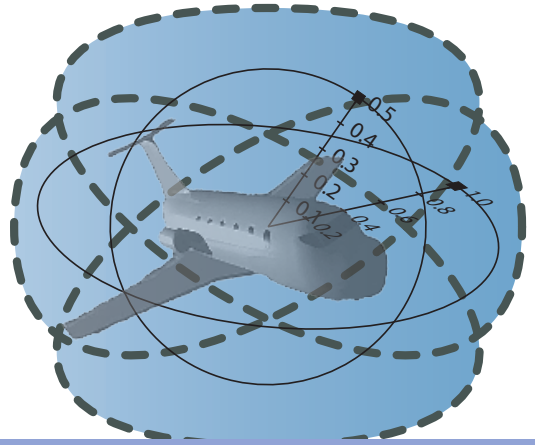
15-424/15-624: Foundations of Cyber-Physical Systems

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



Outline

Outline

Cyber-Physical Systems Analysis: Aircraft Example

Which control decisions are safe for aircraft collision avoidance?

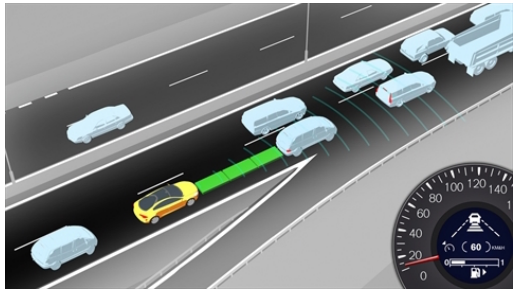
CPSs Promise Transformative Impact!

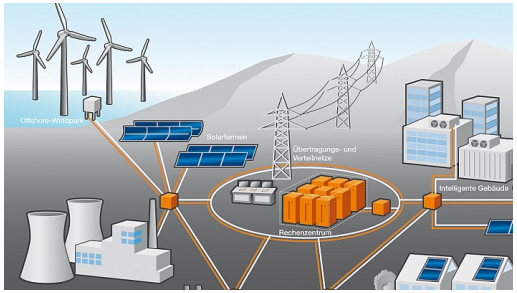
Prospects: Safe & Efficient

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?

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

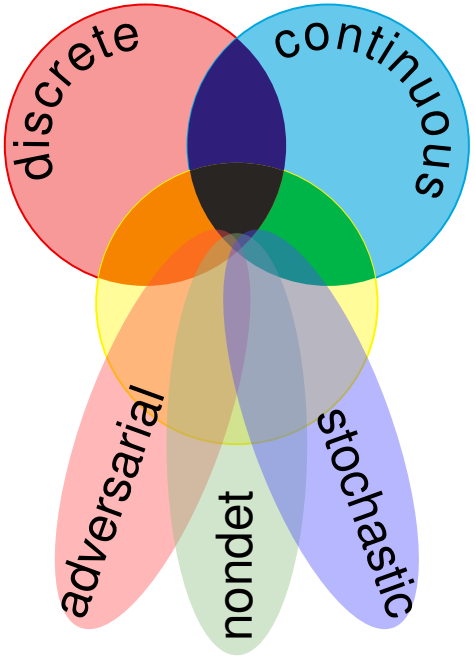
Cyber-physical Systems

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.

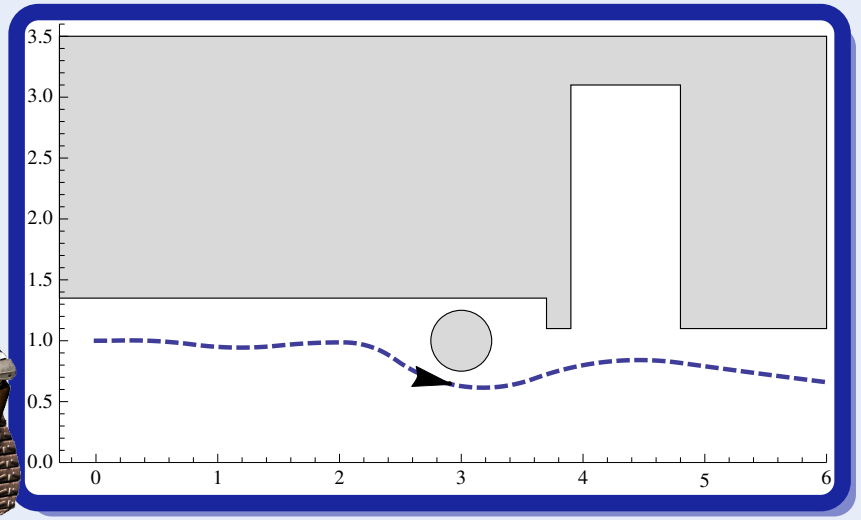
Tame Parts

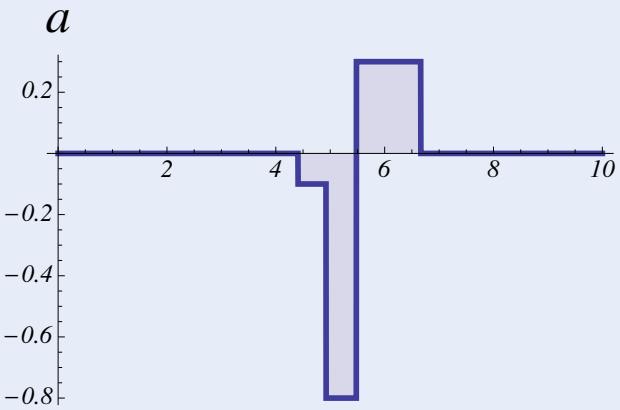
Exploiting compositionality tames CPS complexity.

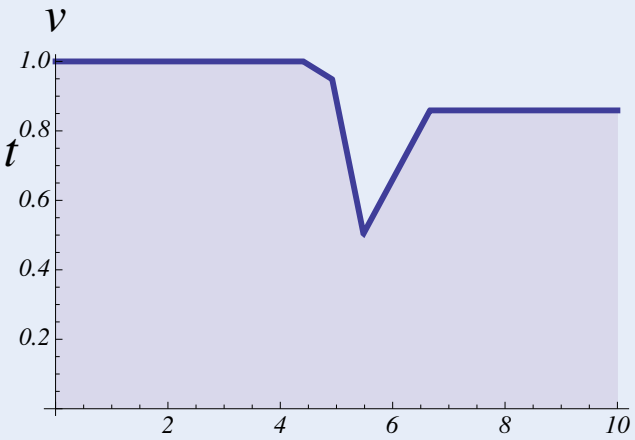
Challenge (CPS)

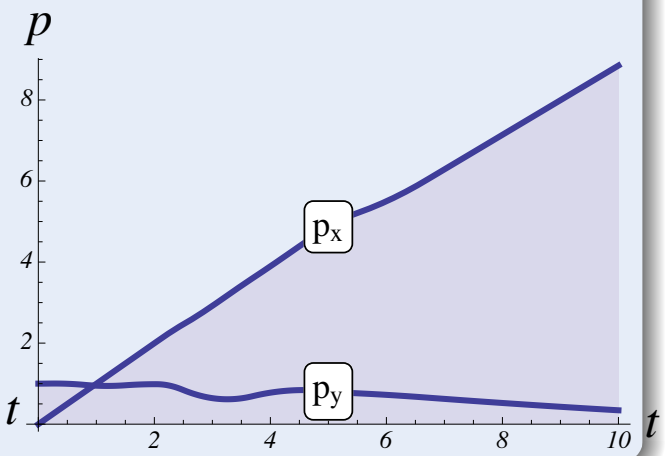
Fixed rule describing state evolution with both

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





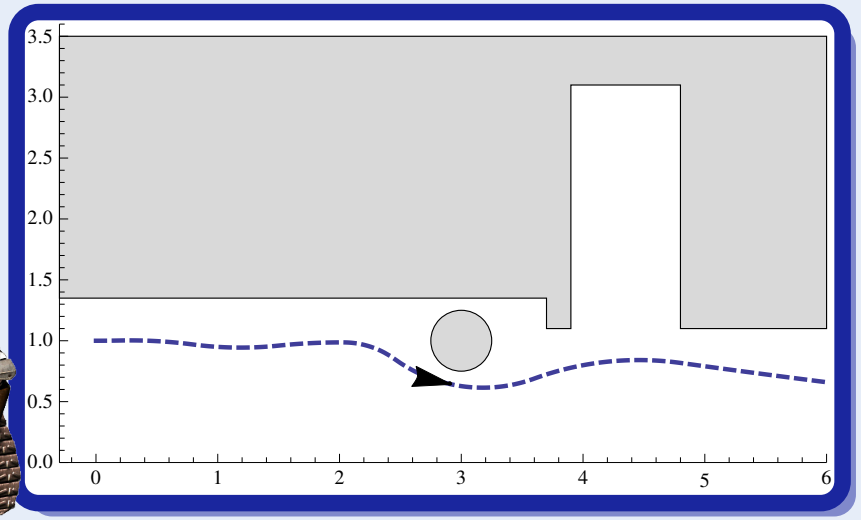


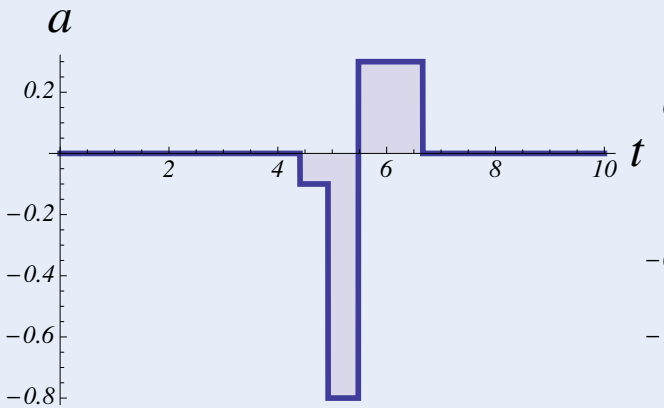


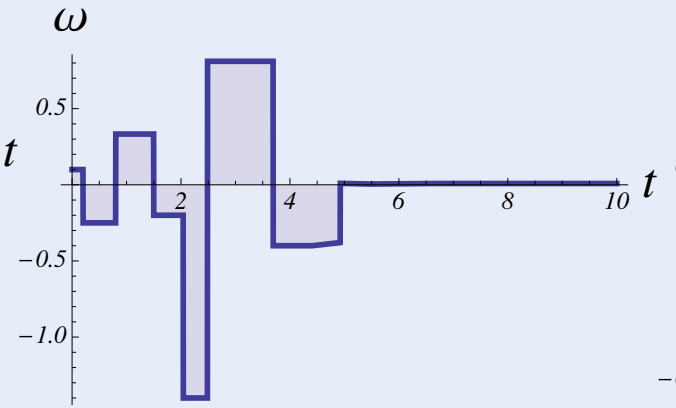
Challenge (CPS)

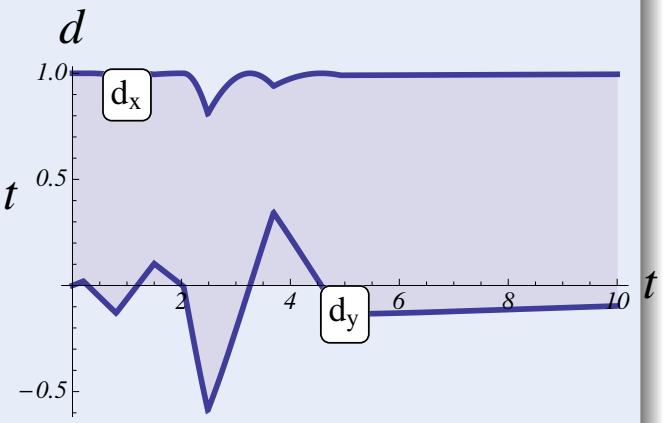
Fixed rule describing state evolution with both

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









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)

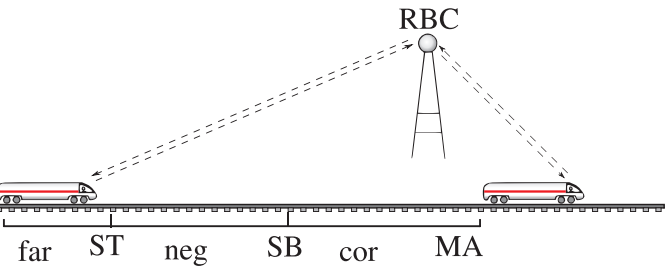
(Distributed network of) computerized control for physical system
Computation, communication and control for physics

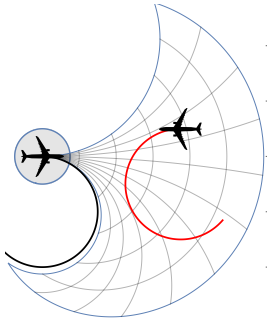
What CPS are around us?

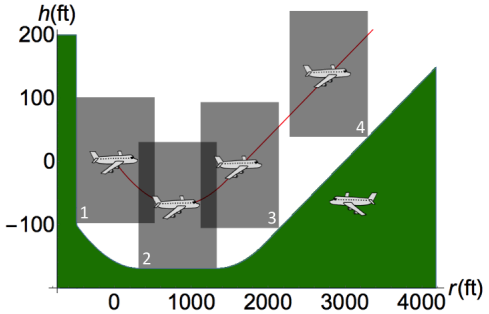
What CPS will be around us in the future?

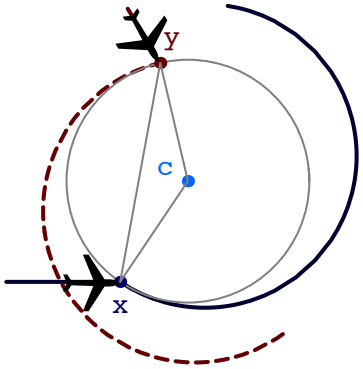
Which CPS do we trust with our lives?

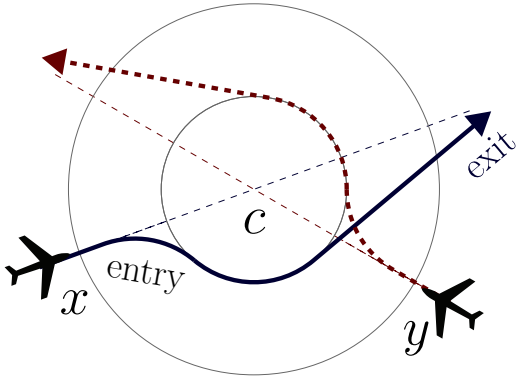
Verified CPS Applications

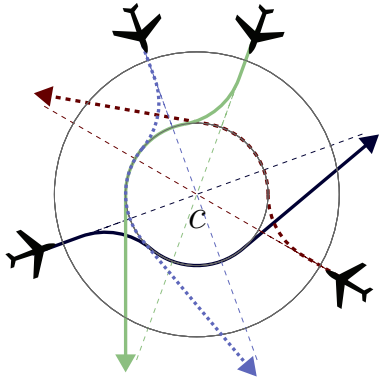


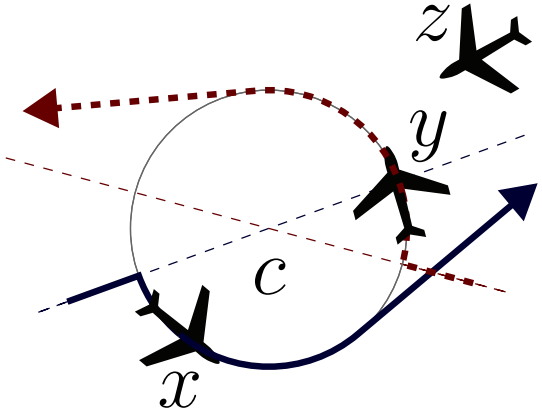


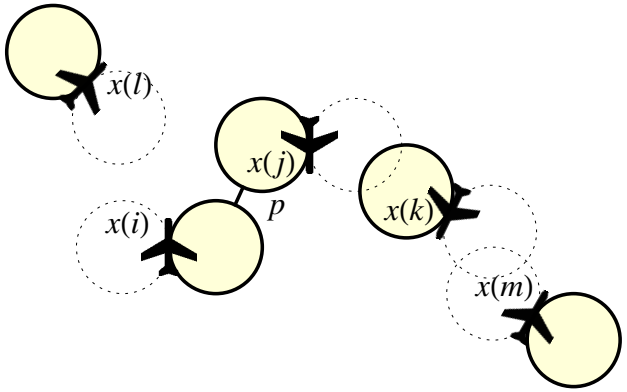


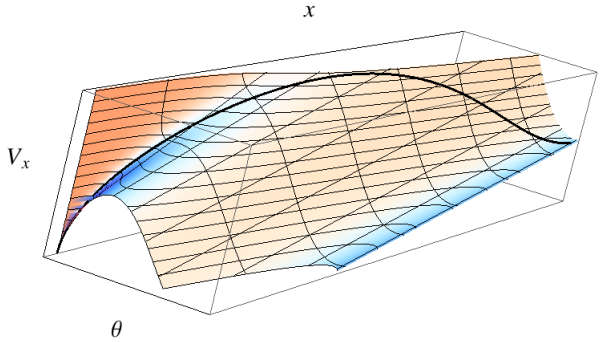






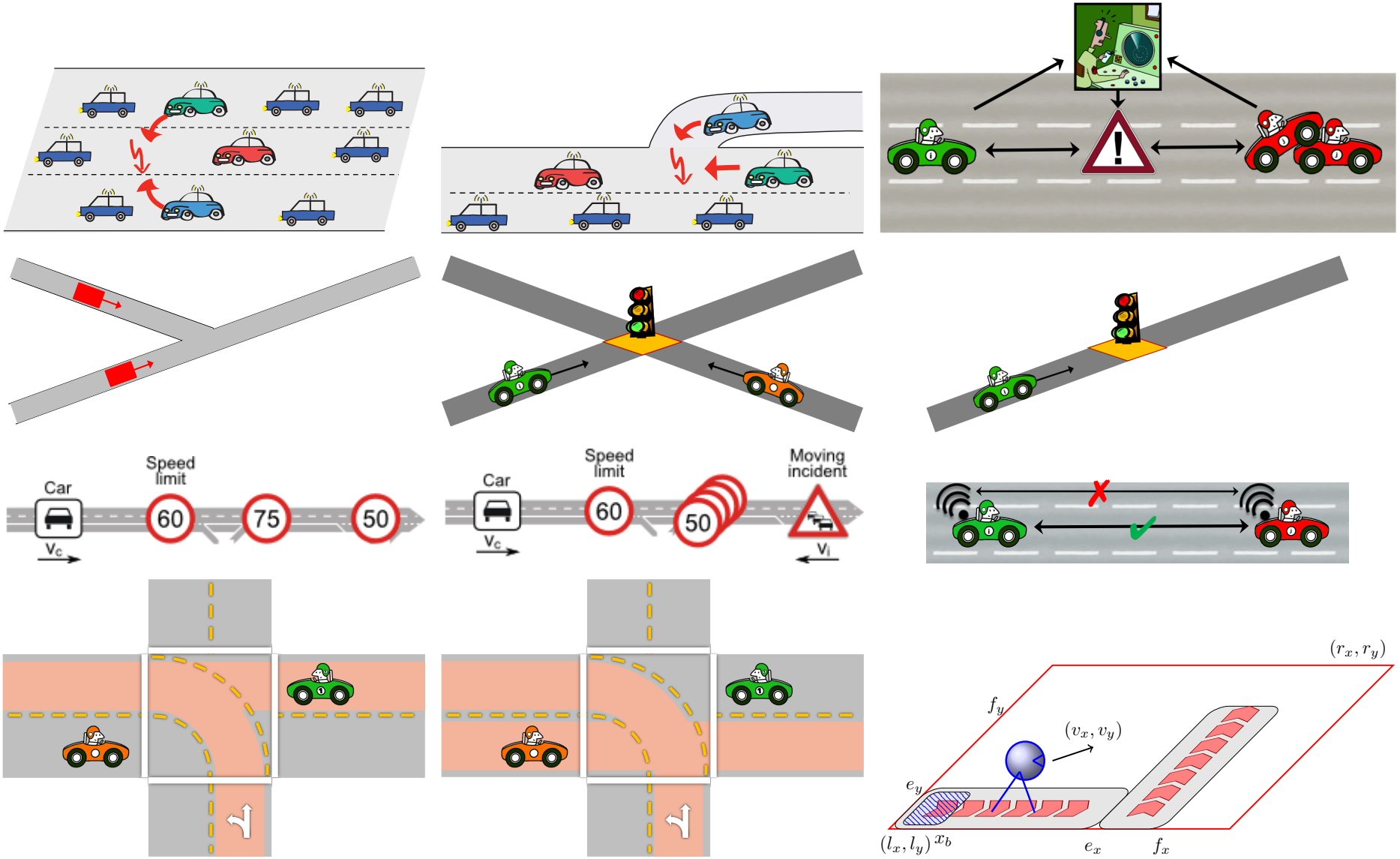






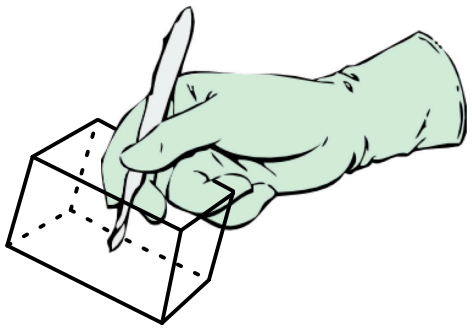
ICFEM'09, JAIS'14, TACAS'15, CAV'08, FM'09, HSCC'11, HSCC'13, TACAS'14

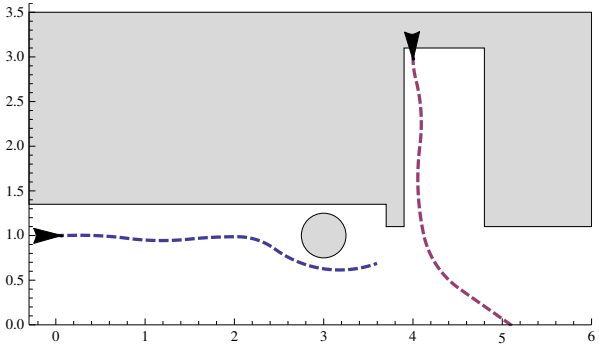
Verified CPS Applications

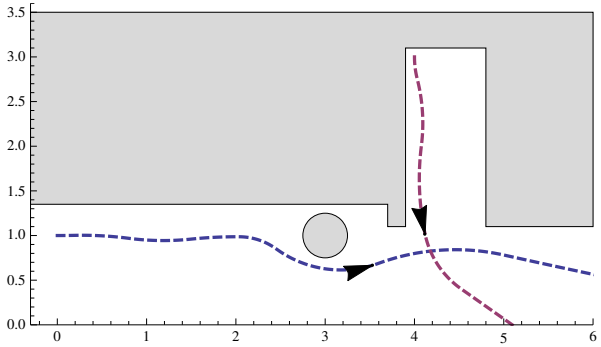


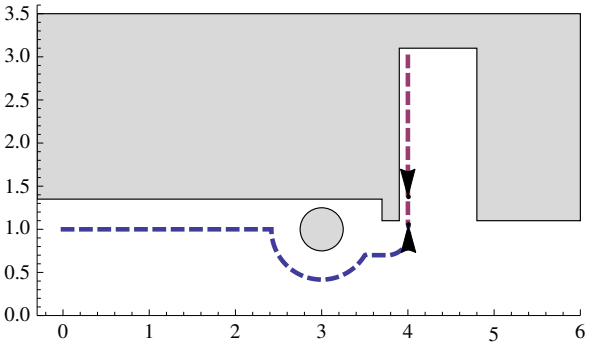
FM'11,LMCS'12,ICCPS'12,ITSC'11,ITSC'13,IJCAR'12

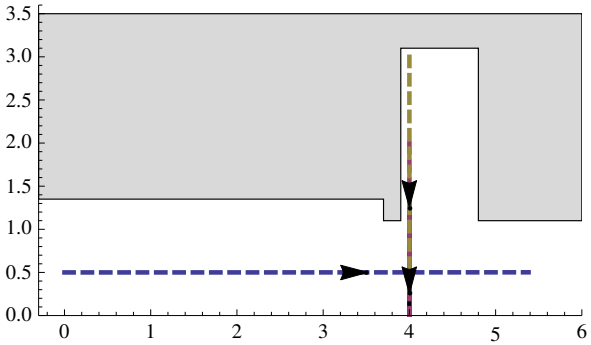
Verified CPS Applications

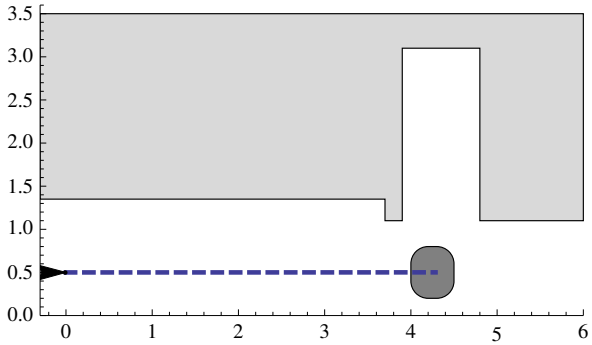


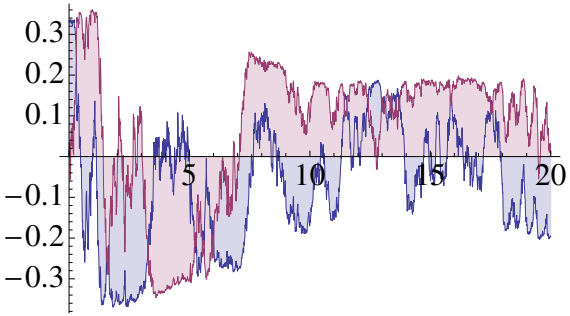


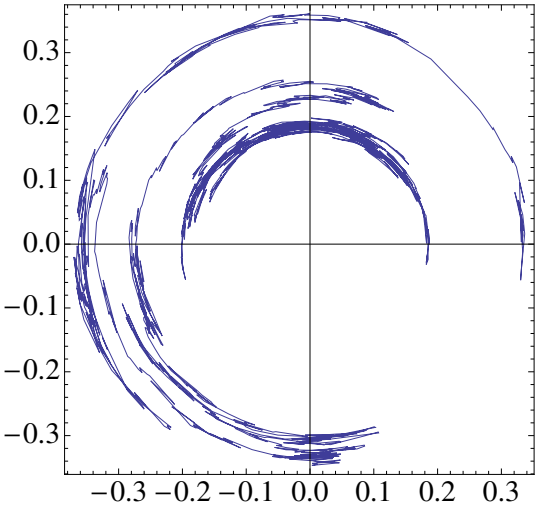


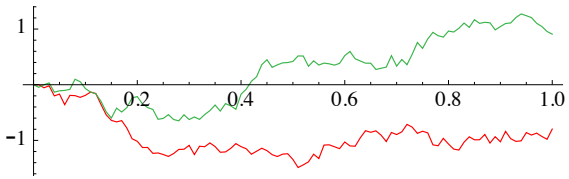






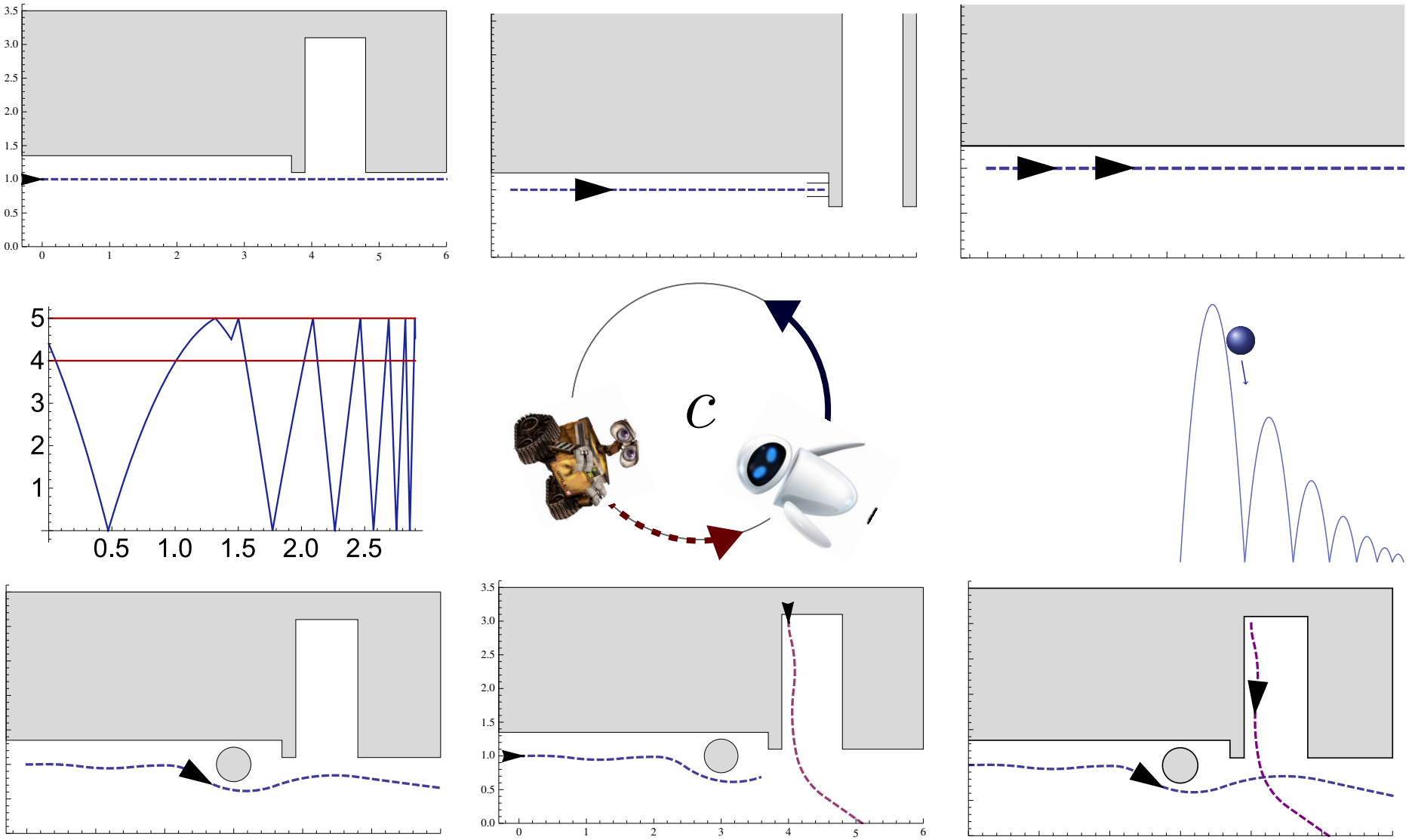






HSCC'13,RSS'13,CADE'12

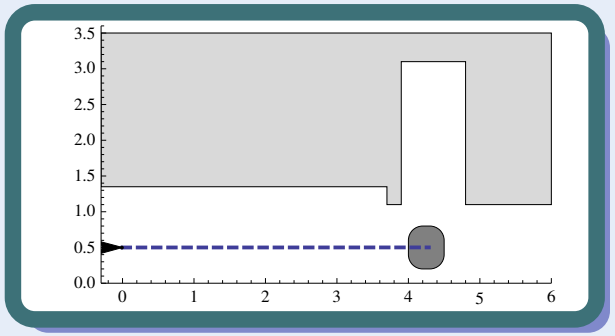
Verified CPS Applications By Undergrads

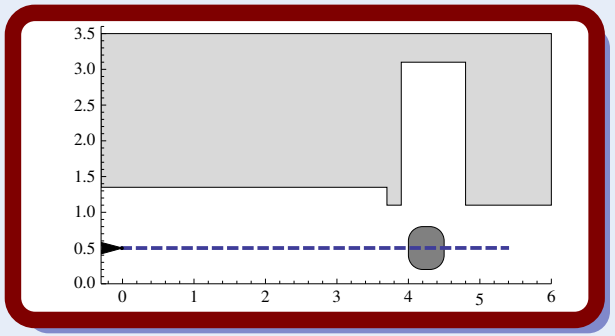


15-424/624 *Foundations of Cyber-Physical Systems* students

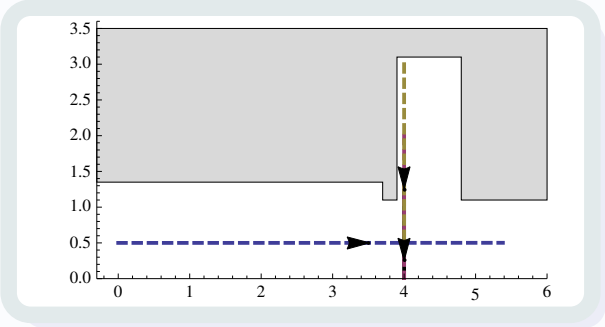
FCPS Labs

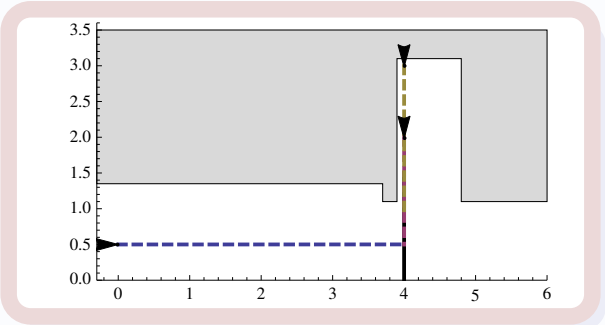
1: Charging Station



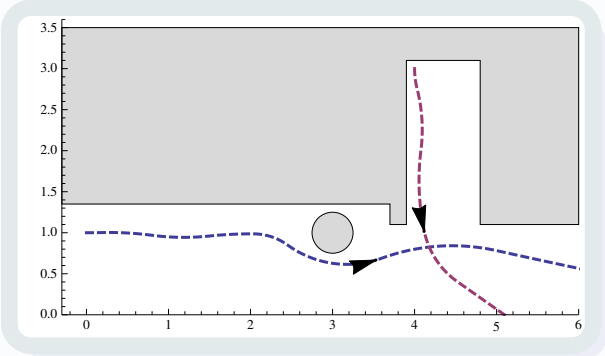


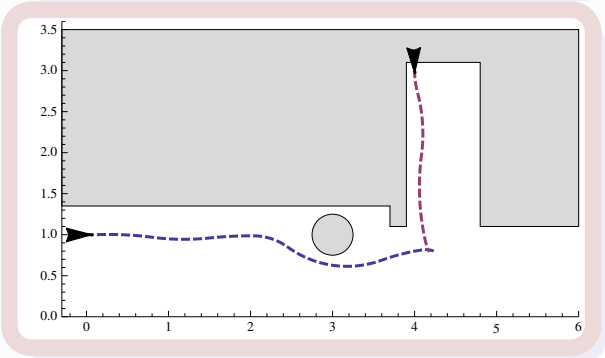
2: Follow the Leader





4: Obstacles

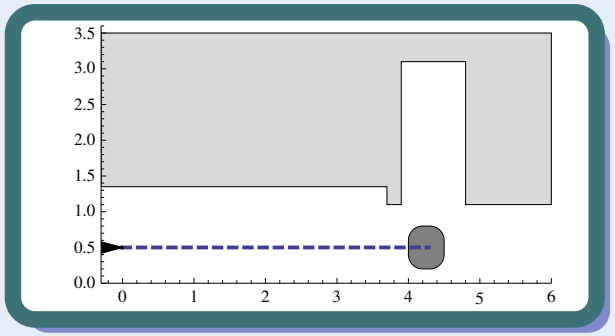


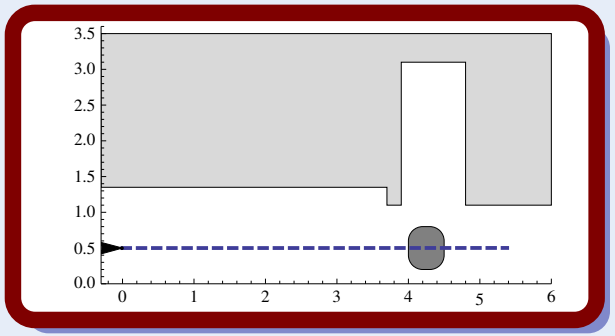


- ✓ Design, model
- ✓ Verify with KeYmaera X

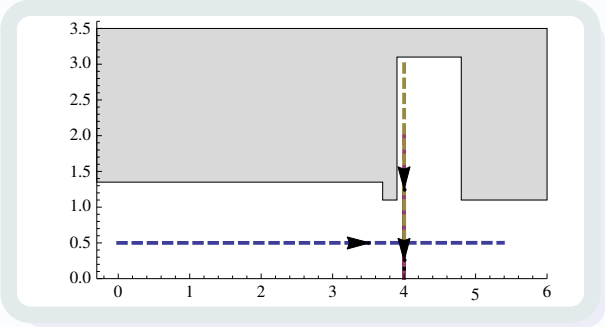
FCPS Labs

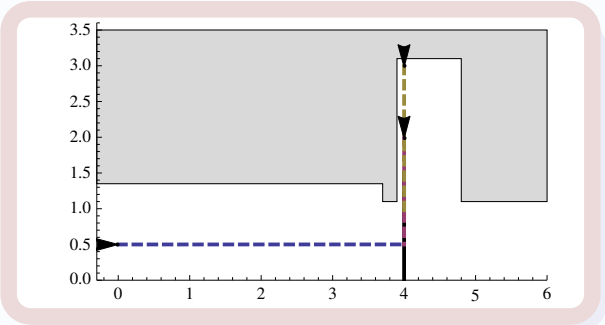
1: Charging Station



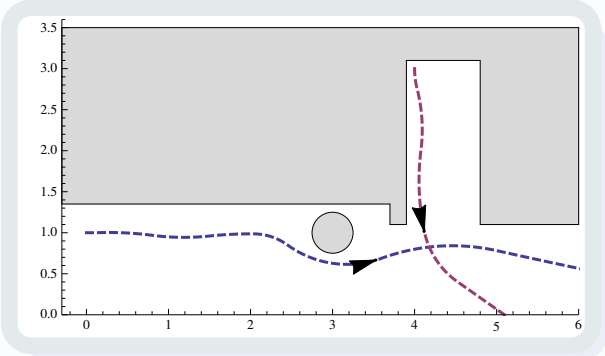


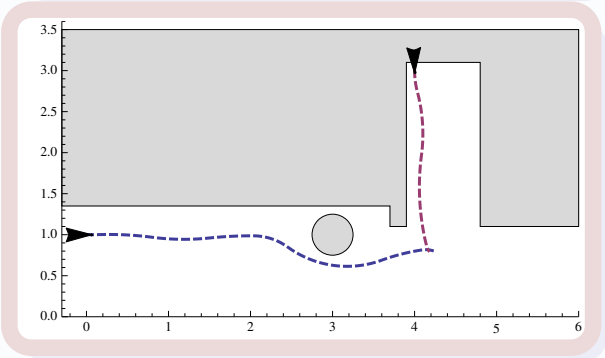
2: Follow the Leader





4: Obstacles

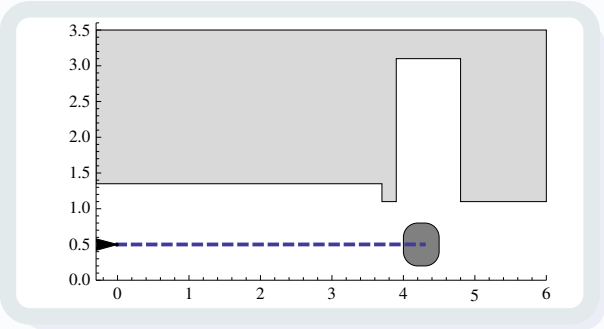


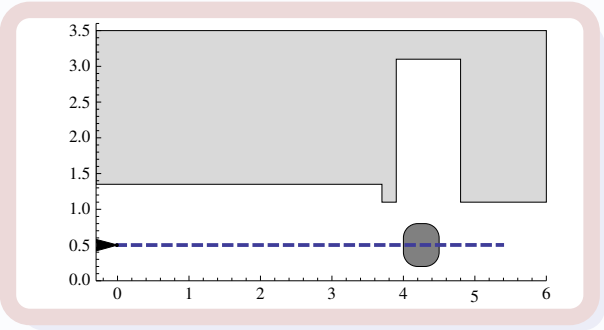


- ✓ Design, model
- ✓ Verify with KeYmaera X

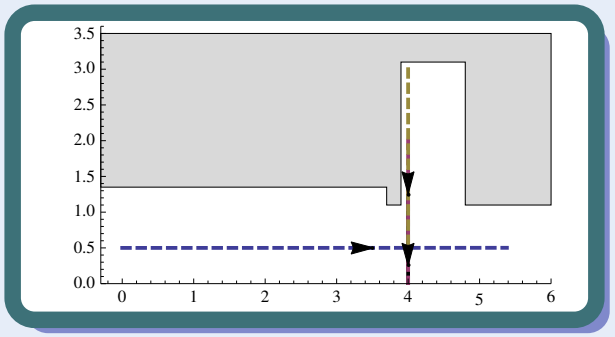
FCPS Labs

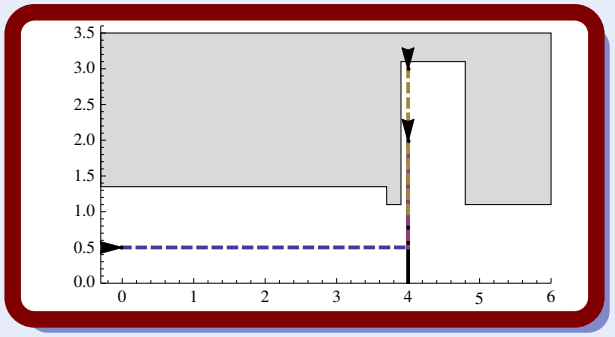
1: Charging Station



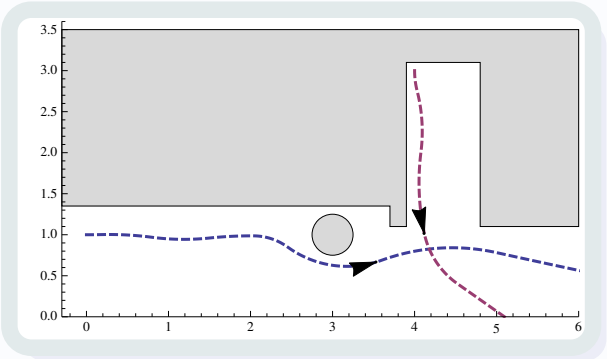


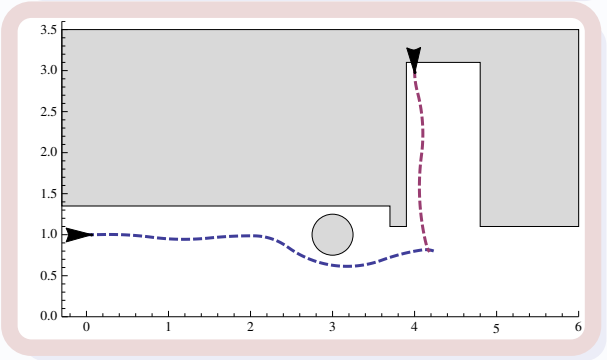
2: Follow the Leader





4: Obstacles

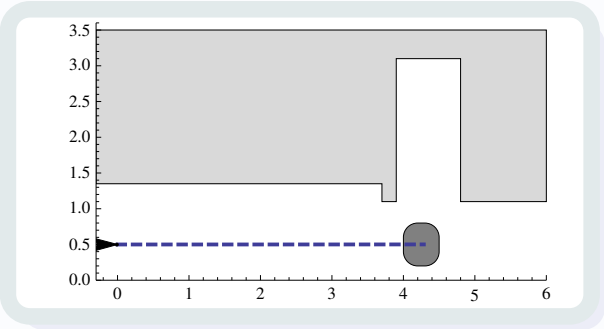


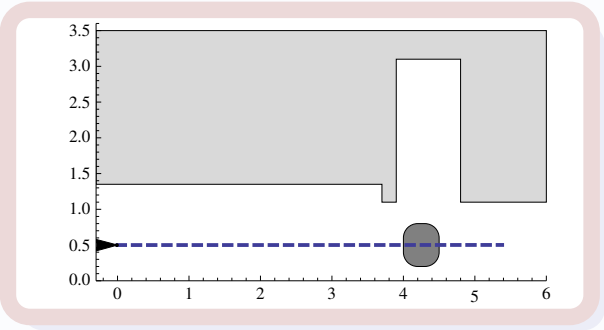


- ✓ Design, model
- ✓ Verify with KeYmaera X

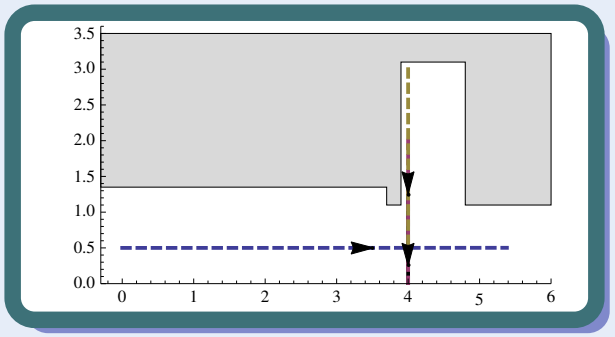
FCPS Labs

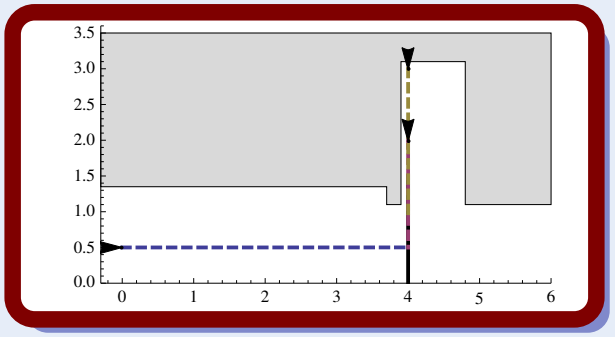
1: Charging Station



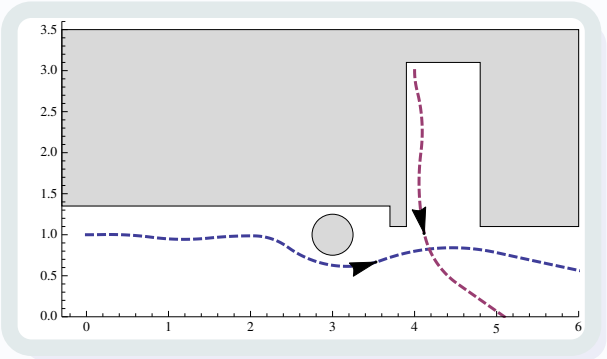


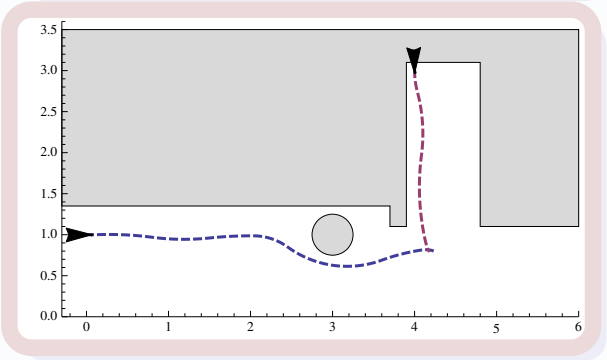
2: Follow the Leader





4: Obstacles

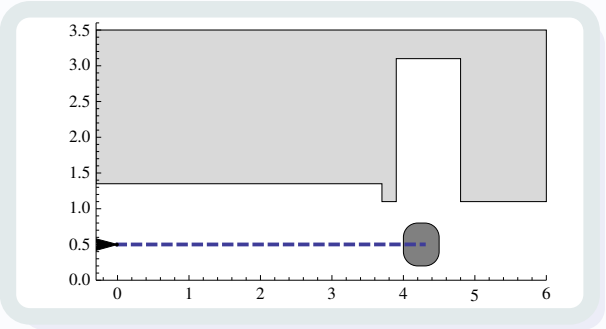


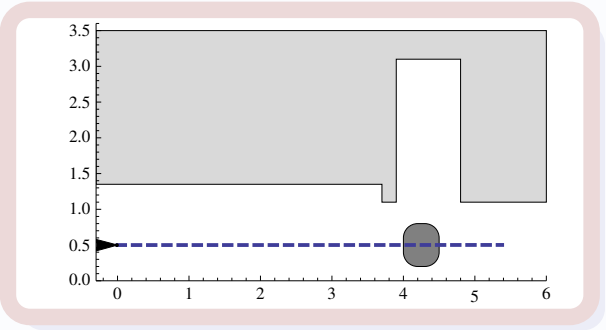


- ✓ Design, model
- ✓ Verify with KeYmaera X

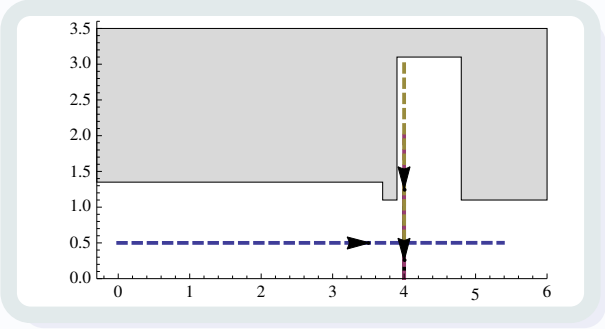
FCPS Labs

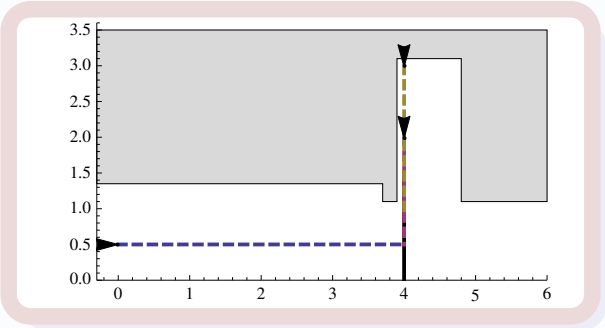
1: Charging Station



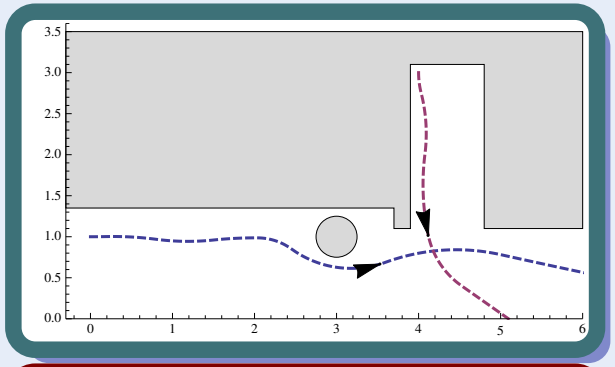


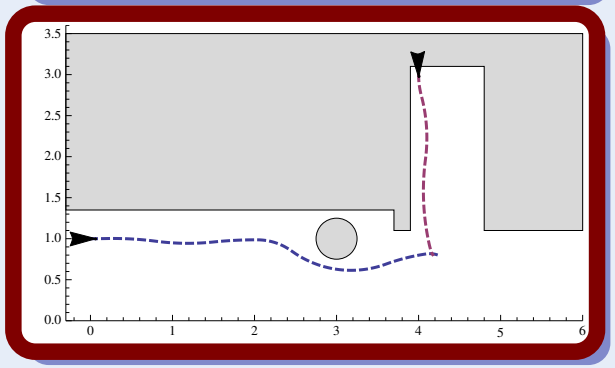
2: Follow the Leader





4: Obstacles

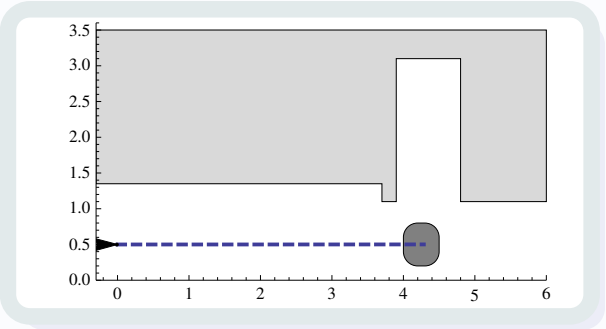


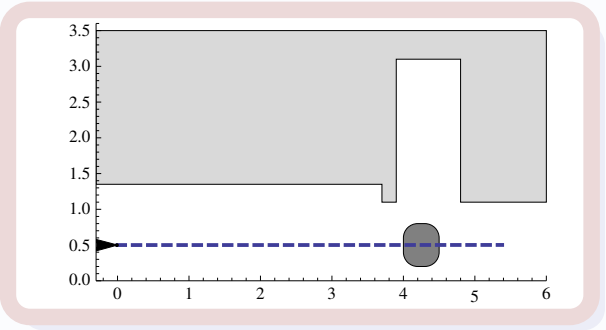


- ✓ Design, model
- ✓ Verify with KeYmaera X

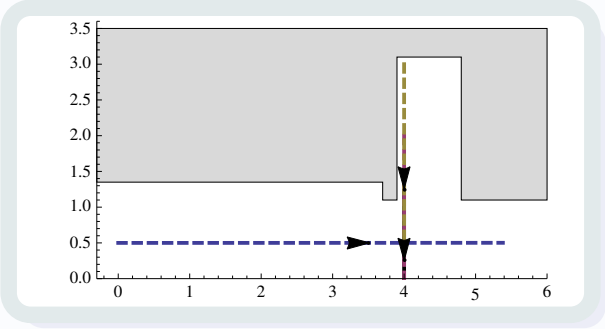
FCPS Labs

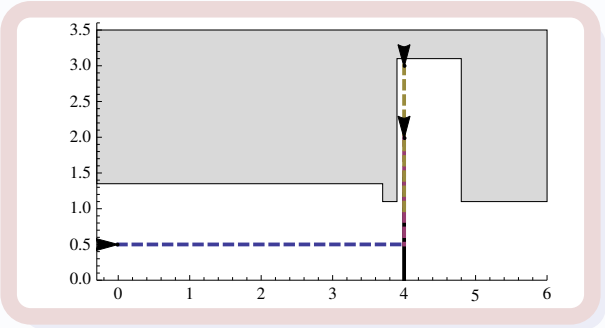
1: Charging Station



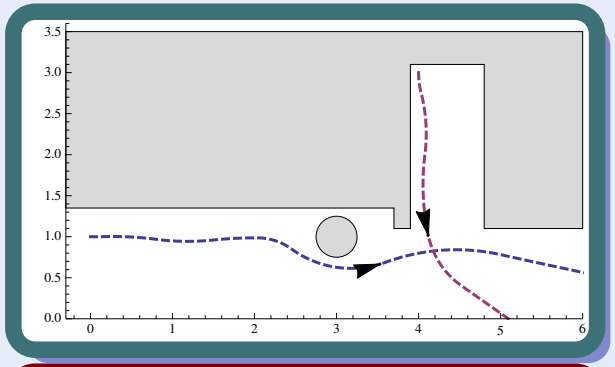


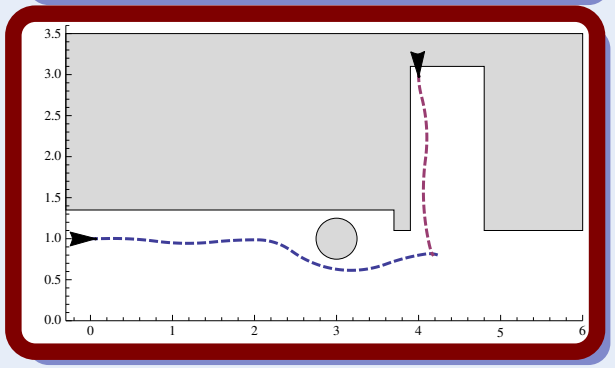
2: Follow the Leader





4: Obstacles

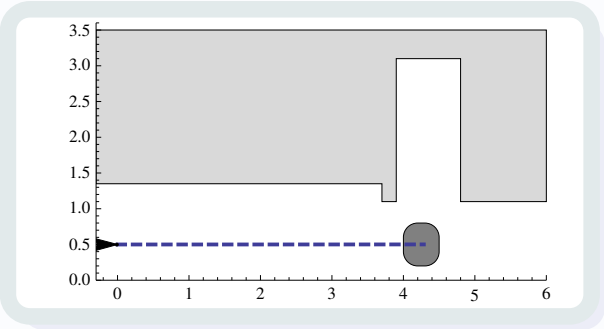


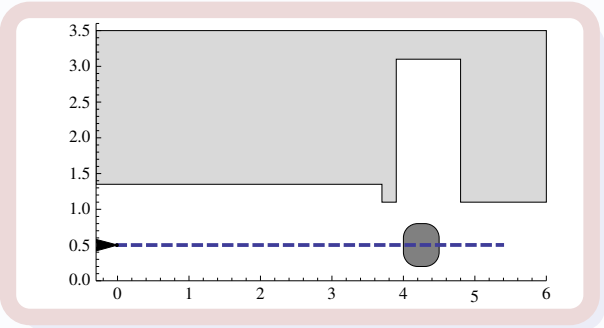


- ✓ Design, model
- ✓ Verify with KeYmaera X

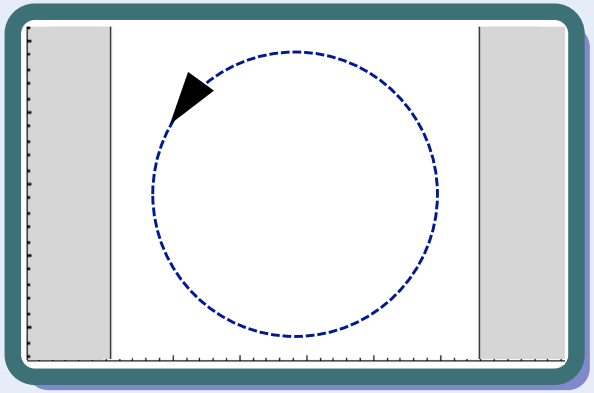
FCPS Labs

1: Charging Station

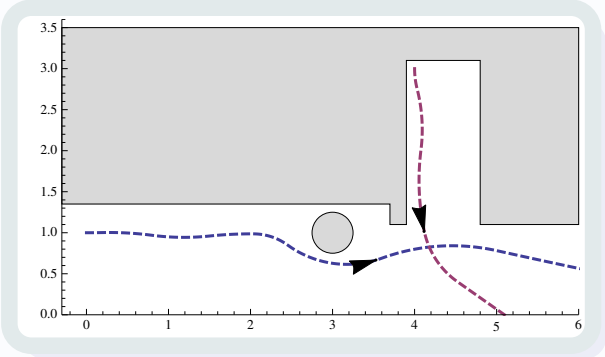


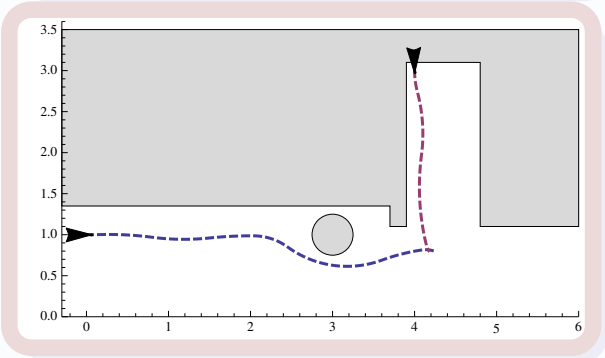


3: Racetrack



4: Obstacles



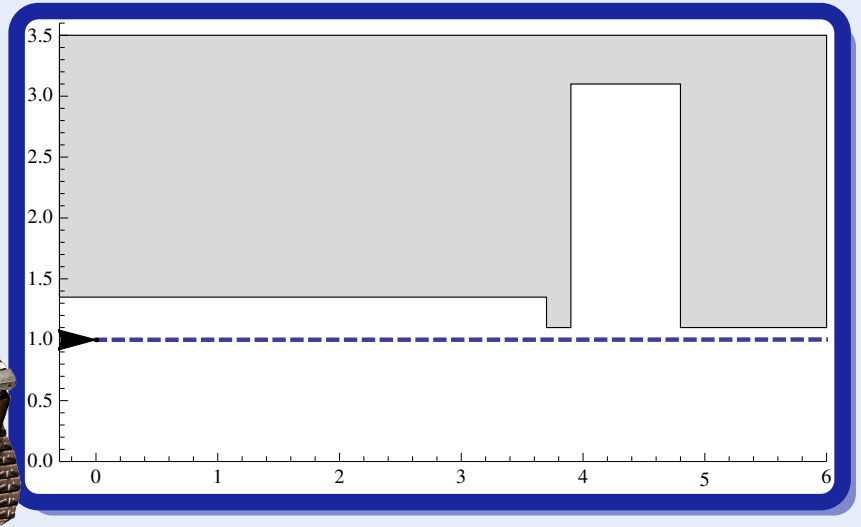


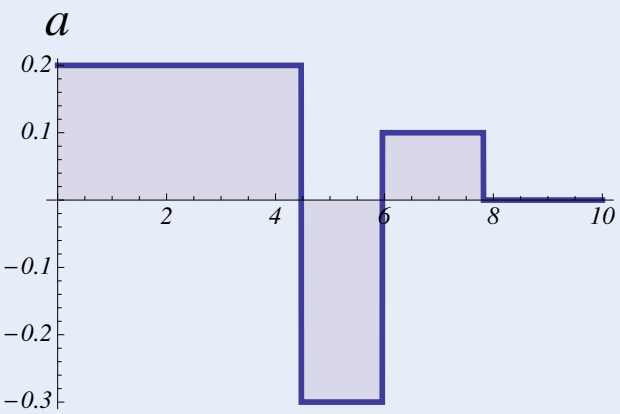
- ✓ Design, model
- ✓ Verify with KeYmaera X

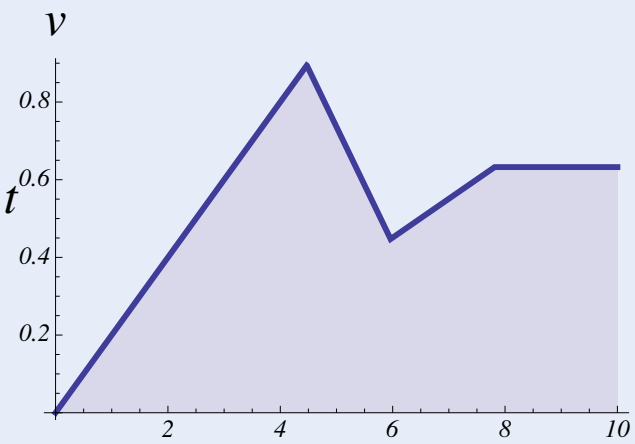
Challenge (Hybrid Systems)

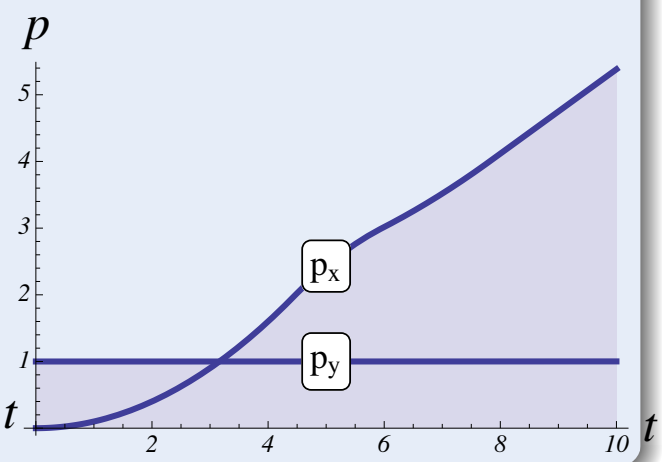
Design & verify controller for a robot avoiding obstacles

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





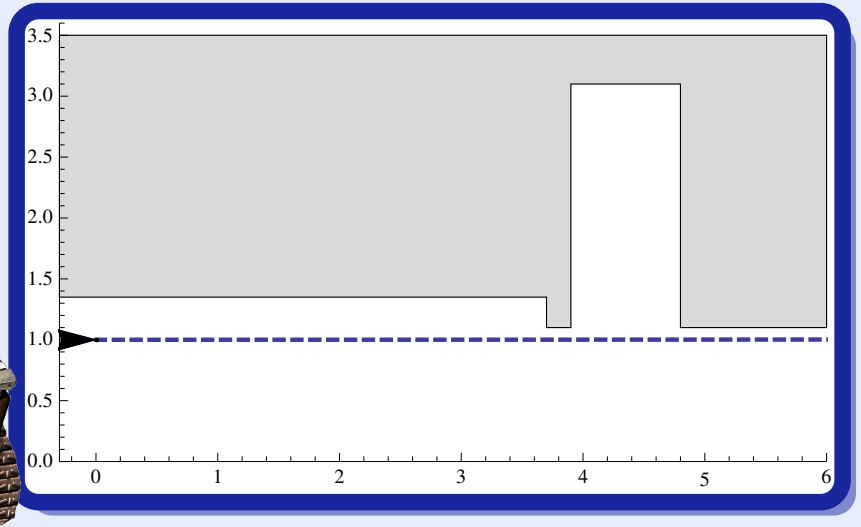


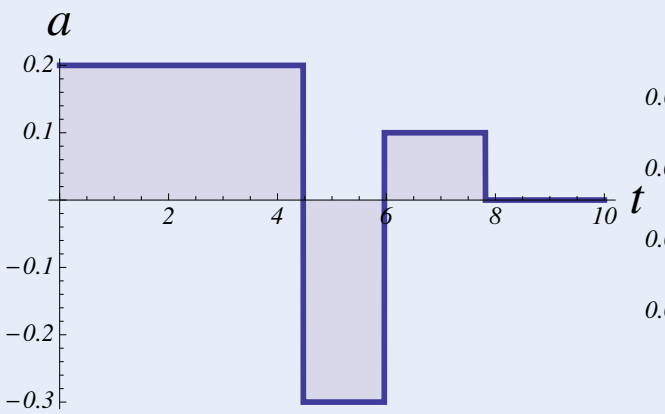


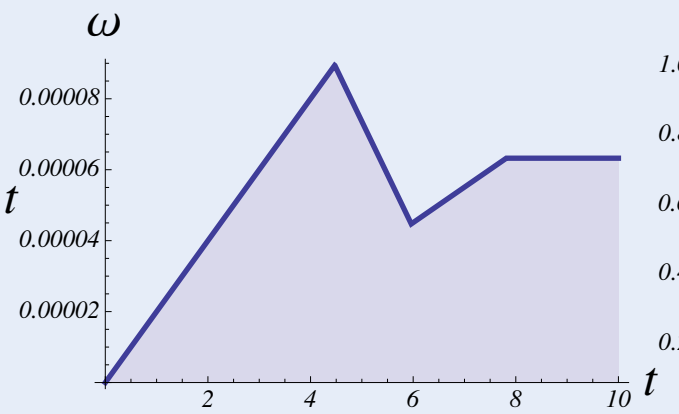
Challenge (Hybrid Systems)

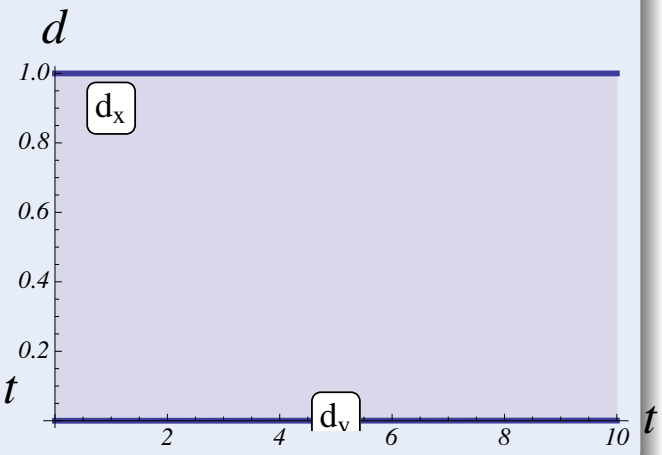
Design & verify controller for a robot avoiding obstacles

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





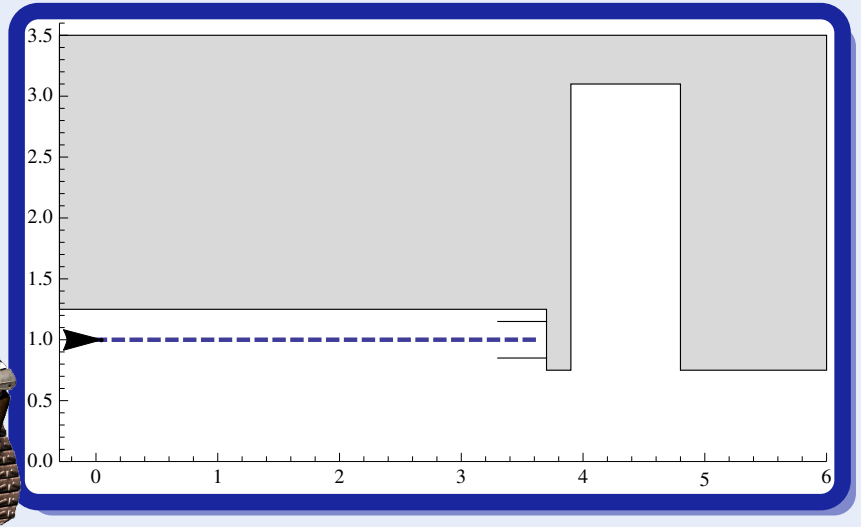


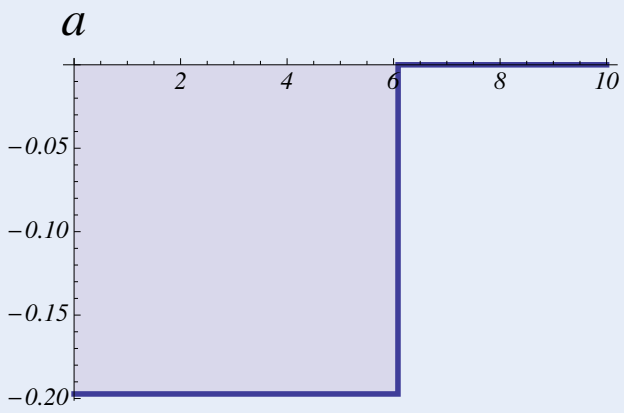


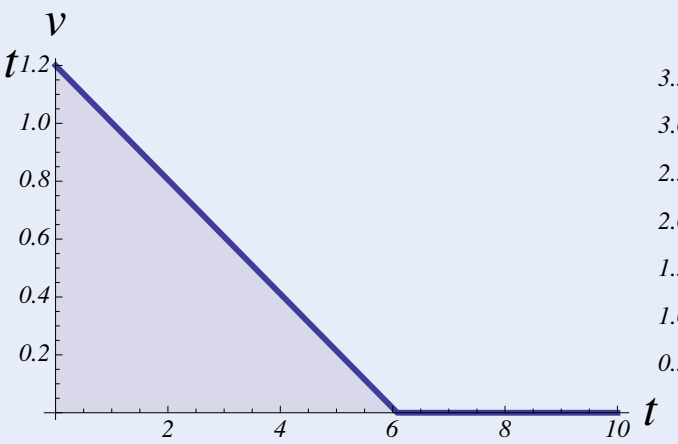
Challenge (Hybrid Systems)

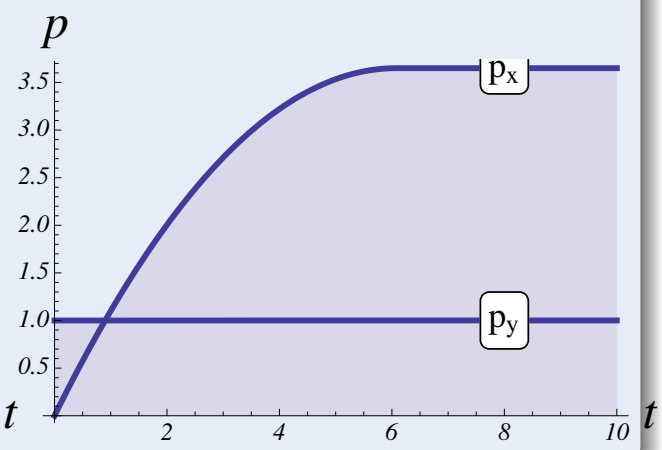
Design & verify controller for a robot avoiding obstacles

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





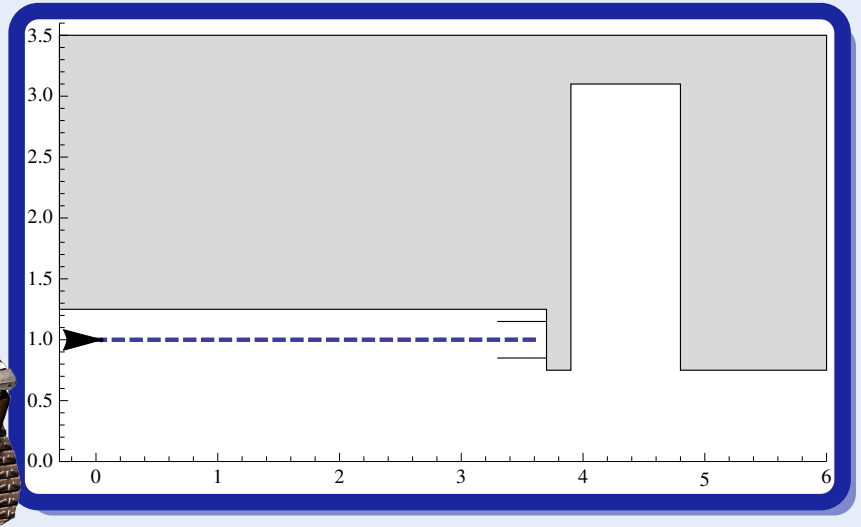


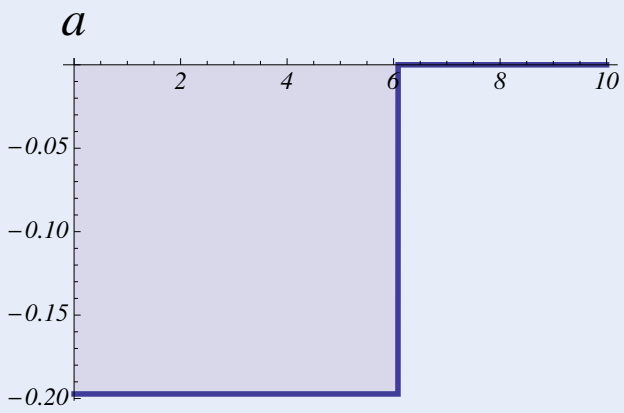


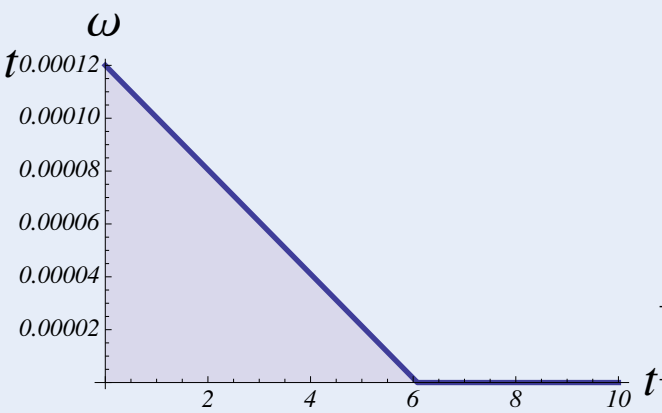
Challenge (Hybrid Systems)

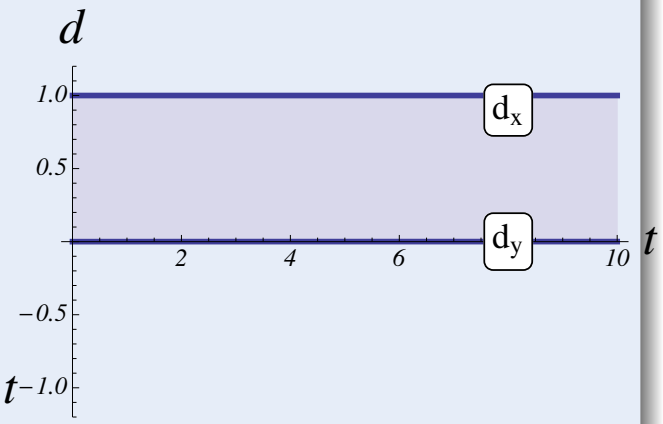
Design & verify controller for a robot avoiding obstacles

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





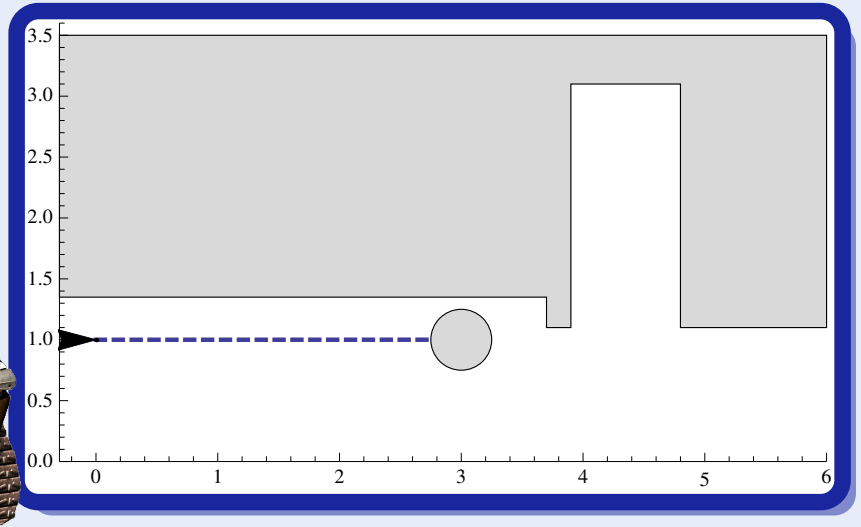


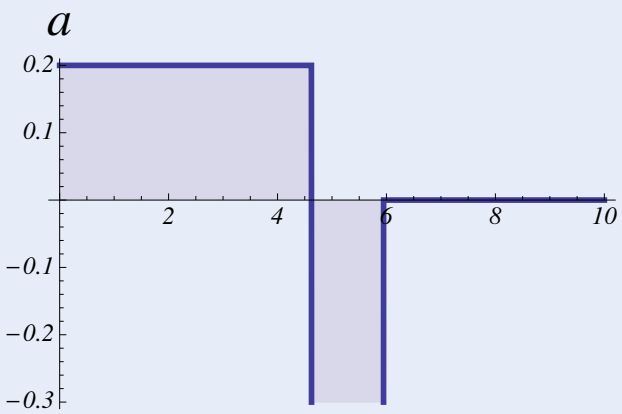


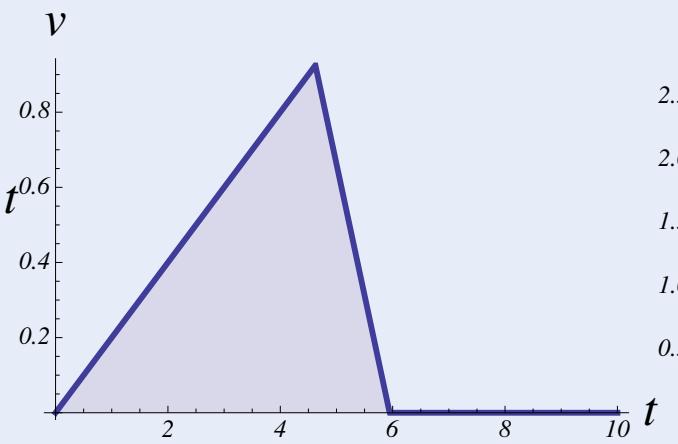
Challenge (Hybrid Systems)

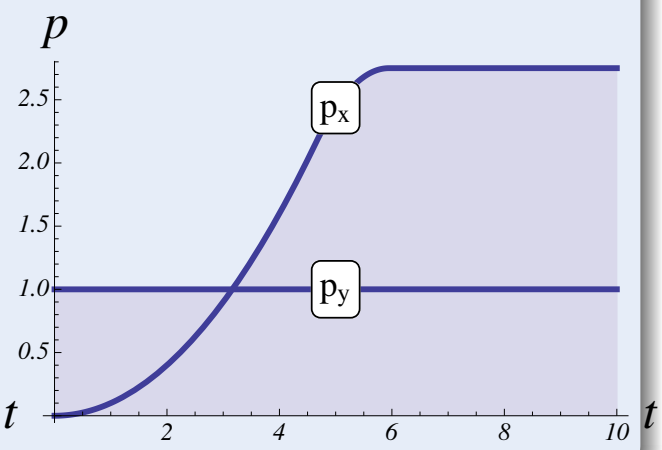
Design & verify controller for a robot avoiding obstacles

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





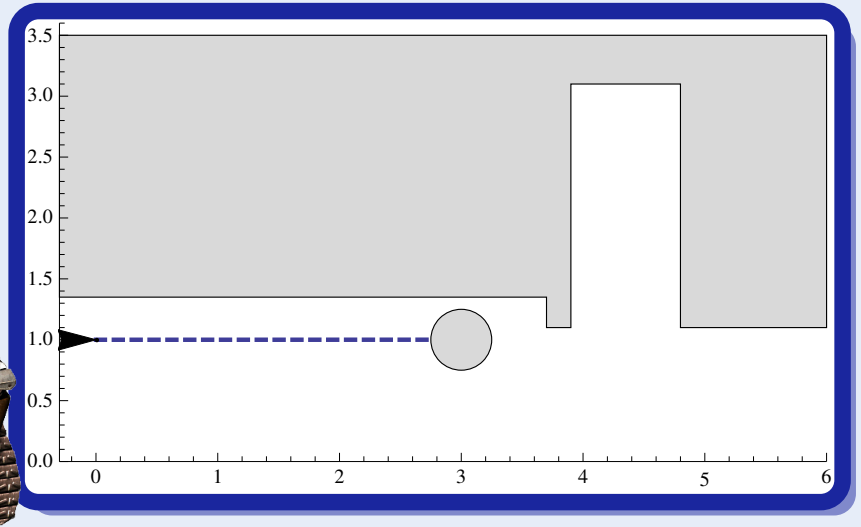


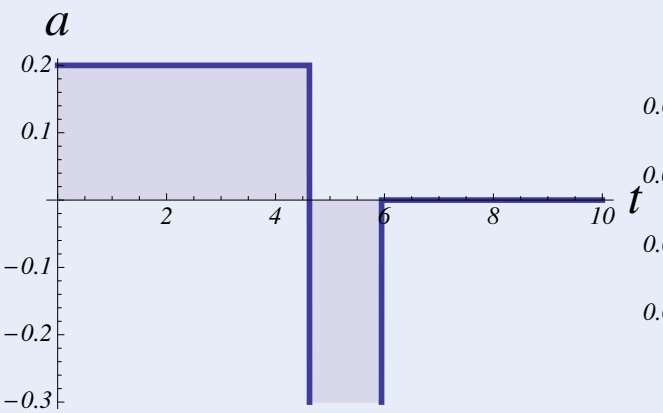


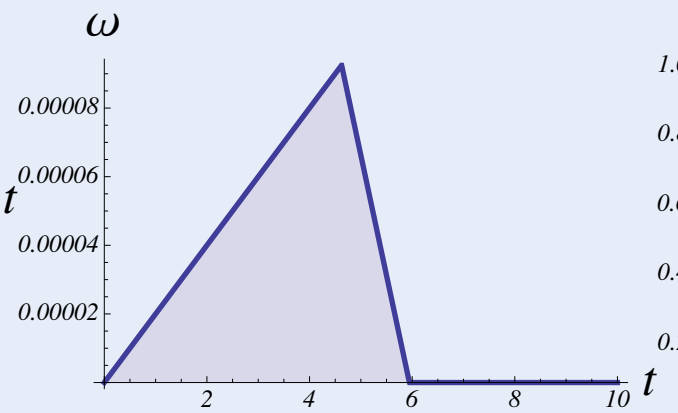
Challenge (Hybrid Systems)

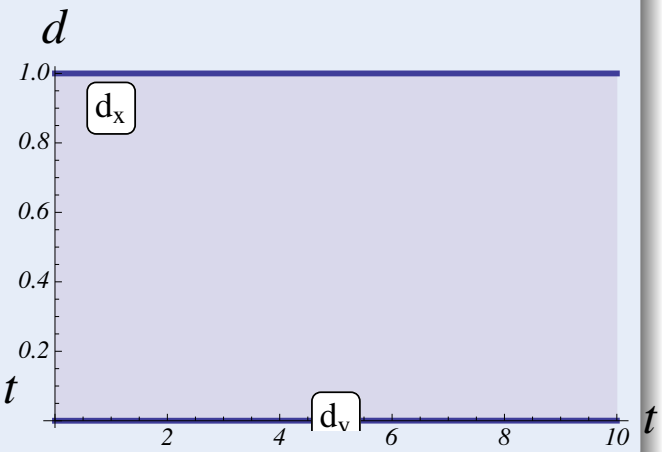
Design & verify controller for a robot avoiding obstacles

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





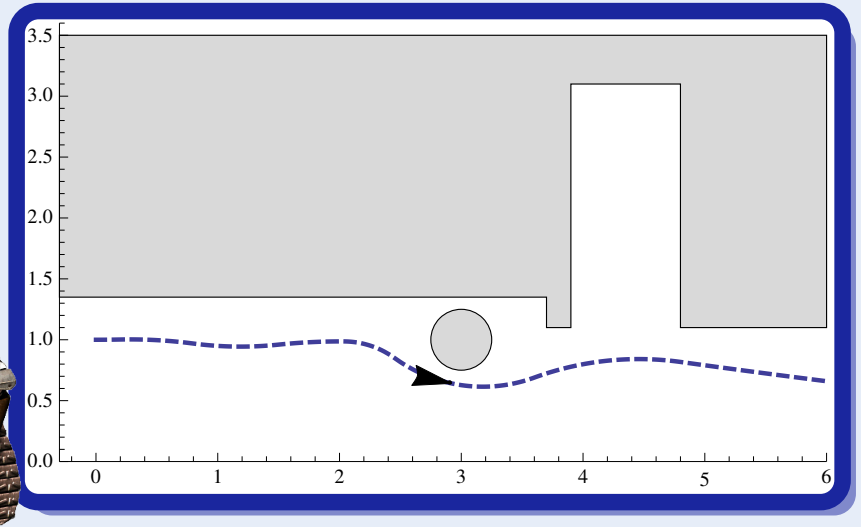


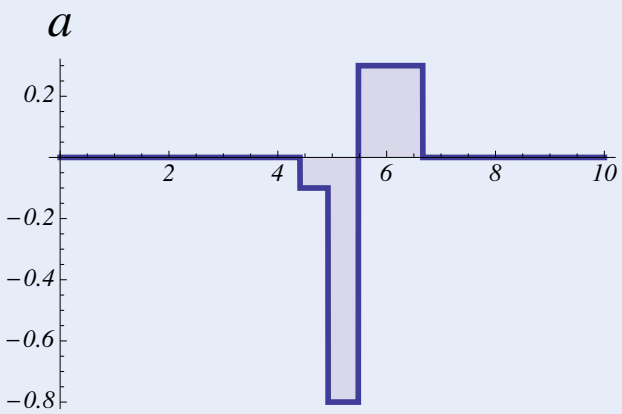


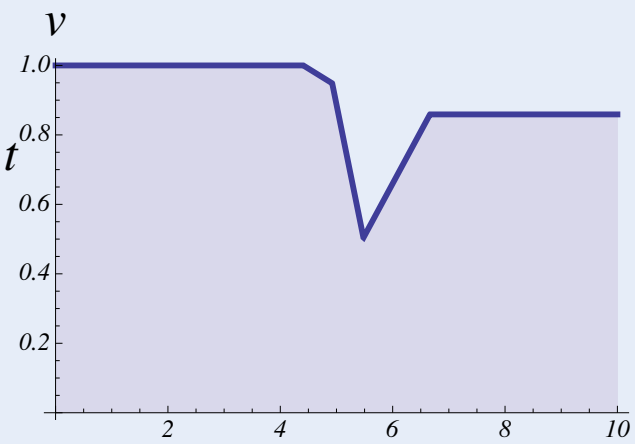
Challenge (Hybrid Systems)

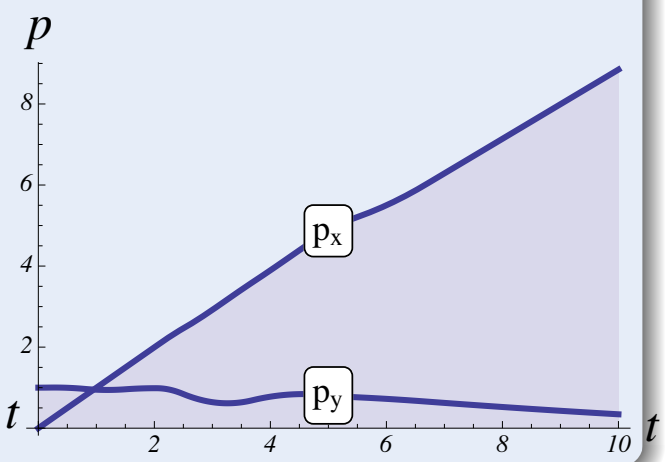
Design & verify controller for a robot avoiding obstacles

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





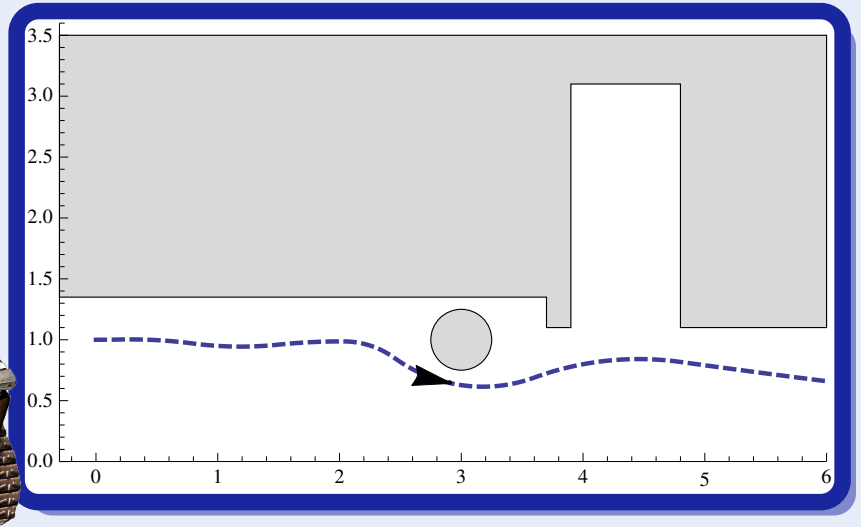


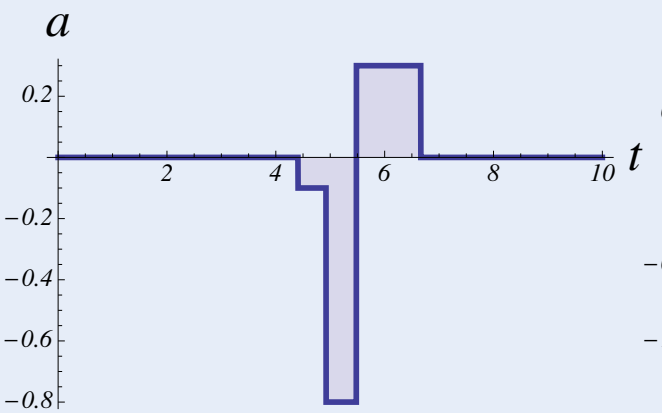


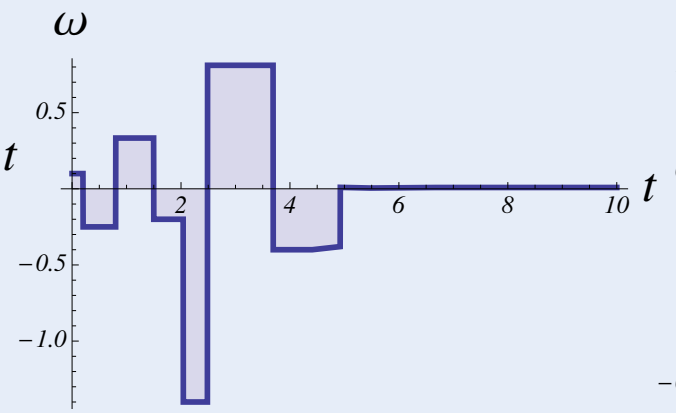
Challenge (Hybrid Systems)

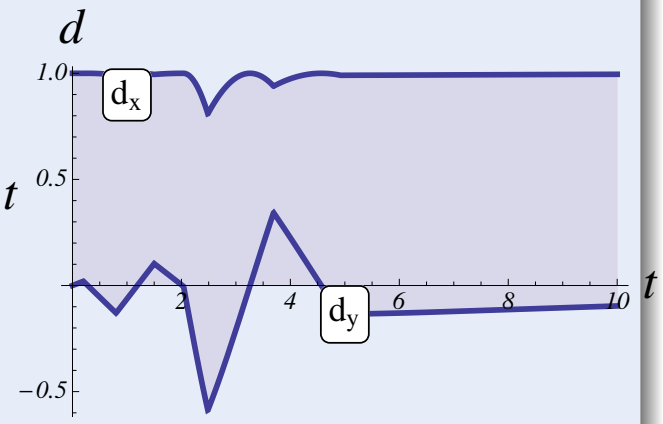
Design & verify controller for a robot avoiding obstacles

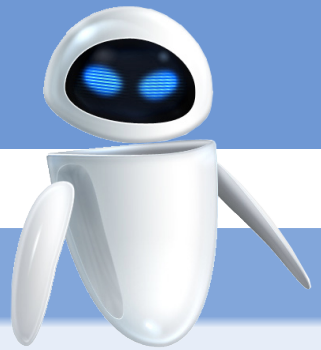
- Accel / brake / steer (discrete dynamics)
- 2D motion (continuous dynamics)







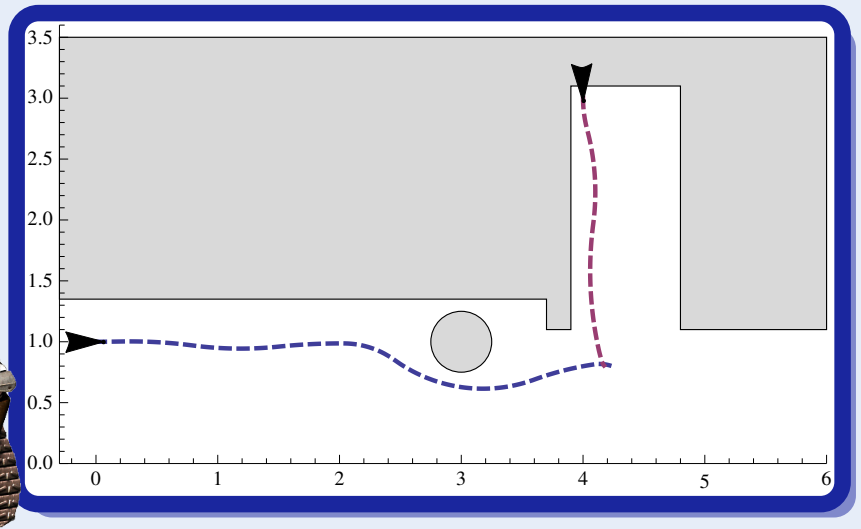


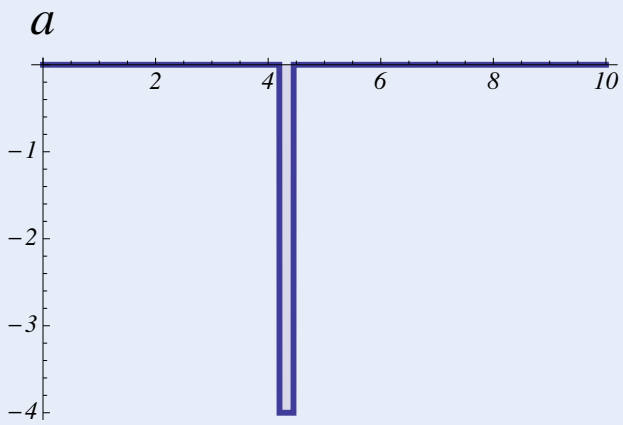


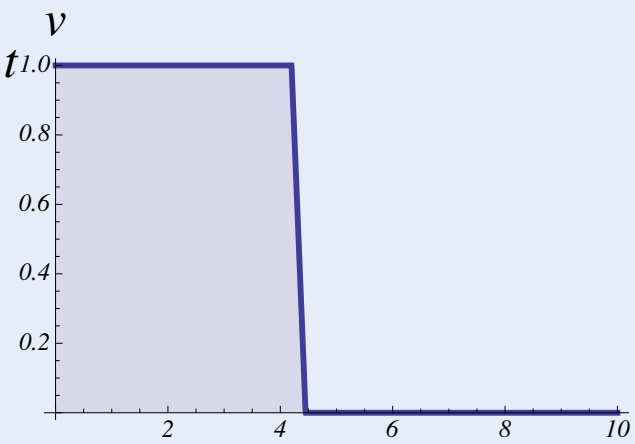
Challenge (Hybrid Systems)

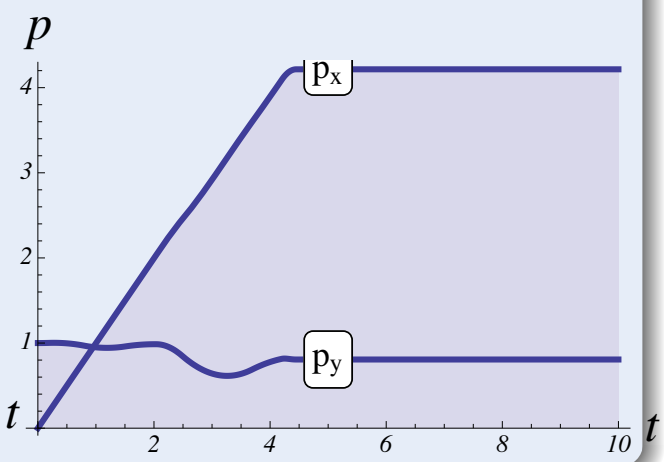
Design & verify controller for a robot avoiding obstacles

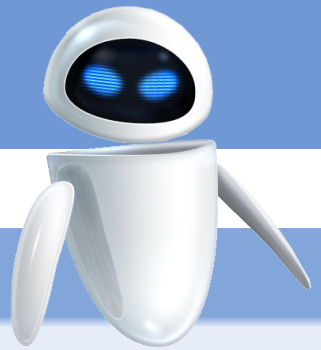
- Dynamic obstacles (other agents)
- Avoid collisions (define safety)







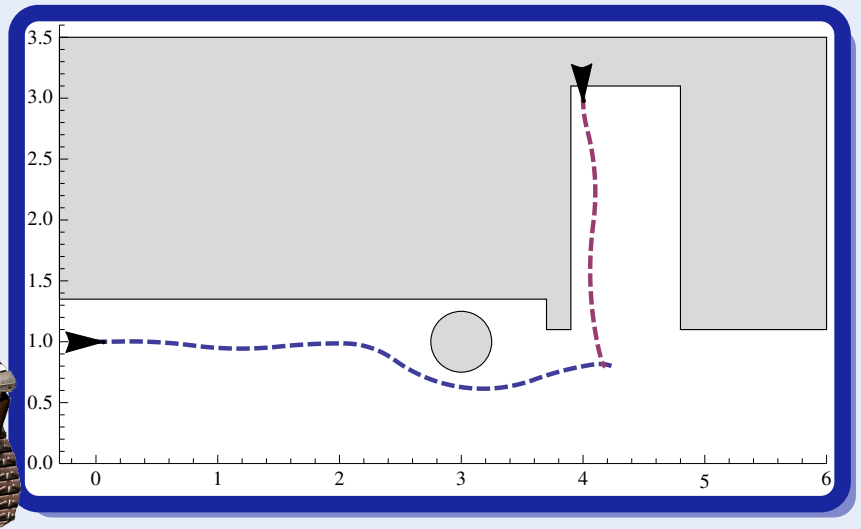


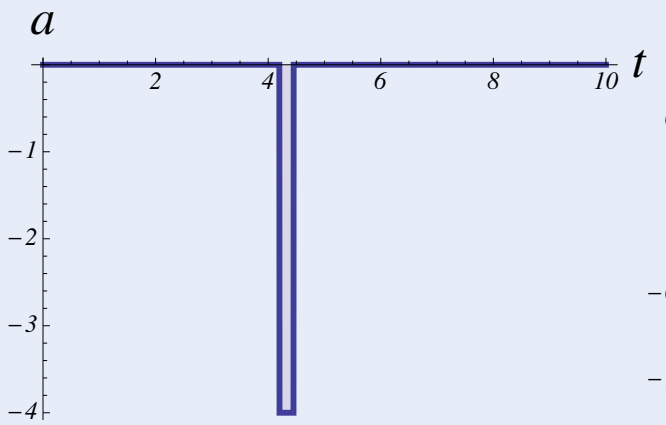


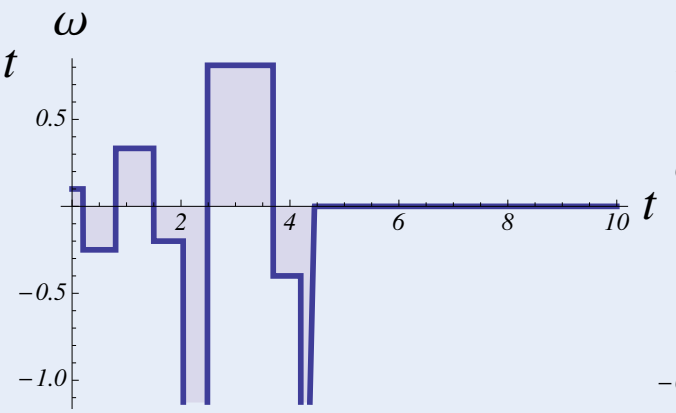
Challenge (Hybrid Systems)

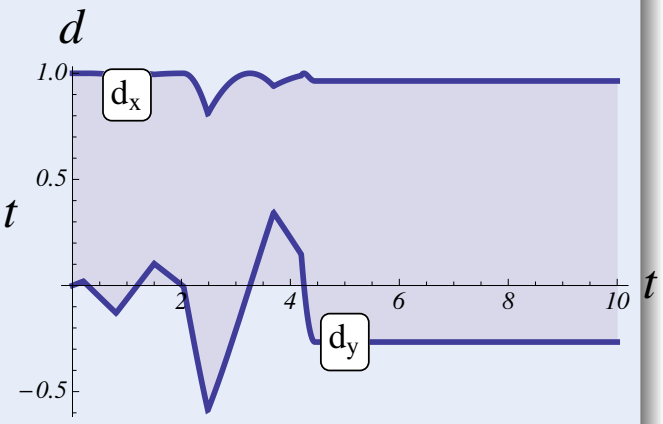
Design & verify controller for a robot avoiding obstacles

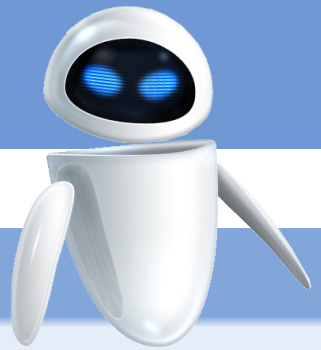
- Dynamic obstacles (other agents)
- Avoid collisions (define safety)







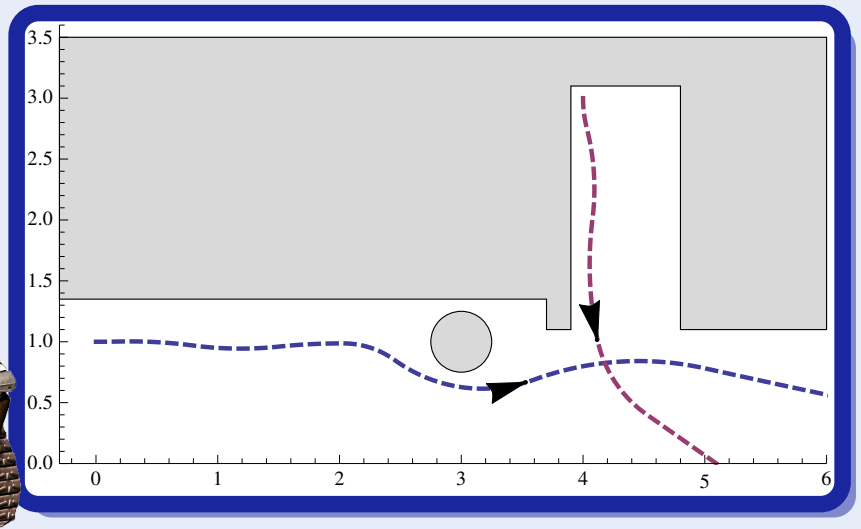


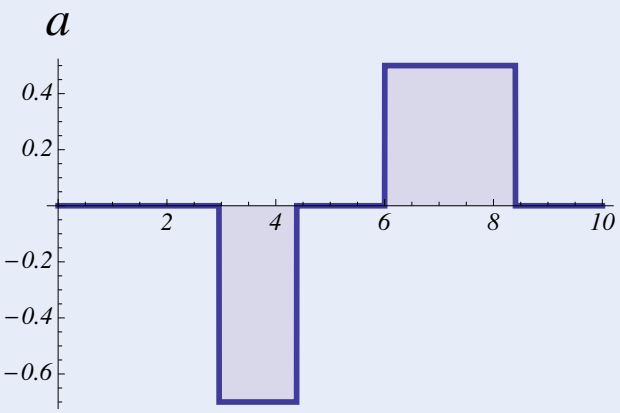


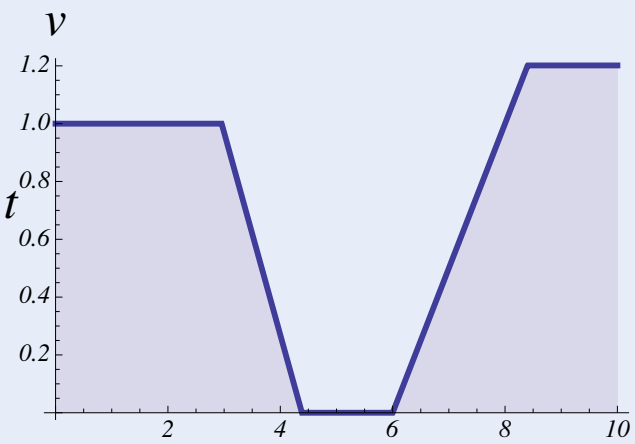
Challenge (Hybrid Systems)

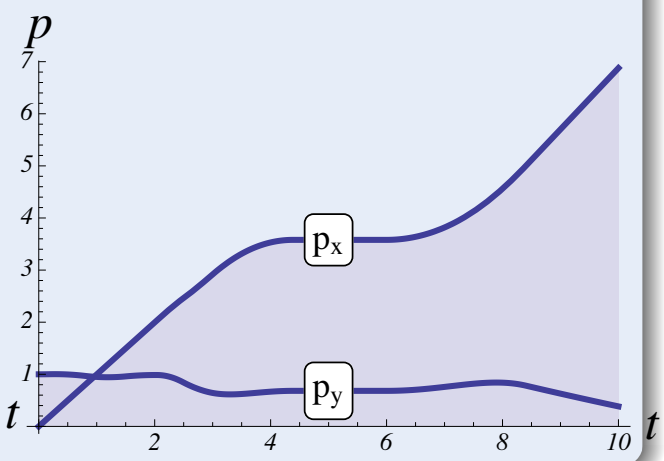
Design & verify controller for a robot avoiding obstacles

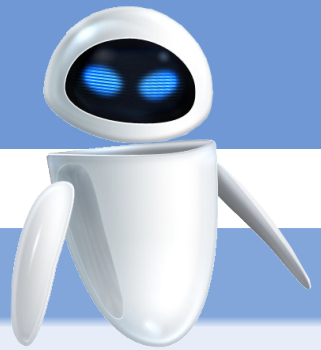
- Control robot (respect delays)
- Environment interaction (obstacles, agents, uncertainty)







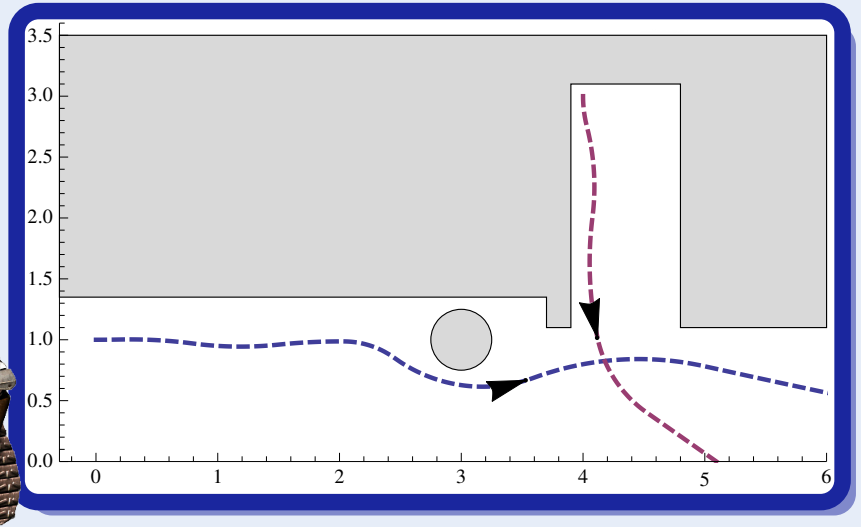


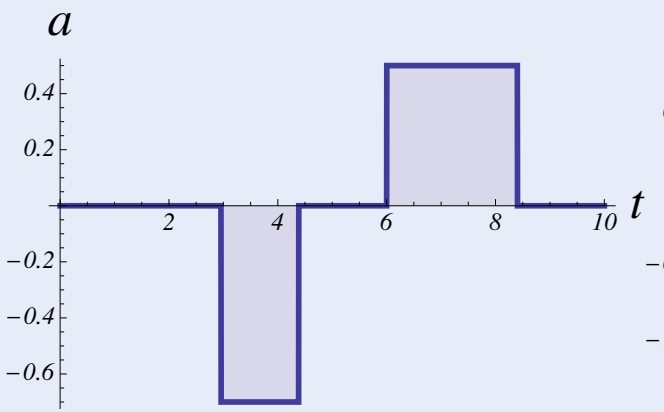


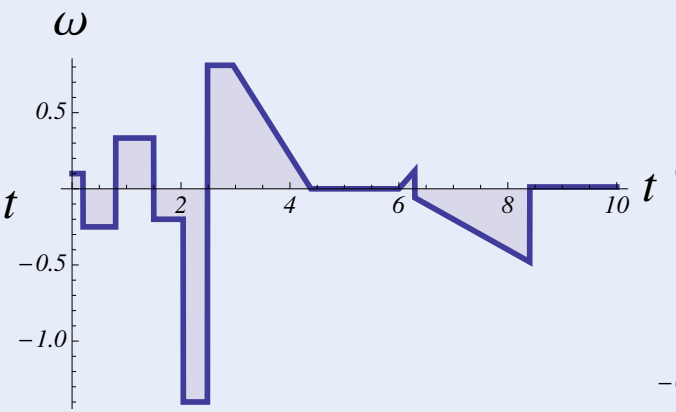
Challenge (Hybrid Systems)

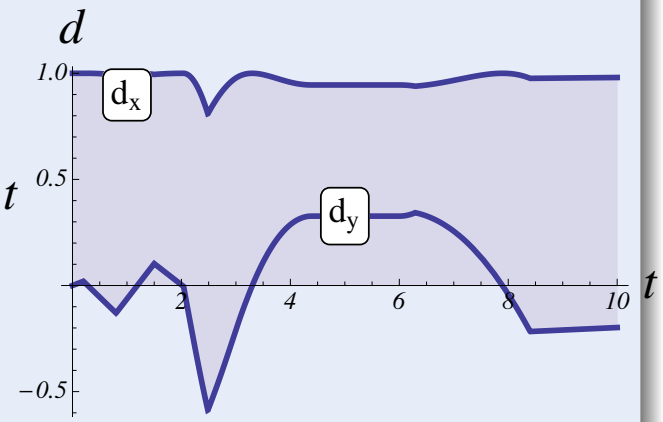
Design & verify controller for a robot avoiding obstacles

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

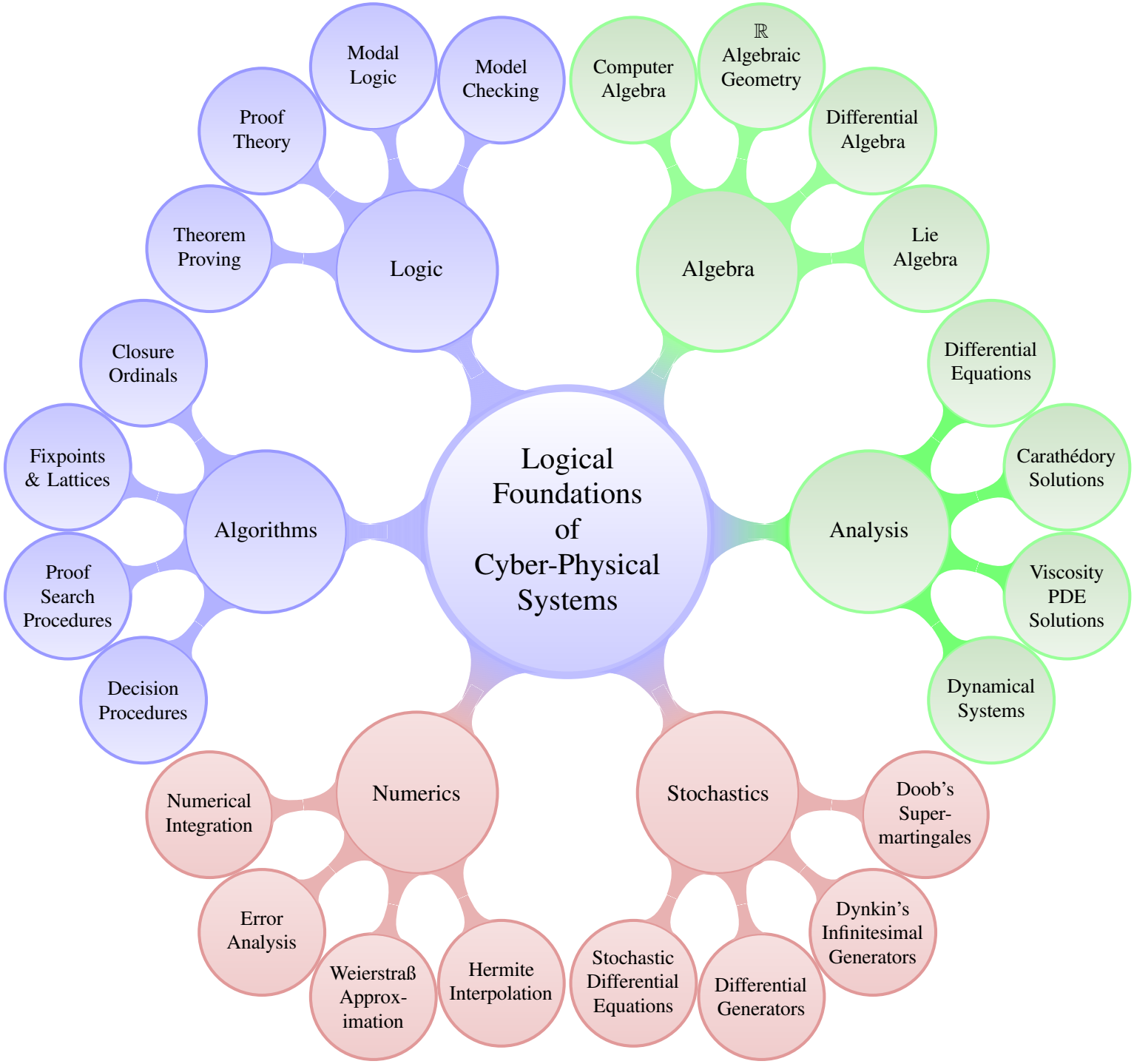








Outline


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
Analysis
Differential Equations
Carathédory Solutions
Viscosity PDE Solutions
Dynamical Systems
Stochastics
Doob's Super-martingales
Dynkin's Infinitesimal Generators
Differential Generators
Stochastic Differential Equations
Numerics
Hermite Interpolation
Weierstraß Approx-imation
Error Analysis
Numerical Integration
Algorithms
Decision Procedures
Proof Search Procedures
Fixpoints & Lattices
Closure Ordinals

How to Teach Cyber-Physical Systems?

Onion Model

1. Going outside in
2. Unpeel layer by layer
3. Progress when all prereqs are covered
4. First study CS $\wedge$ math $\wedge$ 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. 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.

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.
- Byproducts
  1. Exposure to numerous math areas in action.
  2. ...

Course Outline

1. Cyber-physical systems: introduction
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
10. Differential equations & differential invariants
11. Differential equations & proofs
12. Dynamic logic & dynamical systems

---

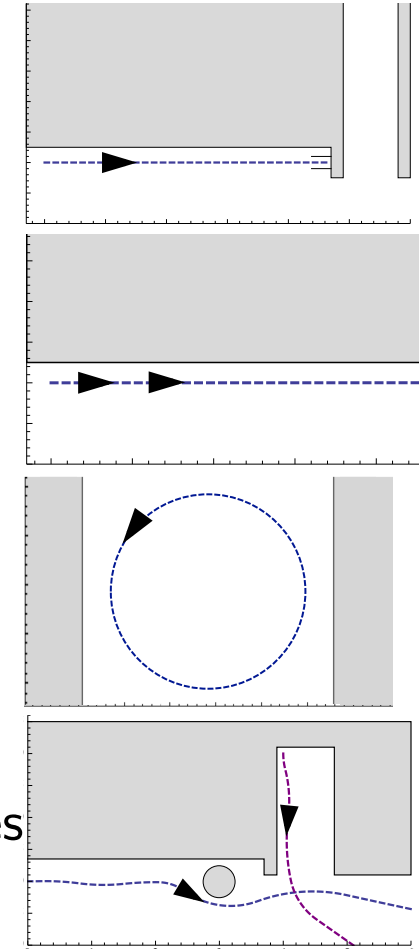
13. Robots / railway / air traffic / car CPS & applications
14. Hybrid systems & hybrid games
15. Virtual substitution & real arithmetic

Assessment

- Read Collaboration and Academic Integrity Policy — Policy
- ≈22% Theory homework — Due at **beginning** of lecture
- ≈51% Labs, including ≈22% final project — Due at 22:00
- Whitepaper — For final project
- Proposal — For final project
- Term paper — Due with final project
- ≈11% Midterm
- ≈11% Final
- ≈5% Participation in class and in online comments
- Partner allowed for labs only and only starting in lab 2

Robot Labs

1. Robot on Rails
   a. Autobots, Roll Out
   b. Charging Station
2. Robot on Highways: Follow the Leader
   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. 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 presented at CPS V&V Grand Prix



▸ CPS v&V Grand Prix

Resources

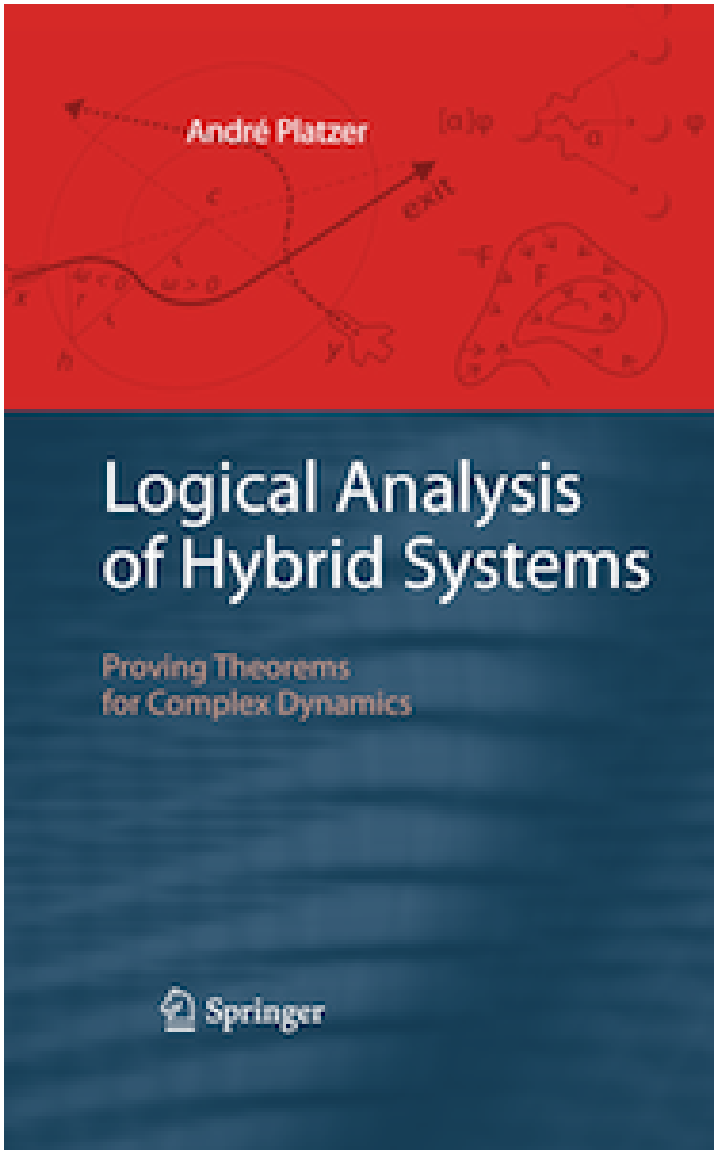
Prerequisites

15-122 Principles of Imperative Computation
21-122 Integration, Differential Equations, and Approximation
(15-251 Great Theoretical Ideas in Computer Science **or**
21-241 Matrix algebra **or**
18-202 Mathematical Foundations of Electrical Engineering)

- 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/fcps16.html
- KeYmaera X
- Piazza
- Autolab
- Ask!

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

Outline

CPS Design & CPS Contracts in Programs

HP Reveal in layers

Contracts Reason about CPS

```
@requires(0<=x & x=H & v=0)
@requires(g>0 & 1>=c>=0)
@ensures(0<=x & x<=H)
  {
    {x'=v, v'=-g, x>=0}
    if (x = 0) {
        v := -c*v;
    }
  }*@invariant(2*g*x <= 2*g*H - v^2 & x>=0)
```

CPS Simulate for intuition

CT Design-by-invariant

CPS Contracts & CPS Logic

dL Logic for CPS

Contracts Reason in Logic

```
  0<=x & x=H & v=0
  & g>0 & 1>=c>=0
->
  [{
    {x'=v, v'=-g, x>=0}
    if (x = 0) {
        v := -c*v;
    }
  }*@invariant(2*g*x <= 2*g*H - v^2 & x>=0)
  ] (0<=x & x<=H)
```

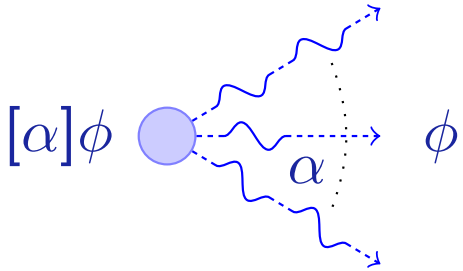
CPS Analyze for precision

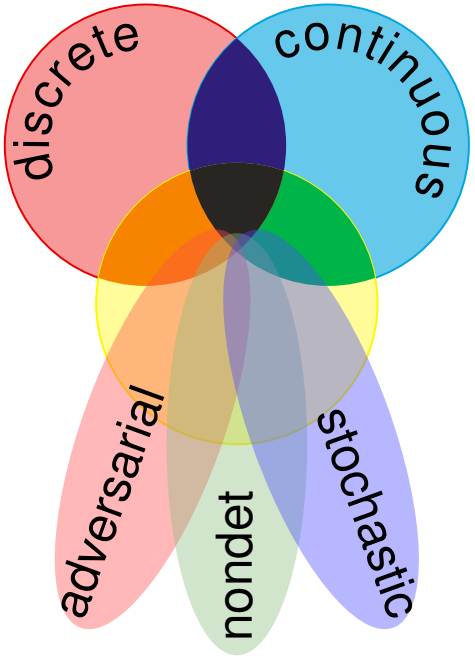
CT Proof-by-invariant

Dynamic Logics for Dynamical Systems

differential dynamic logic

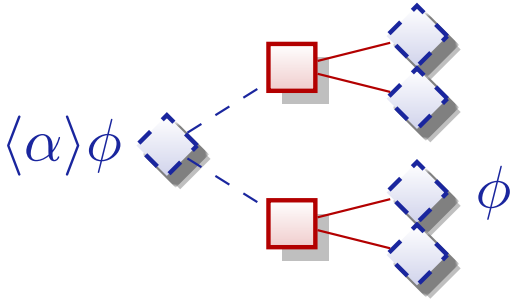
$\mathsf{d}\mathcal{L} = \mathsf{DL} + \mathsf{HP}$





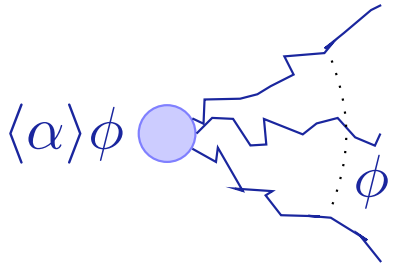
differential game logic

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



stochastic differential DL

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



quantified differential DL

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

JAR'08,CADE'11,LMCS'12,LICS'12

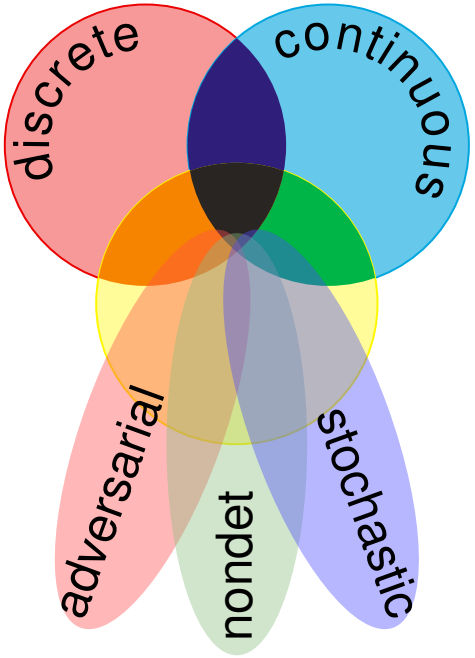
LICS'12,CADE'15,TOCL'15

Outline

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.

André Platzer.
Foundations of cyber-physical systems.
Lecture Notes 15-424/624, Carnegie Mellon University, 2014.

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

André Platzer.
Logics of dynamical systems.
In LICS [11], pages 13–24.

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.

André Platzer.
A uniform substitution calculus for differential dynamic logic.
In Amy Felty and Aart Middeldorp, editors, *CADE*, volume 9195 of *LNCS*, pages 467–481. Springer, 2015.

André Platzer.
Differential game logic.
ACM Trans. Comput. Log., 17(1):1:1–1:51, 2015.

André Platzer.
The complete proof theory of hybrid systems.
In LICS [11], pages 541–550.

André Platzer.
A complete axiomatization of quantified differential dynamic logic for distributed hybrid systems.
Log. Meth. Comput. Sci., 8(4):1–44, 2012.
Special issue for selected papers from CSL'10.

André Platzer.
Stochastic differential dynamic logic for stochastic hybrid programs.

In Nikolaj Bjørner and Viorica Sofronie-Stokkermans, editors, *CADE*, volume 6803 of *LNCS*, pages 431–445. Springer, 2011.

Proceedings of the 27th Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2012, Dubrovnik, Croatia, June 25–28, 2012. IEEE, 2012.