Teaching and Proving CPS:

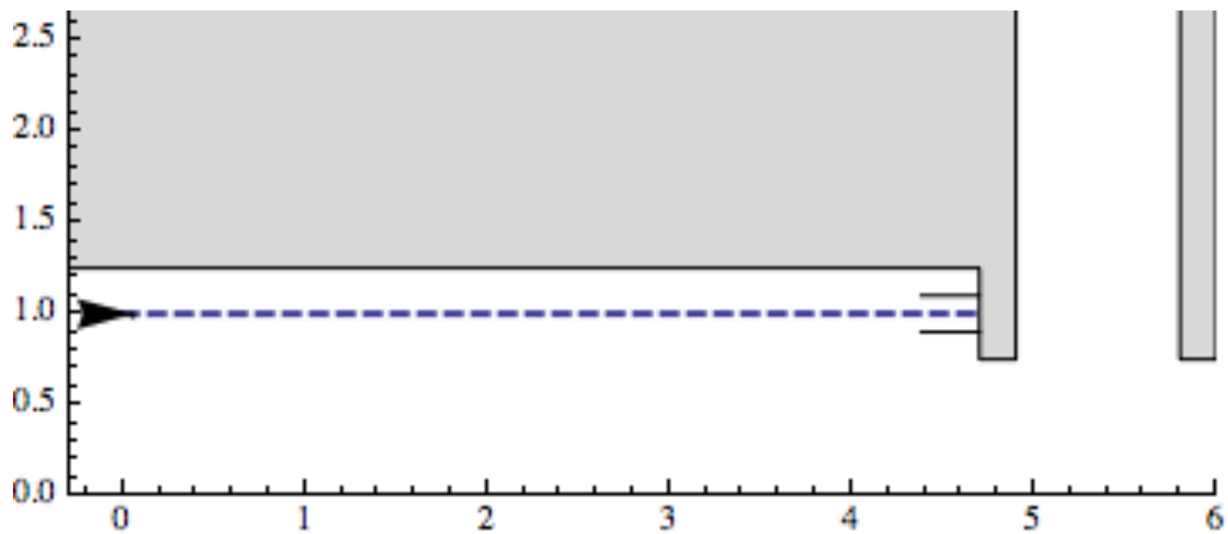
A tutorial for KeYmaera and and discussion of how to teach CPS.

Sarah M. Loos and André Platzer

Computer Science Department

Carnegie Mellon University

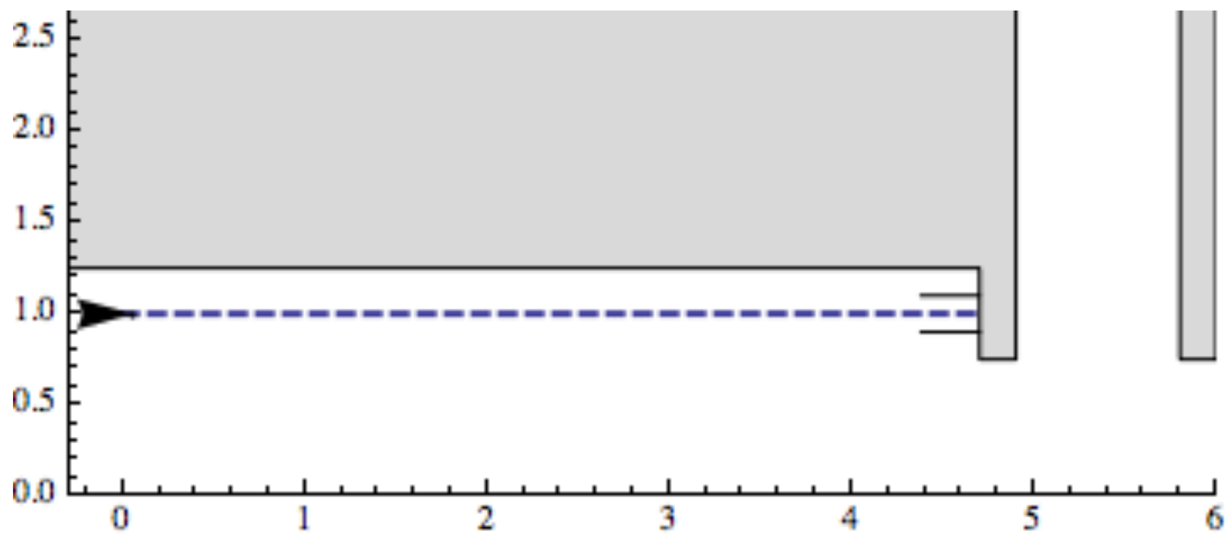
Charging Station



- Single-shot controller
- Straight line dynamics
- Prove the robot decelerates properly, (i.e. reaches charging station but does not overshoot).

Demo ⏏

Charging Station



$$v(t) = at + v_0$$

$$v(t_{stop}) = 0$$

$$t_{stop} = -v_0/a$$

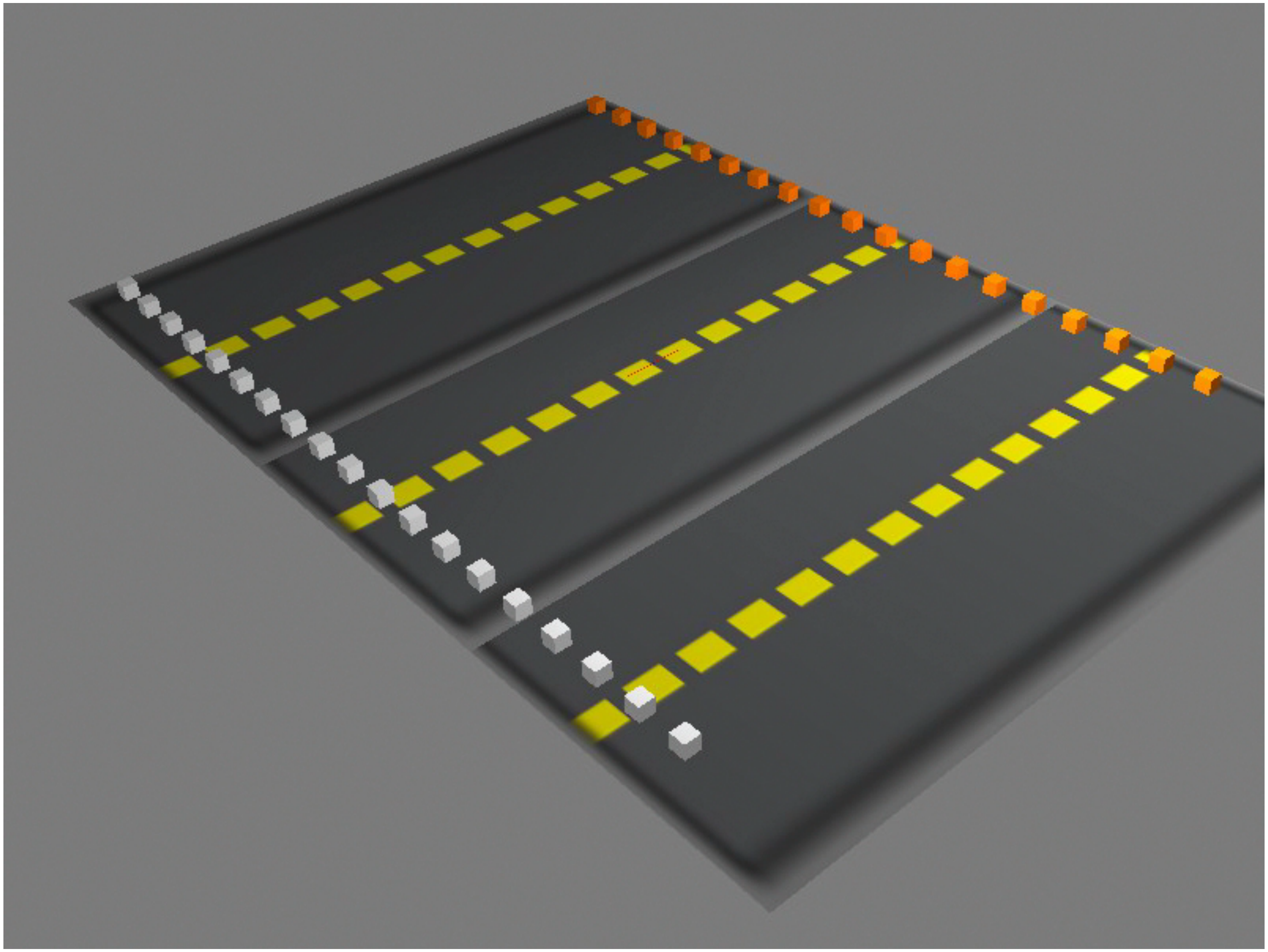
$$\boxed{a = \frac{-v_0^2}{2(s - x_0)}}$$

$$x(t) = \frac{1}{2}at^2 + v_0 t + x_0$$

$$x(t_{stop}) = s$$

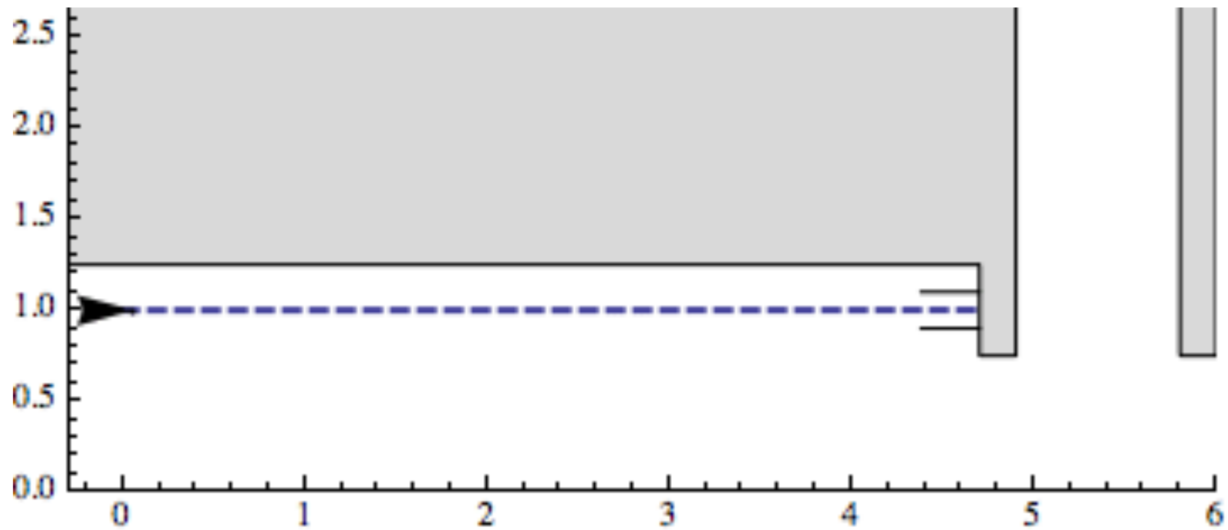
$$s = \frac{1}{2}at_{stop}^2 + v_0 t_{stop} + x_0$$

Simulations

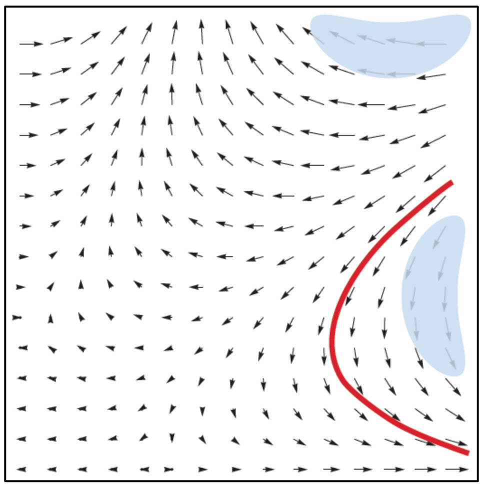


Charging Station

now using differential invariants

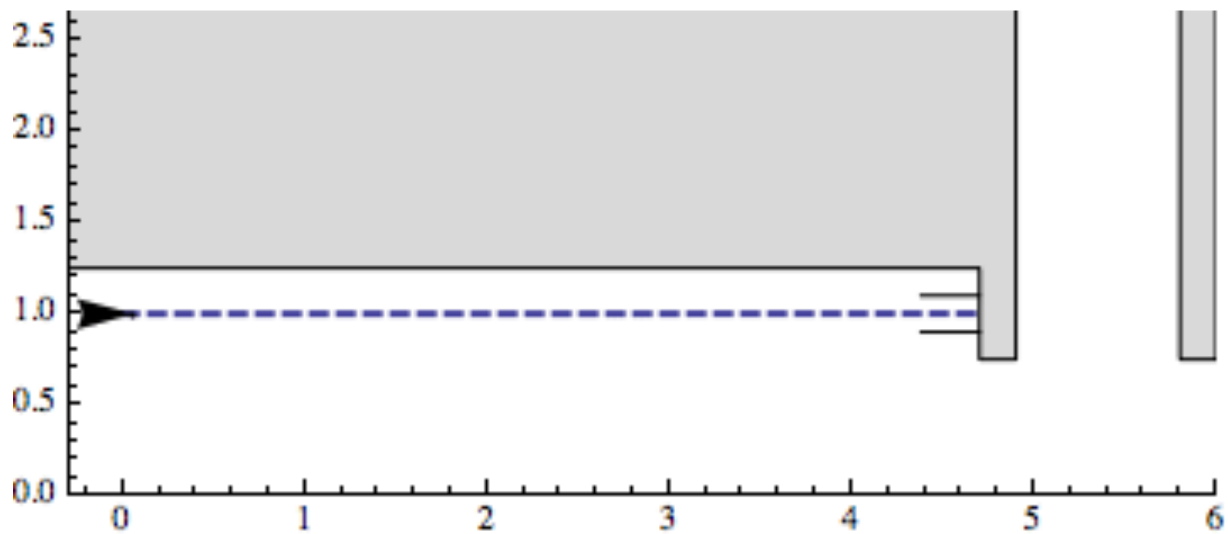


- Suppose we disable the ODE solver.



Charging Station

now using differential invariants



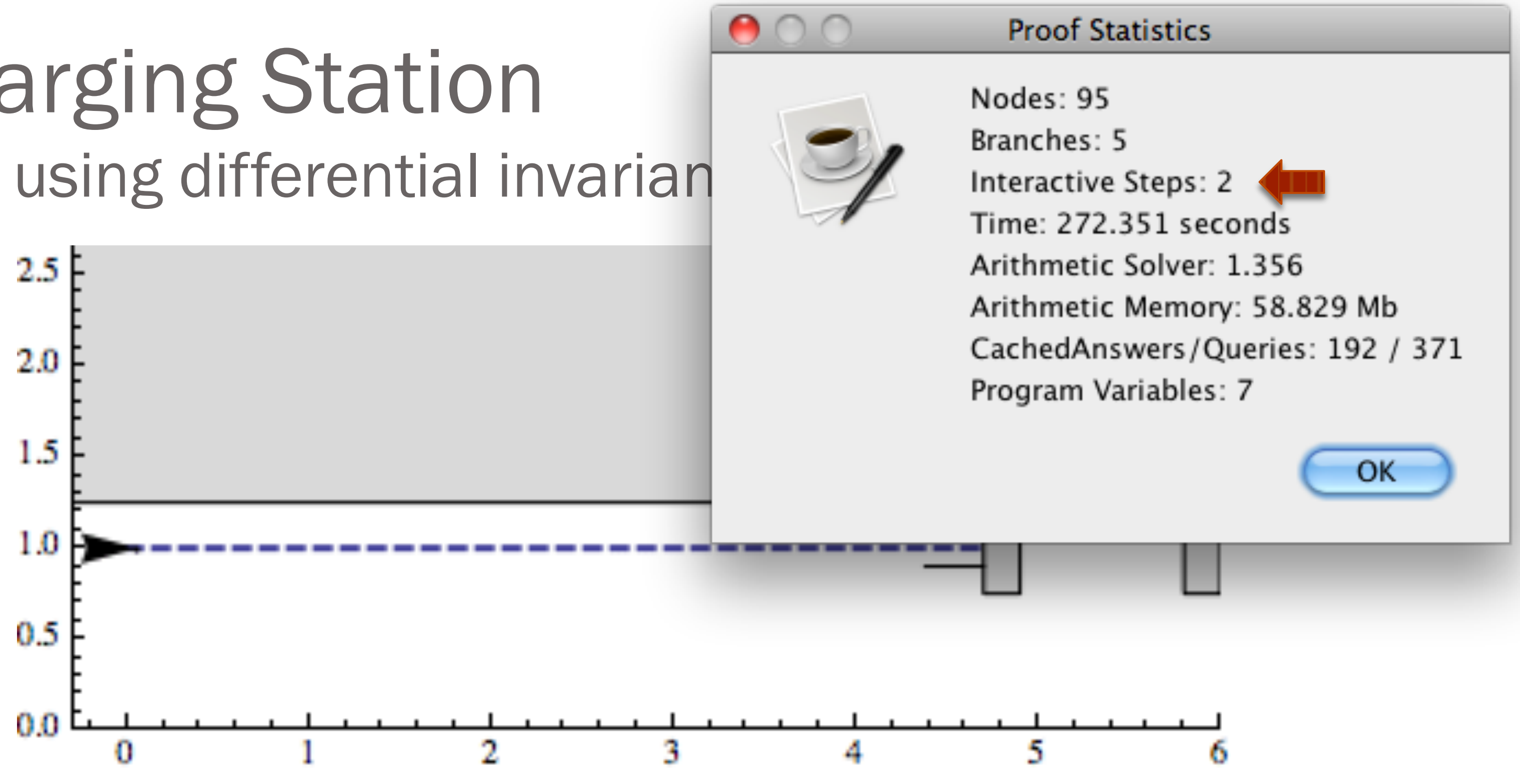
- Suppose we disable the ODE solver.
- The user can cut in solutions, and KeYmaera will check and then use them:

$$x = \frac{1}{2}at^2 + v_0 t + x_0 \qquad v = at + v_0$$

Demo ⏏

Charging Station

now using differential invarian

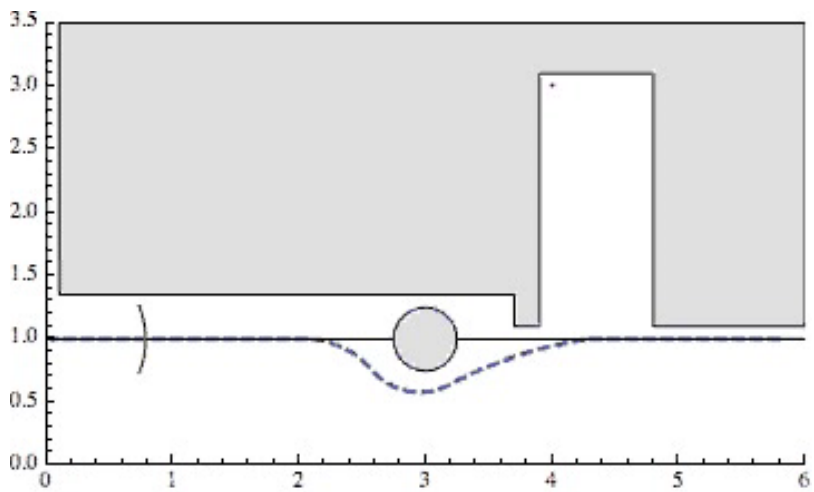


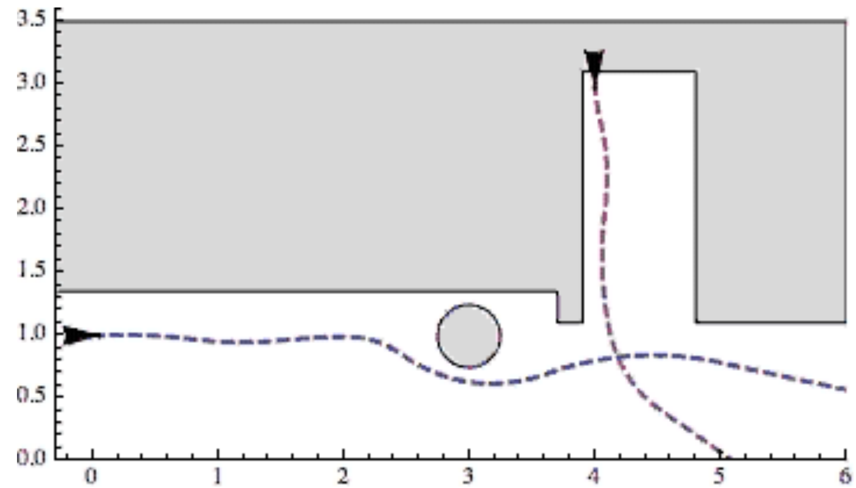
- Suppose we disable the ODE solver.
- The user can cut in solutions, and KeYmaera will check and then use them:

$$x = \frac{1}{2}at^2 + v_0 t + x_0 \qquad v = at + v_0$$

2D Motion

with static and dynamic obstacles





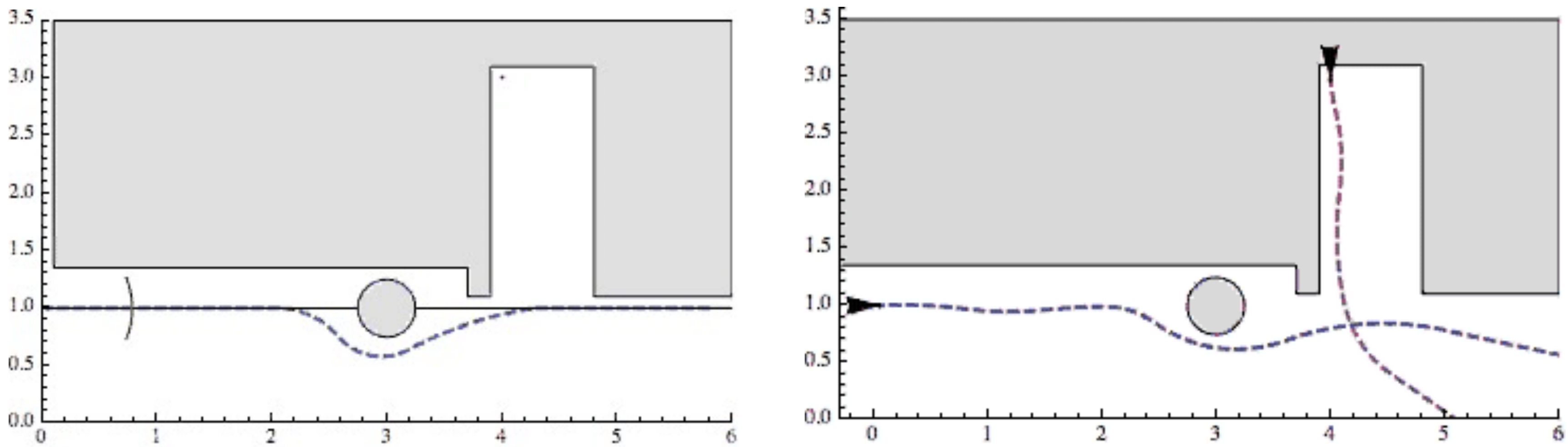
New Challenges:

- System Loops
- 2D Motion (Dubins Model)
- Nondeterministic Controller
- Nonlinear and Smooth Paths
- Nonlinear Controller
- Complex Differential Invariants
- Proof Interactions and Branching
- What is safety now?

Demo ⏏

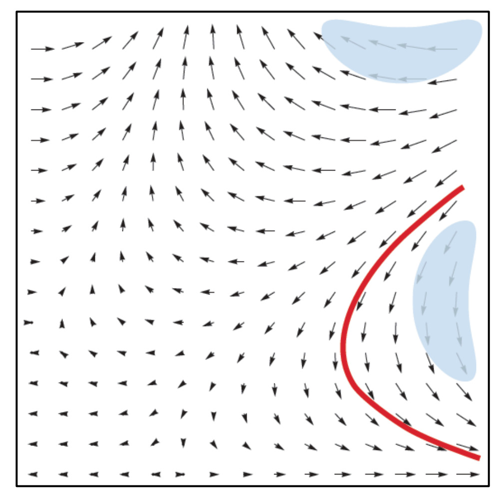
2D Motion

with static and dynamic obstacles



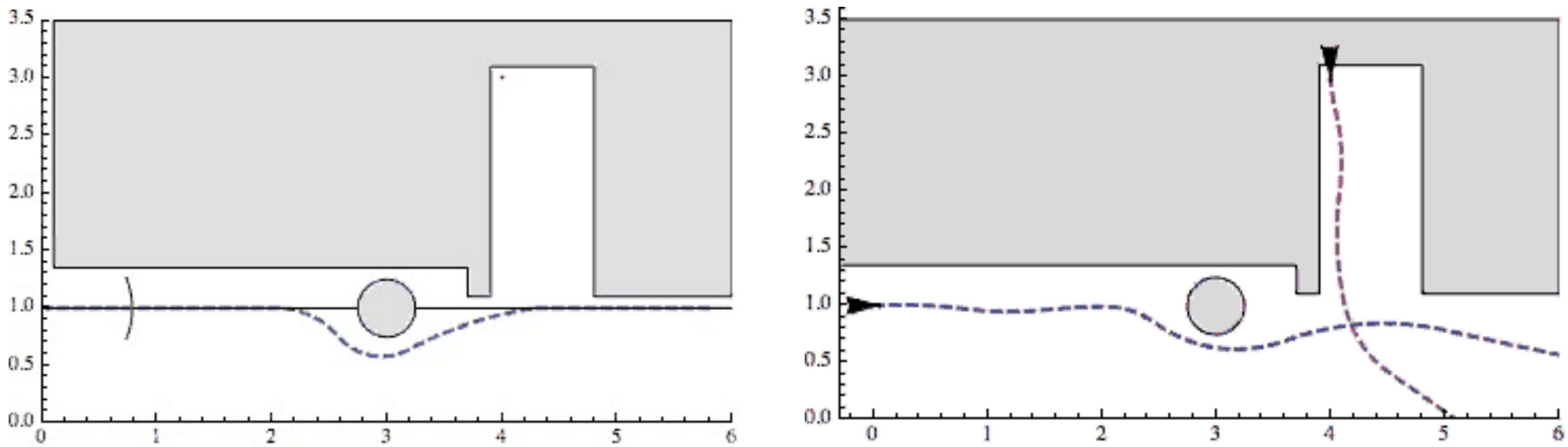
Differential Invariants:

- $v = v_0 + at$
- $d^2 + e^2 = 1$



2D Motion

with static and dynamic obstacles

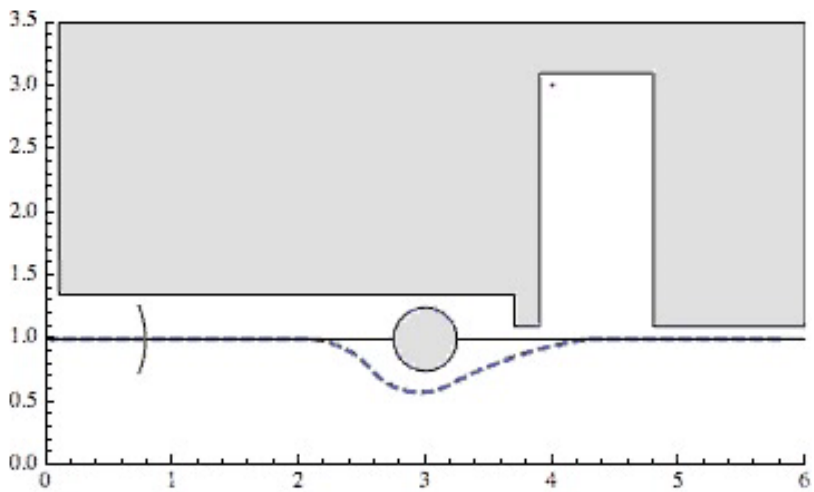


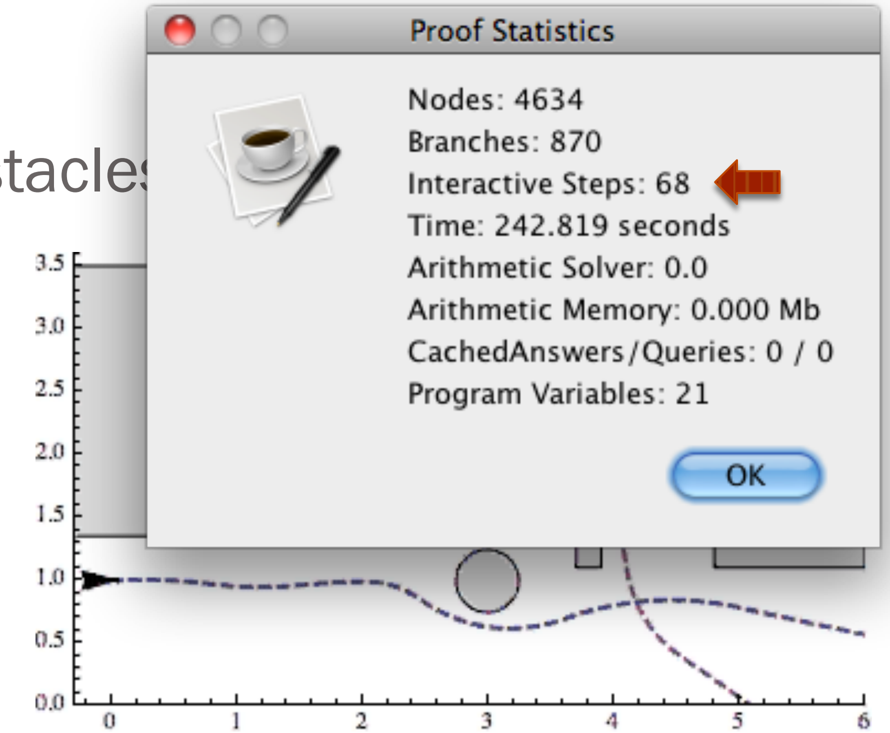
Differential Invariants:

- $v = v_0 + at$
- $d^2 + e^2 = 1$
- $|x - x_0| \leq \frac{1}{2}at^2 + v_0 t$
- Similarly for all obstacles

2D Motion

with static and dynamic obstacles



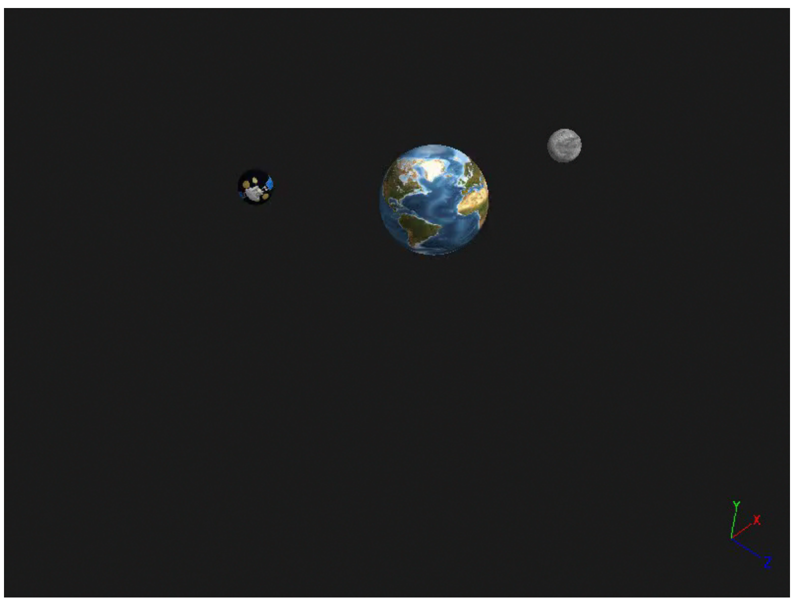


New Challenges:

- System Loops
- 2D Motion (Dubins Model)
- Nondeterministic Controller
- Nonlinear and Smooth Paths
- Nonlinear Controller
- Complex Differential Invariants
- Proof Interactions and Branching
- What is safety now? “Passive”

Simulations

- Students get quick feedback
- We generate counter examples by hand
- We also send a simulation of our own solution.



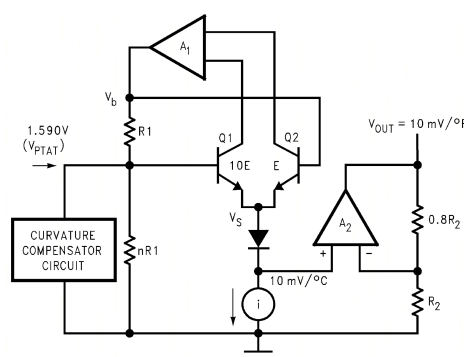
Final Project and Term Paper

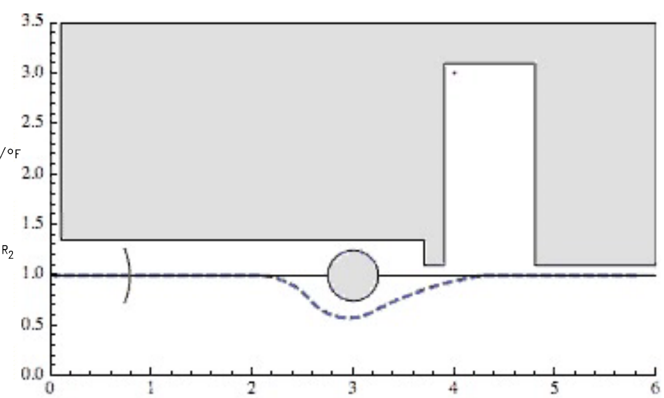
Their Ideas:

- Wall-E and Eve meet in space
- Electrical Circuits
- 3D Avoidance Maneuvers
- and more to come…

Our Suggestions:

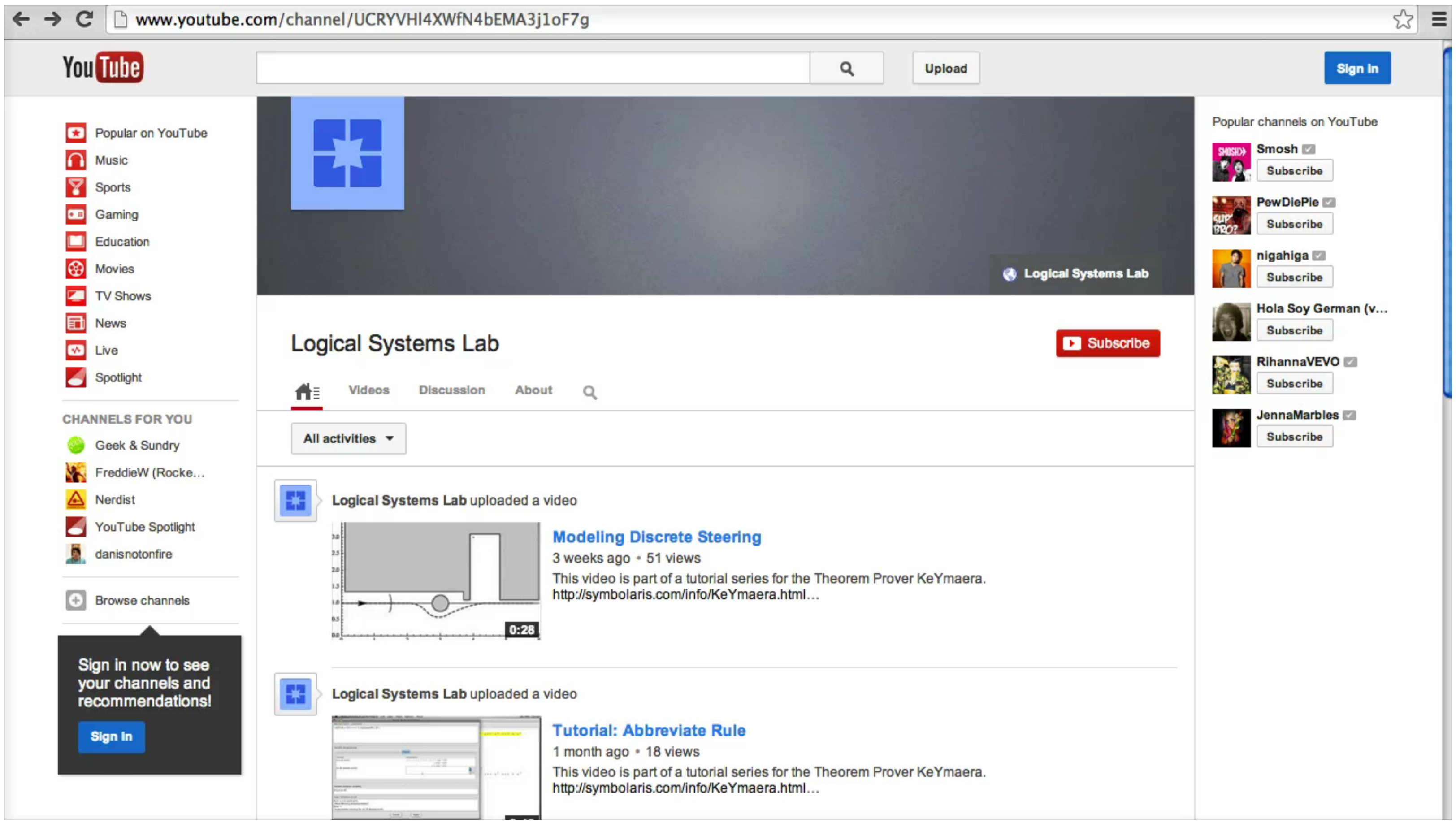
- Predator/Prey Models
- Verified PID Controller
- Extensions to the 2D obstacle avoidance lab: noisy sensors, more complex obstacles, etc.





YouTube Tutorial Videos

Connect chalkboard concepts to KeYmaera implementations.



What the students say

Early Course Evaluations:

"Structure of class is good: theory, then the intuition, then example."

"**Simulation** is so cute! Can we get it for the final submission, too?"

"One more recitation would be helpful to see more applications of the theory."

"The **lecture notes** are really useful and have helped me a lot in the course."

"**Tests** before labs are crucial! I would have failed the labs otherwise."

"Would like to see **more examples** of HPs and their proofs."

Takeaway:
Undergrads can design and verify CPS!

Good Ideas:

- Simulations and two-round submission process.
- YouTube tutorial videos.
- Serves as a bridge between CS and engineering.
- Students appreciate complexity and importance of CPS design and analysis.
- As far as we know, this is the most advanced undergrad CPS course offered.

Lessons Learned:

- Better automation can lead to a steeper learning curve.
- Differential Invariants are tough.
- The jump from 1D to 2D is also challenging.
- Provide more examples.