

Teaching and Proving CPS:

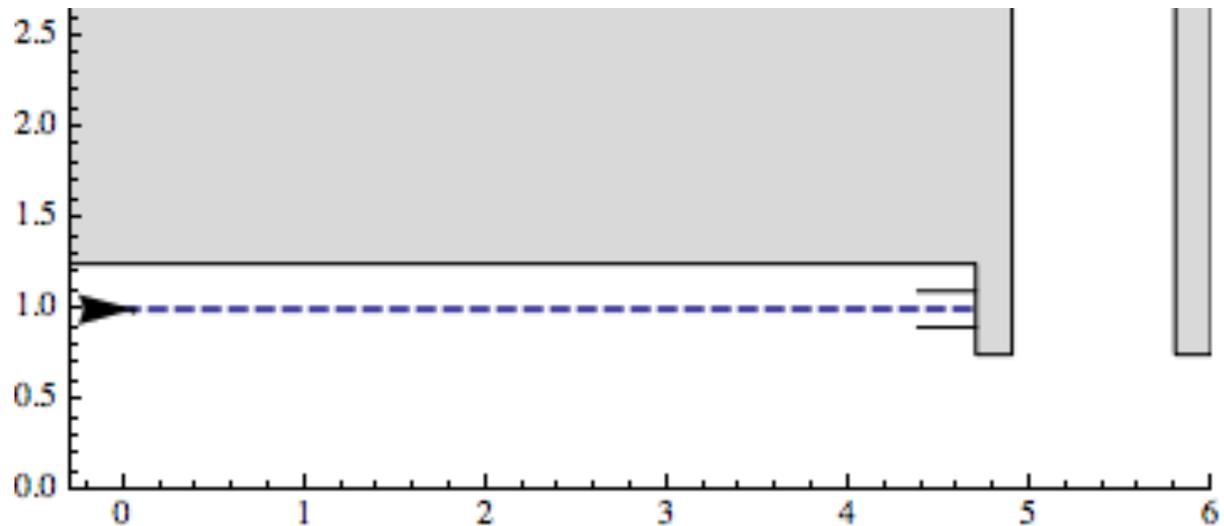
A tutorial for KeYmaera and a discussion of how to teach CPS.

Sarah M. Loos and André Platzer

Computer Science Department

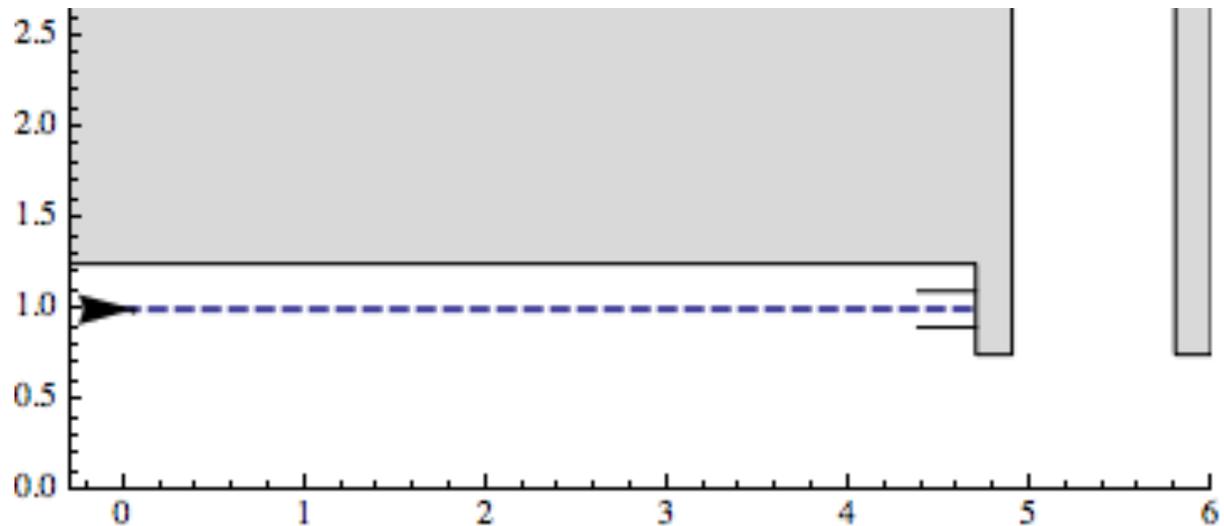
Carnegie Mellon University

Charging Station



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

Charging Station



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

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

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

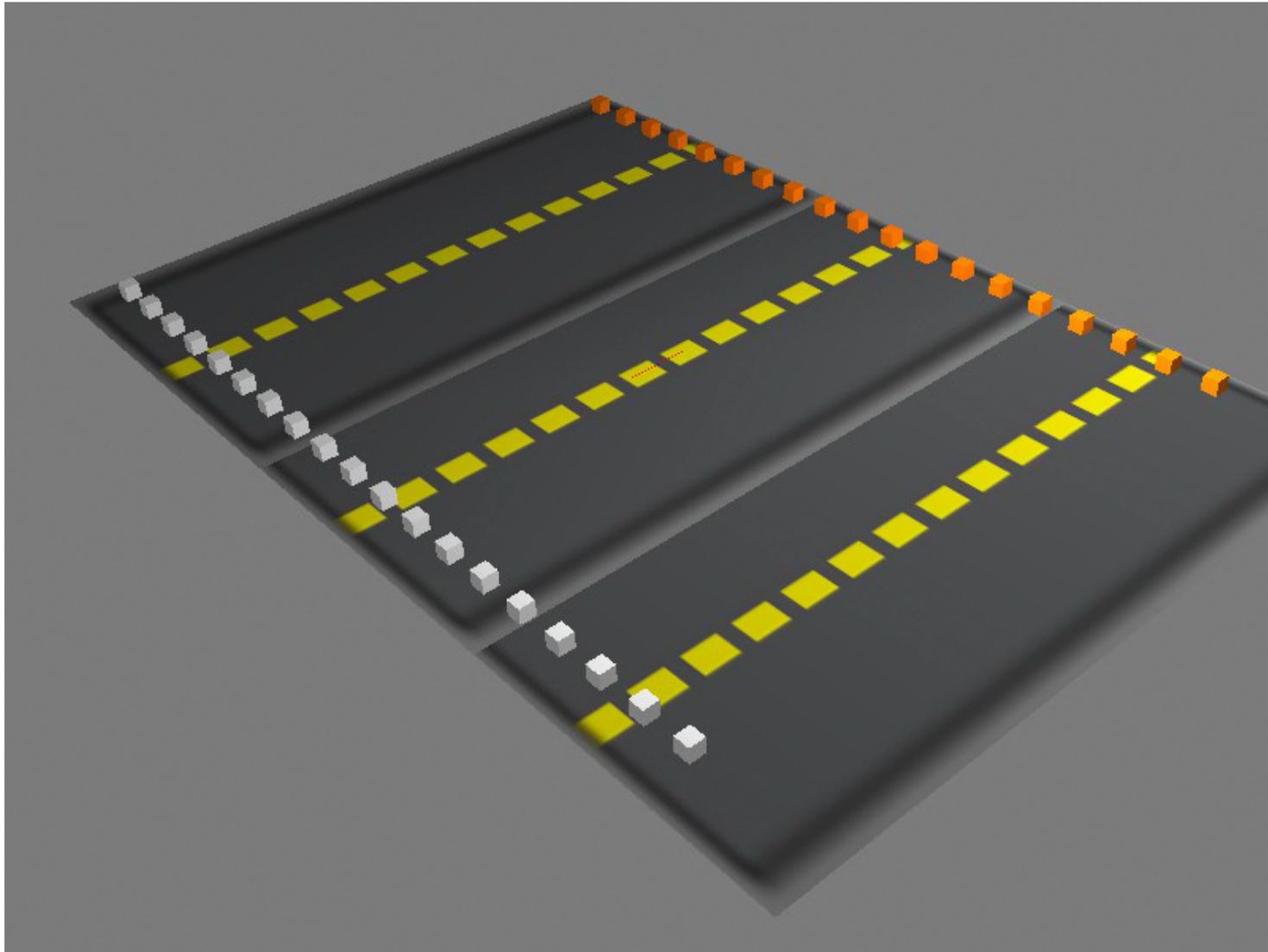
$$a = \frac{-v_0^2}{2(s - x_0)}$$

$$x(t) = \frac{1}{2}at^2 + v_0t + x_0$$

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

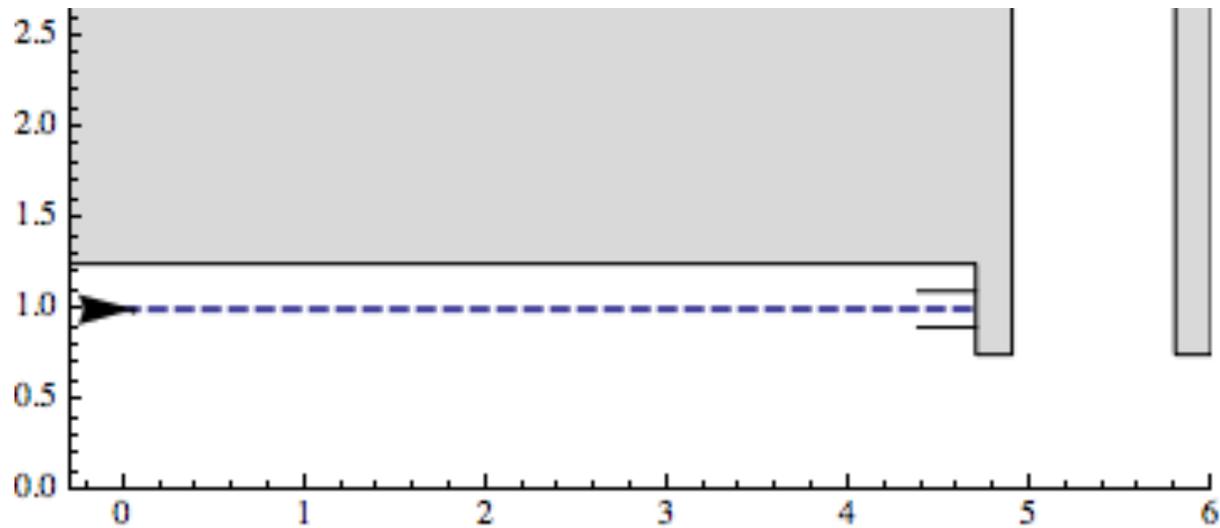
$$s = \frac{1}{2}at_{stop}^2 + v_0t_{stop} + x_0$$

Simulations

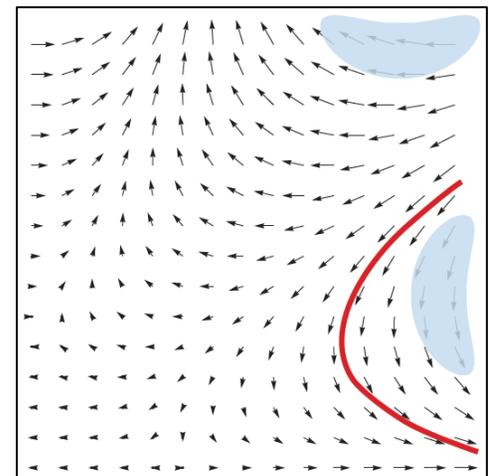


Charging Station

now using differential invariants

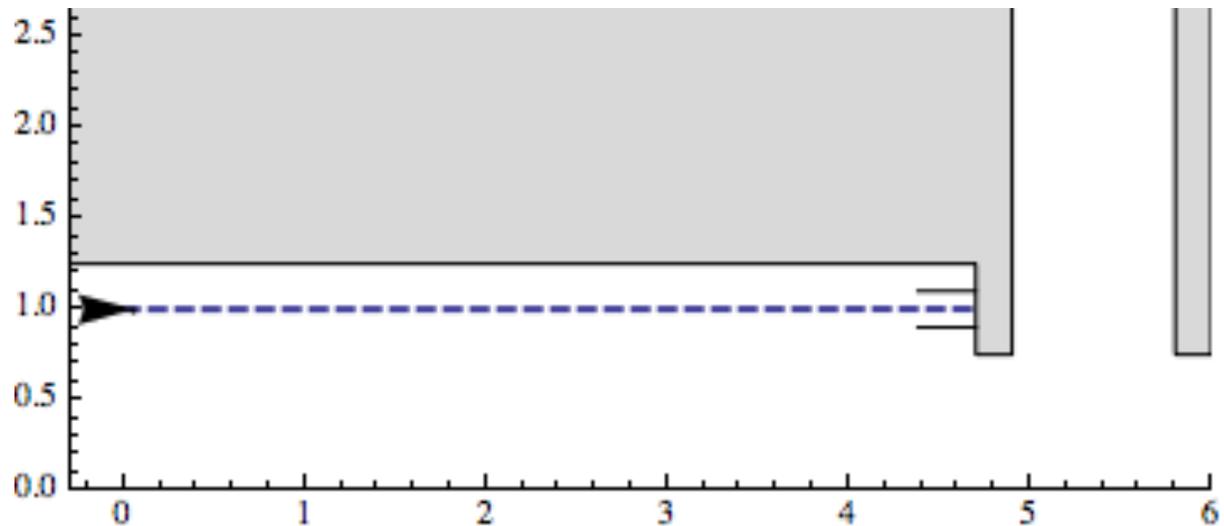


- Suppose we disable the ODE solver.



Charging Station

now using differential invariants



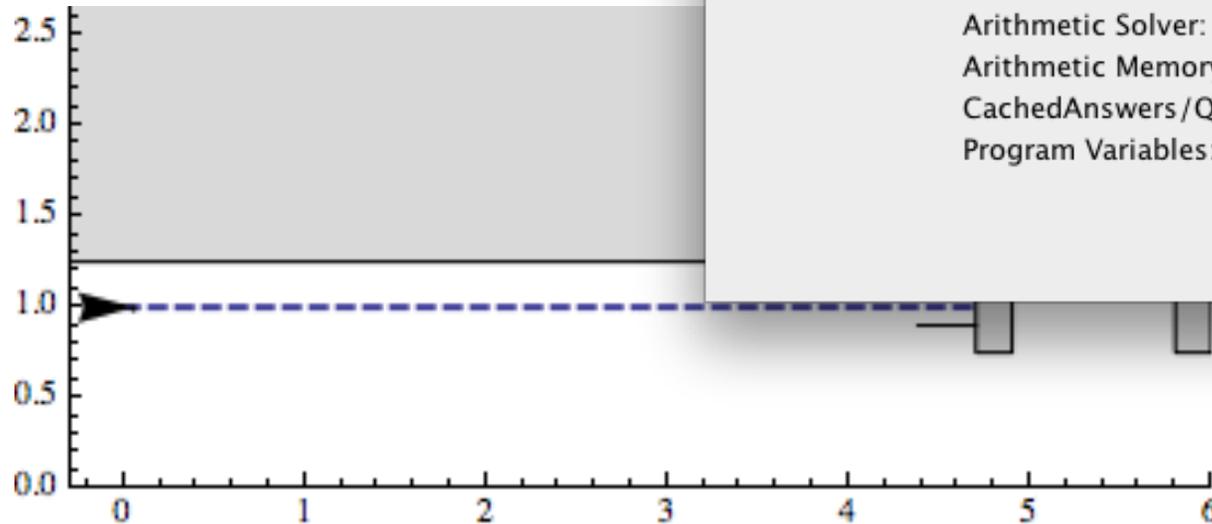
- Suppose we disable the ODE solver.
- The user can cut in solutions, and KeYmaera will check and then use them:

$$x = \frac{1}{2}at^2 + v_0t + x_0 \quad v = at + v_0$$

Demo ▲

Charging Station

now using differential invariants

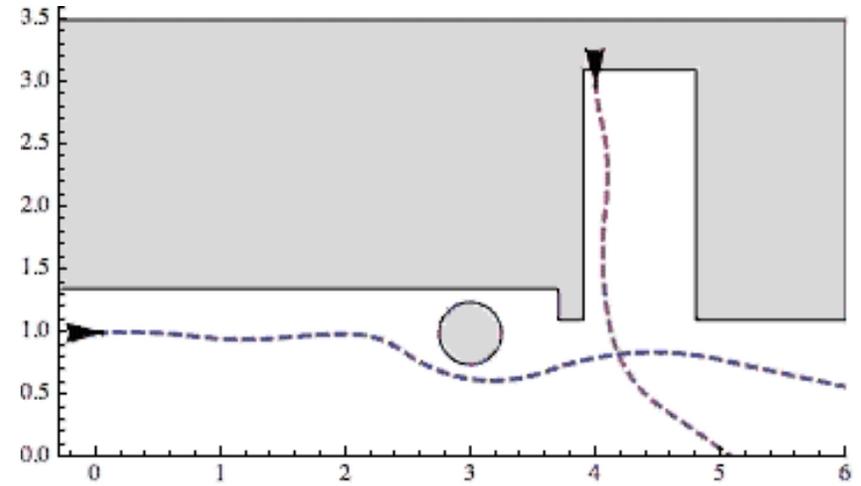
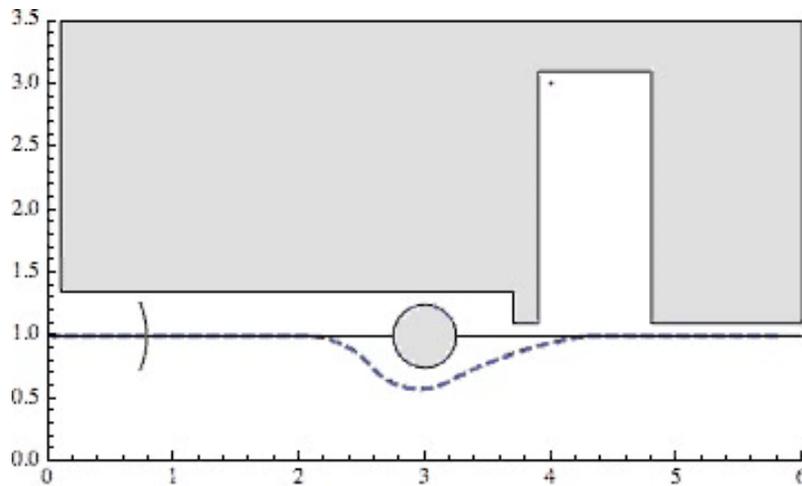


- Suppose we disable the ODE solver.
- The user can cut in solutions, and KeYmaera will check and then use them:

$$x = \frac{1}{2}at^2 + v_0t + x_0 \quad v = at + v_0$$

2D Motion

with static and dynamic obstacles



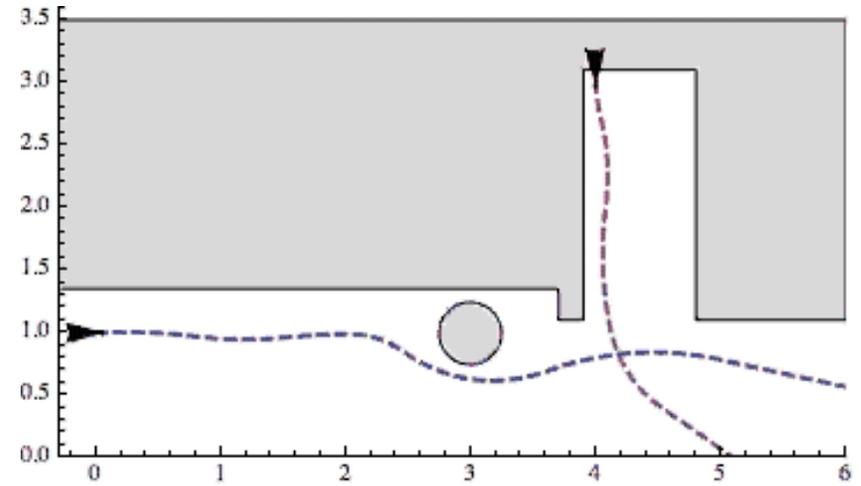
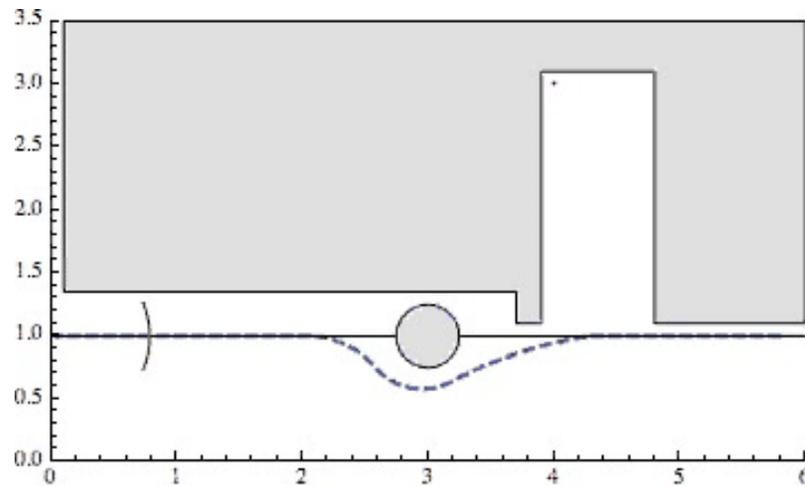
New Challenges:

- 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 ▲

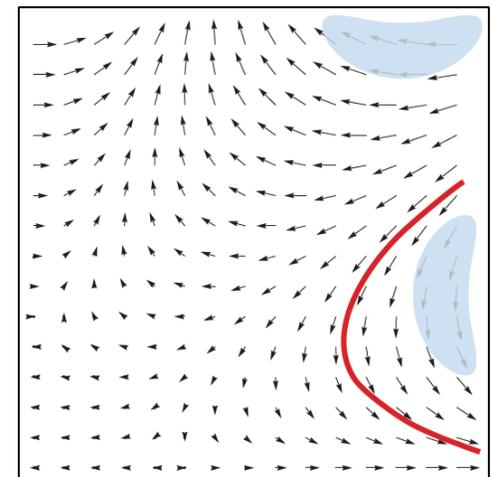
2D Motion

with static and dynamic obstacles



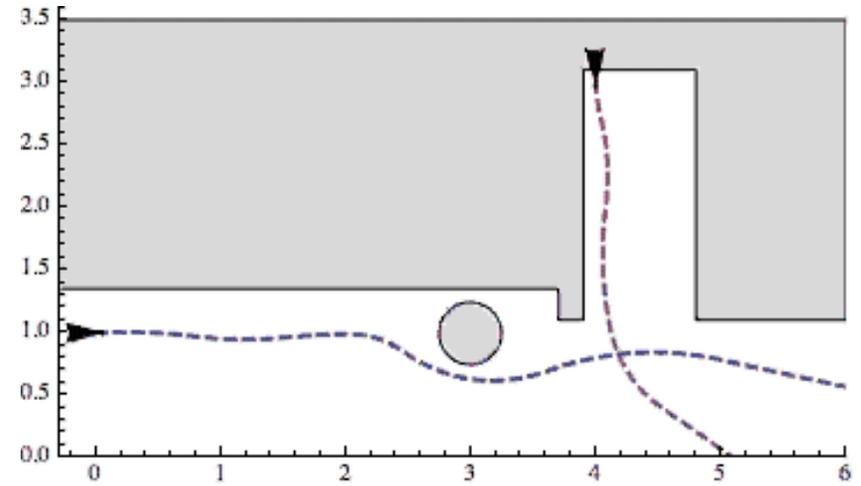
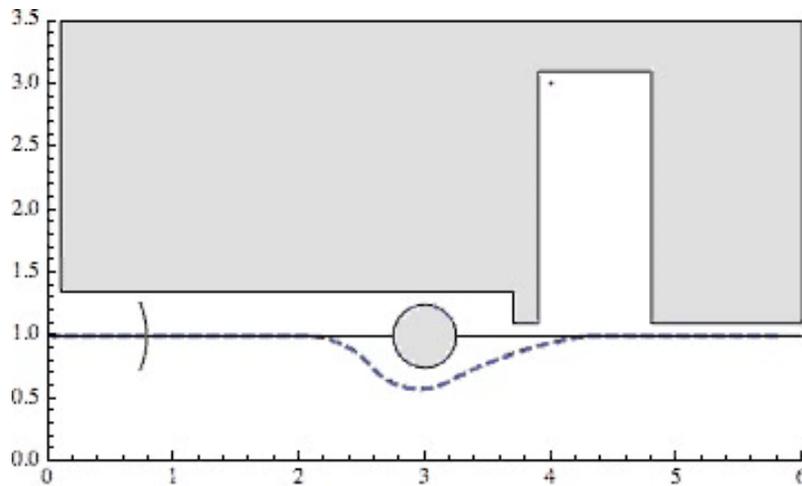
Differential Invariants:

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



2D Motion

with static and dynamic obstacles

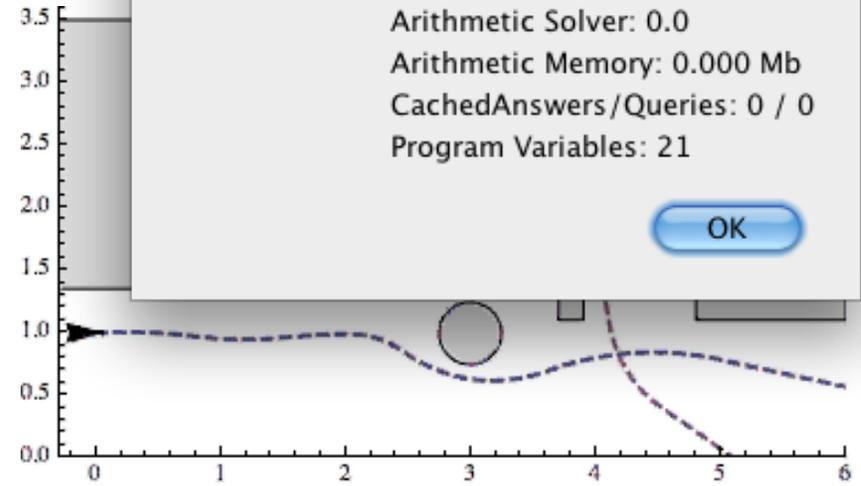
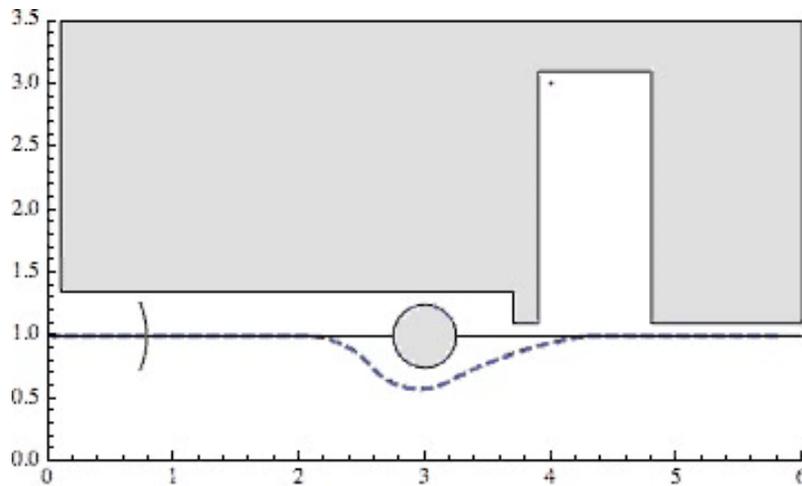


Differential Invariants:

- $v = v_0 + at$
- $d^2 + e^2 = 1$
- $|x - x_0| \leq \frac{1}{2}at^2 + v_0t$
- Similarly for all obstacles

2D Motion

with static and dynamic obstacles

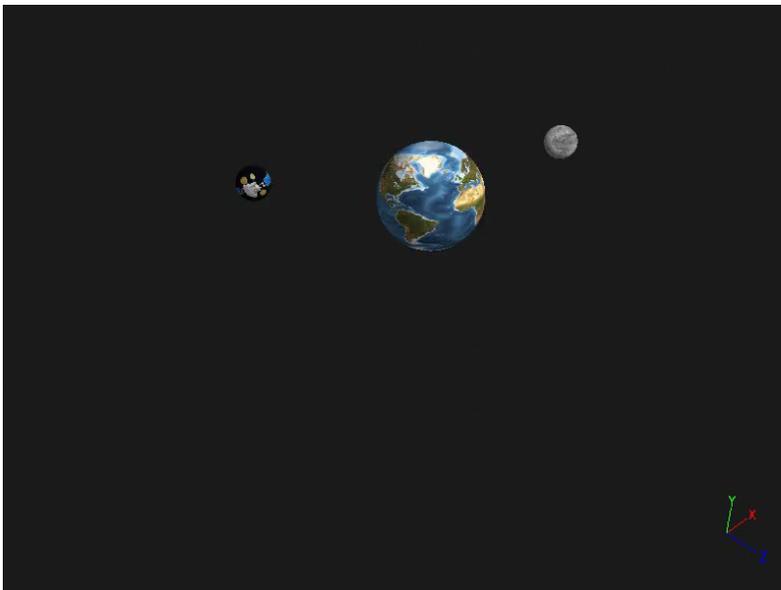


New Challenges:

- 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.



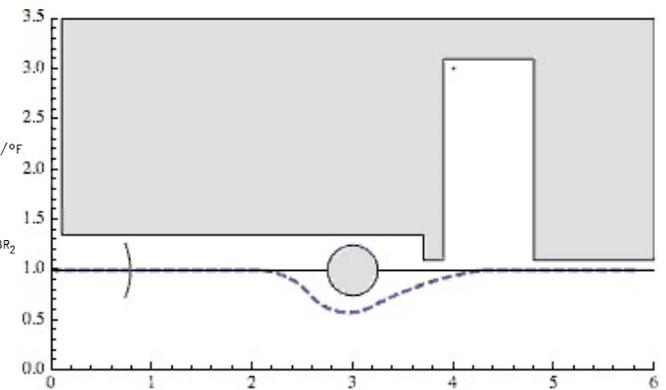
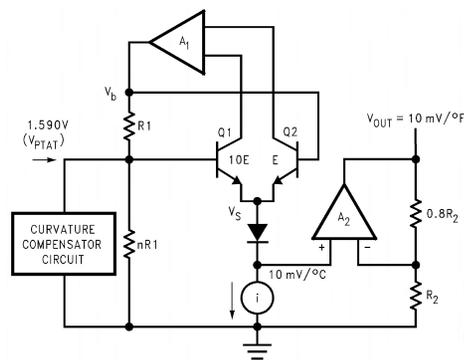
Final Project and Term Paper

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.

The screenshot shows the YouTube channel page for Logical Systems Lab. The browser address bar displays `www.youtube.com/channel/UCRYVHI4XWfN4bEMA3j1oF7g`. The channel banner features a blue square logo with a white star. The channel name "Logical Systems Lab" is prominently displayed with a red "Subscribe" button. Below the banner, navigation tabs for "Videos", "Discussion", and "About" are visible, along with a search icon. A dropdown menu shows "All activities".

The main content area lists two video uploads:

- Logical Systems Lab uploaded a video**
Modeling Discrete Steering
3 weeks ago • 51 views
This video is part of a tutorial series for the Theorem Prover KeYmaera.
<http://symbolaris.com/info/KeYmaera.html>
- Logical Systems Lab uploaded a video**
Tutorial: Abbreviate Rule
1 month ago • 18 views
This video is part of a tutorial series for the Theorem Prover KeYmaera.
<http://symbolaris.com/info/KeYmaera.html>

The left sidebar includes "Popular on YouTube" categories (Music, Sports, Gaming, Education, Movies, TV Shows, News, Live, Spotlight) and "CHANNELS FOR YOU" (Geek & Sundry, FreddieW (Rocke..., Nerdist, YouTube Spotlight, danisnotonfire). A "Sign in now to see your channels and recommendations!" prompt is also present.

The right sidebar lists "Popular channels on YouTube" with "Subscribe" buttons for Smosh, PewDiePie, nigahiga, Hola Soy German (v..., RihannaVEVO, and JennaMarbles.

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.

