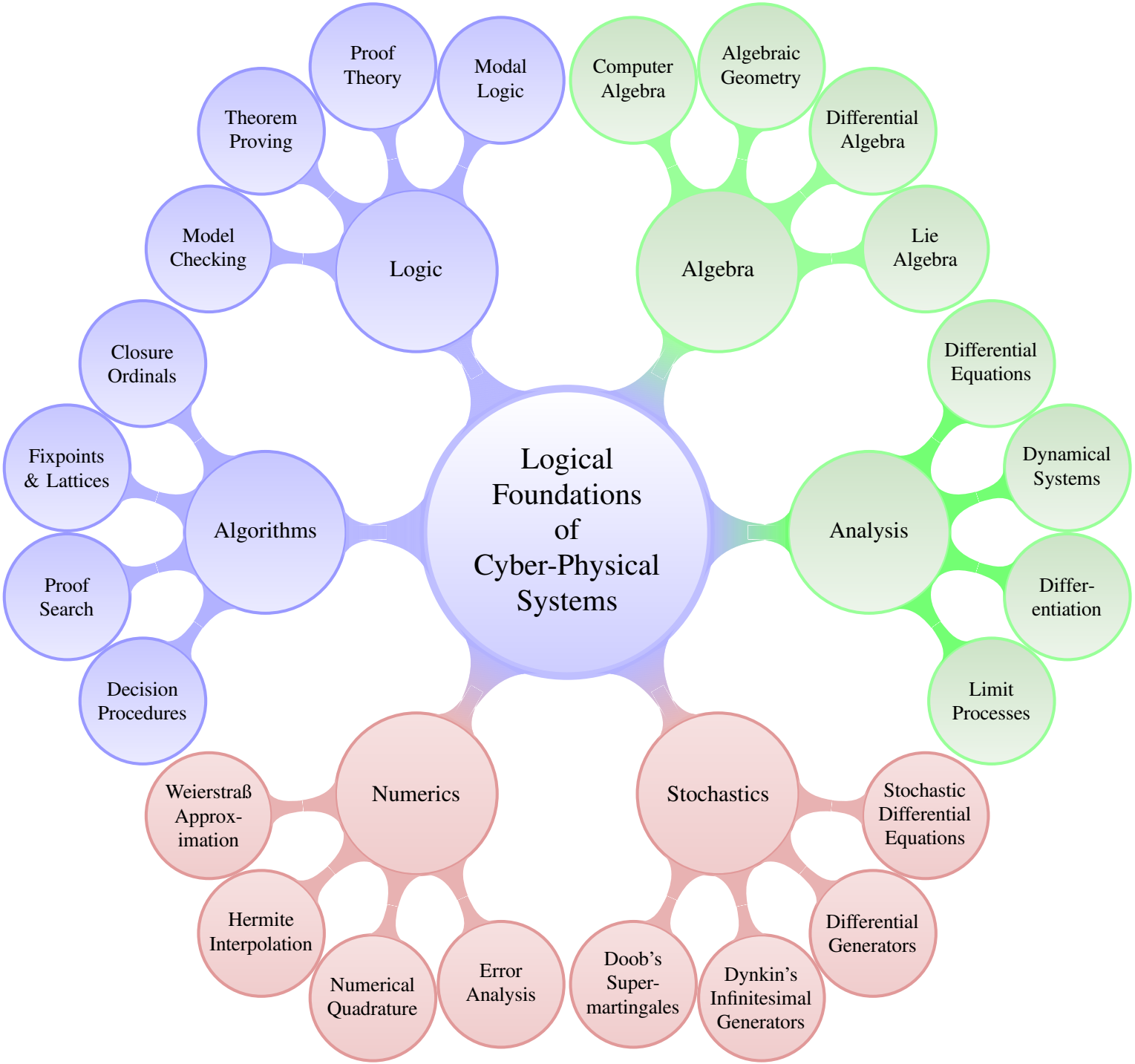
- Control robot (respect delays)
- Environment interaction (obstacles, agents, uncertainty)










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

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

About 15-424/14-624 Foundations of CPS

- 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 — ▸ Policy
- ≈20% Theory homework — Due at **beginning** of lecture
- ≈50% Labs — Due at 23:59
- Term paper — Due with Lab 6
- ≈10% Midterm
- ≈20% Final

Robot Labs

1. Robot on Rails
   a. Autobots, Roll Out
   b. Charging Station
2. Robot on Highways
   a. with event-driven 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. free motion
   b. with obstacle avoidance
5. Robot vs. Roguebot
   a. avoid collisions with moving obstacles
6. Robot in Star-lab

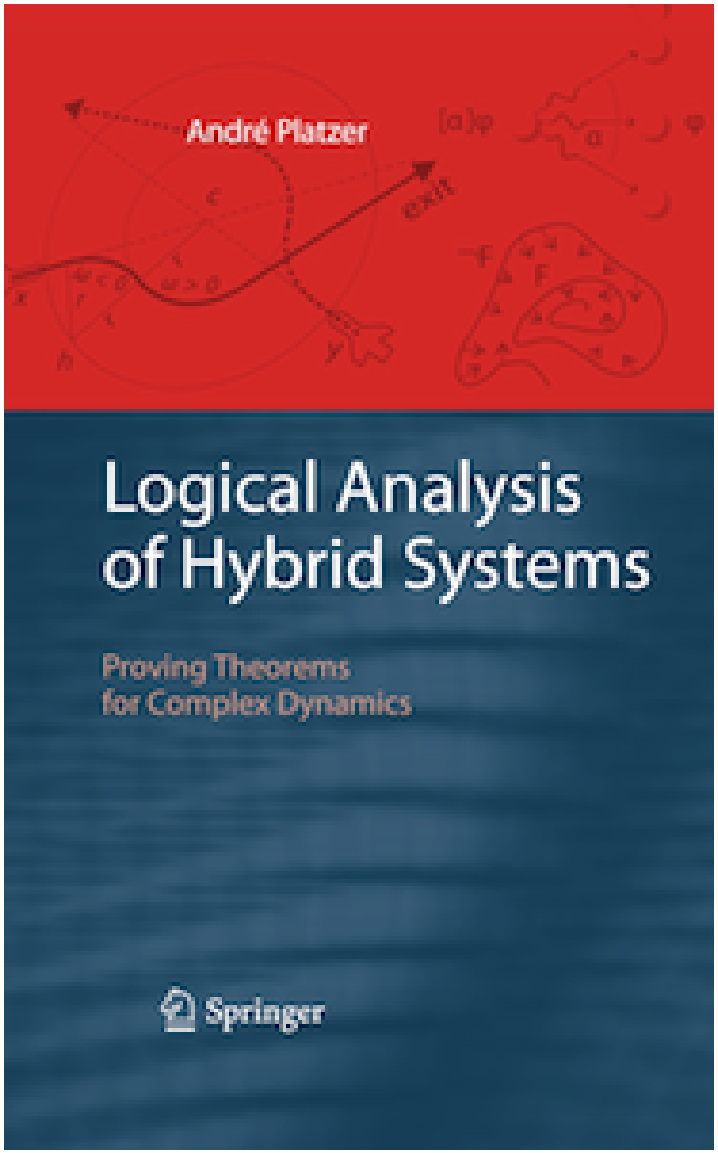
Resources

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
  http://symbolaris.com/course/fcps13.html
- Piazza
- Autolab
- KeYmaera
- Ask!

Textbook



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

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

CPS Design & CPS Contracts in Programs

HP Reveal in layers

Contracts Reason about CPS

```
@requires(v^2 <= 2*b*(m-x))
@requires(v >= 0 & A >= 0 & b > 0)
@ensures(x <= m)
  {
    if (v^2 <= 2*b*(m-x) - (A+b)*(A+2*v)) {
        a := A;
    } else {
        a := -b;
    }
    t := 0;
    {x'=v, v'=a, t'=1, v>=0 & t<=1}
  }*@invariant(v^2 <= 2*b*(m-x))
```

CPS Simulate for intuition

CT Design-by-invariant

CPS Contracts & CPS Logic

dL Logic for CPS

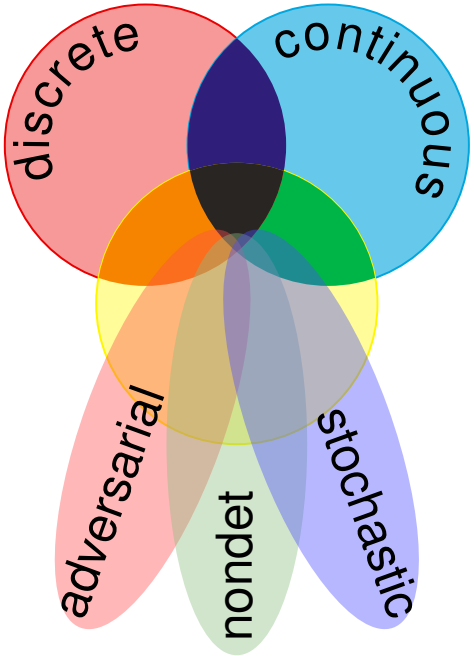
Contracts Reason in Logic

```
   v^2 <= 2*b*(m-x)
  & v >= 0 & A >= 0 & b > 0
->
   [{
      if (v^2 <= 2*b*(m-x) - (A+b)*(A+2*v)) {
          a := A;
      } else {
          a := -b;
      }
      t := 0;
      {x'=v, v'=a, t'=1, v>=0 & t<=1}
   }*@invariant(v^2 <= 2*b*(m-x))
   ] (x <= m)
```

CPS Analyze for precision

CT Proof-by-invariant

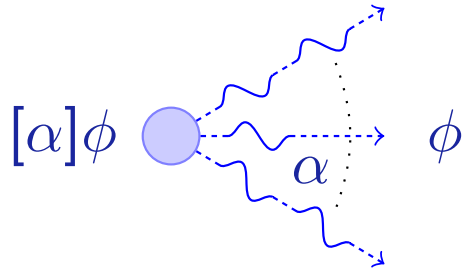
Family of Differential Dynamic Logics

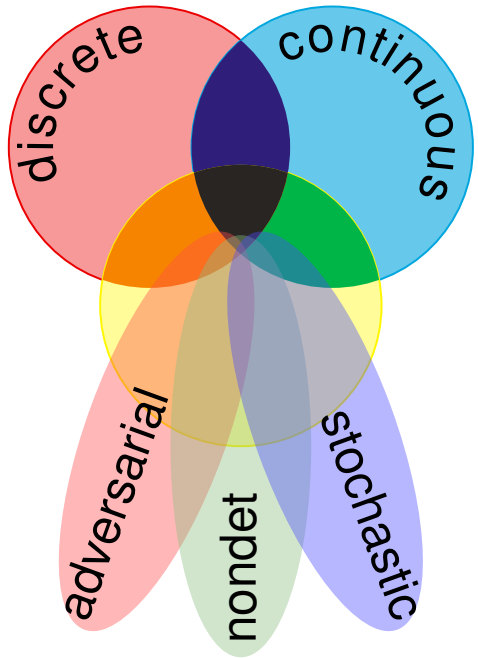


Family of Differential Dynamic Logics

differential dynamic logic

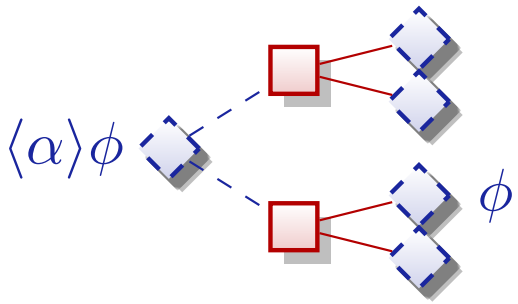
$$\mathsf{d}\mathcal{L} = \mathsf{DL} + \mathsf{HP}$$





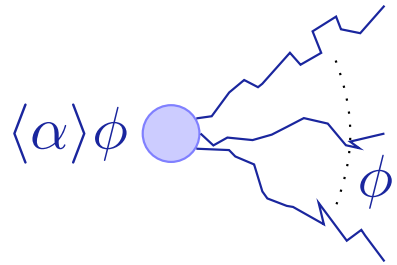
differential game logic

$$\mathsf{dG}\mathcal{L} = \mathsf{GL} + \mathsf{HG}$$



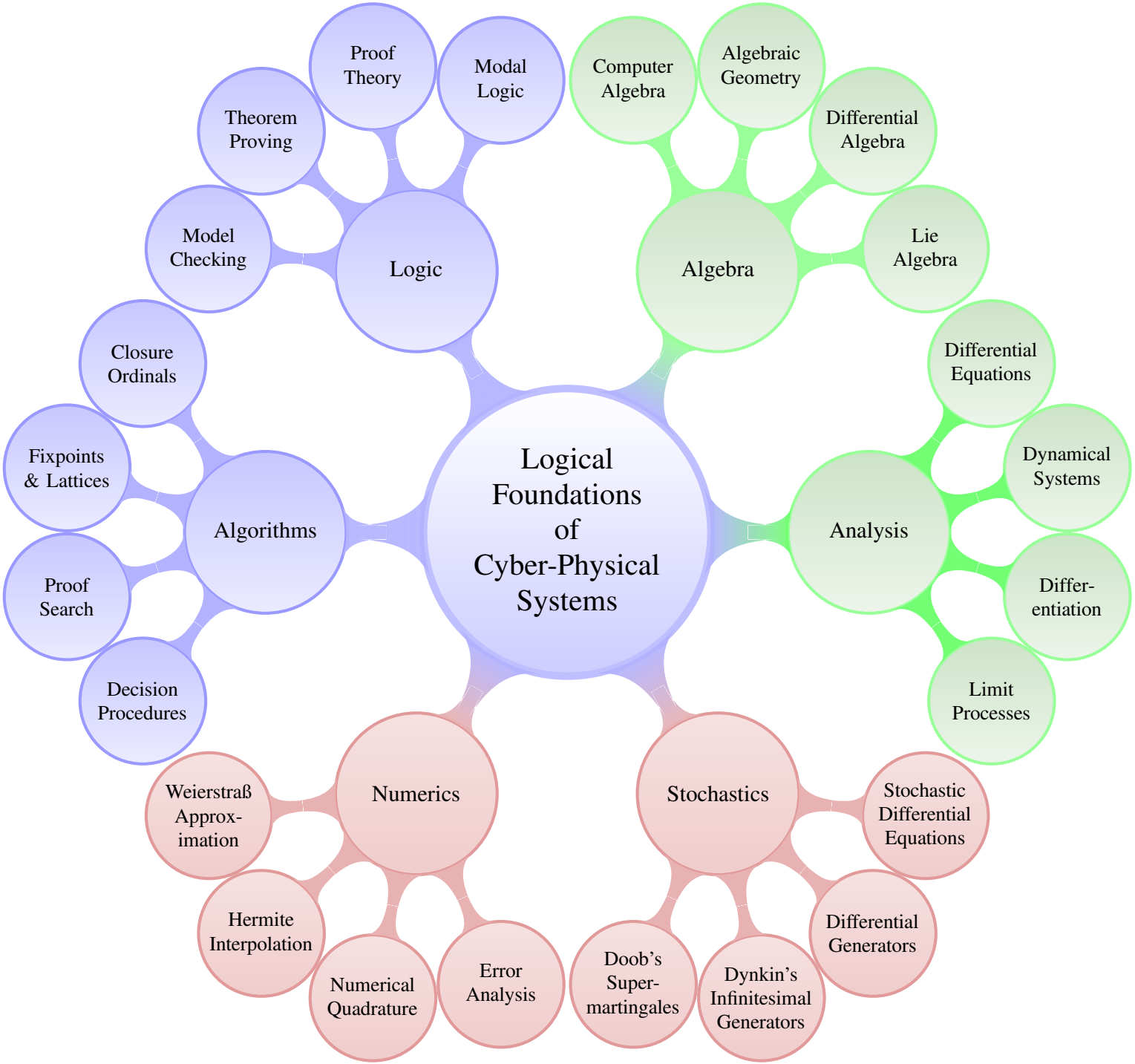
stochastic differential DL

$$\mathsf{Sd}\mathcal{L} = \mathsf{DL} + \mathsf{SHP}$$



quantified differential DL

$$\mathsf{Qd}\mathcal{L} = \mathsf{FOL} + \mathsf{DL} + \mathsf{QHP}$$


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

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.
In *LICS*, pages 13–24. IEEE, 2012.


André Platzer.
Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics.
Springer, Heidelberg, 2010.


André Platzer.
Differential dynamic logic for hybrid systems.
J. Autom. Reas., 41(2):143–189, 2008.


André Platzer.
Differential dynamic logic for verifying parametric hybrid systems.
In Nicola Olivetti, editor, *TABLEAUX*, volume 4548 of *LNCS*, pages 216–232. Springer, 2007.