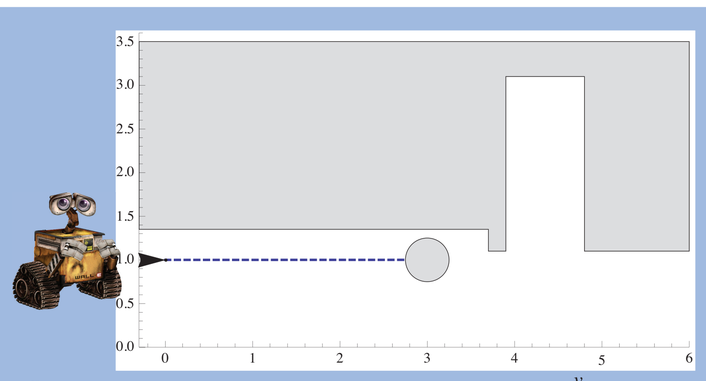
Carnegie Mellon

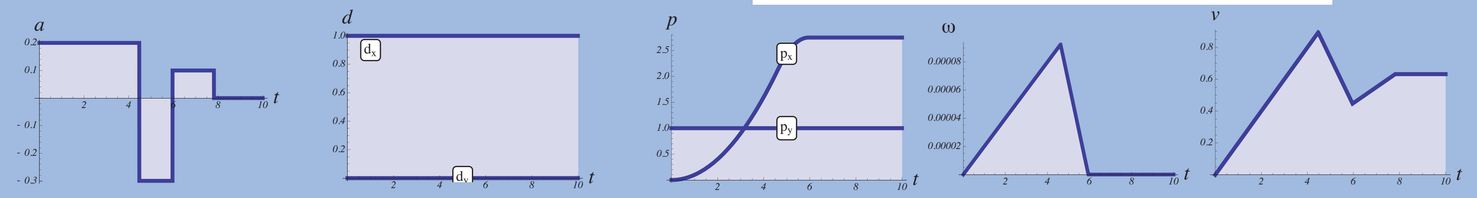
Teaching CPS Foundations With Contracts

André Platzer
Computer Science Department
Carnegie Mellon University

Lab 1

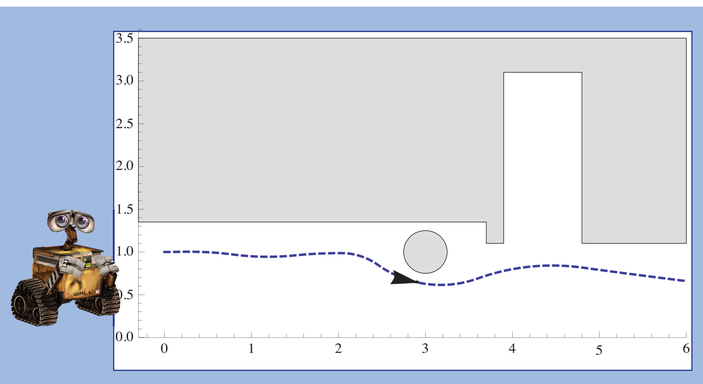
Design & verify controller for a robot avoiding obstacles
- Accelerate / brake
  (discrete dynamics)
- 1D motion
  (continuous dynamics)

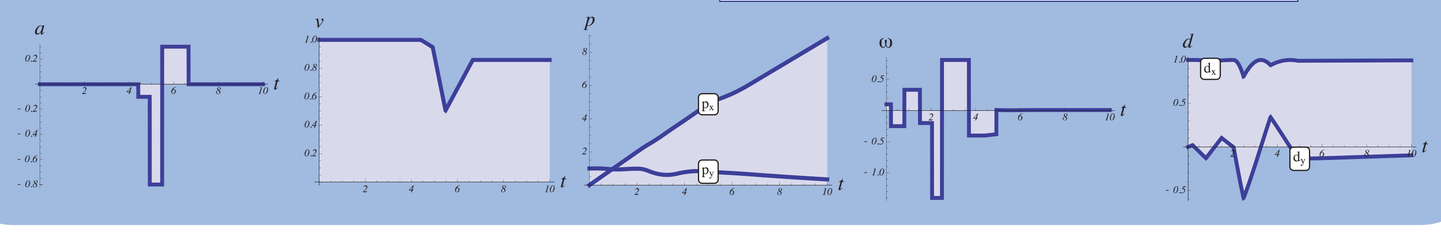




Lab 2

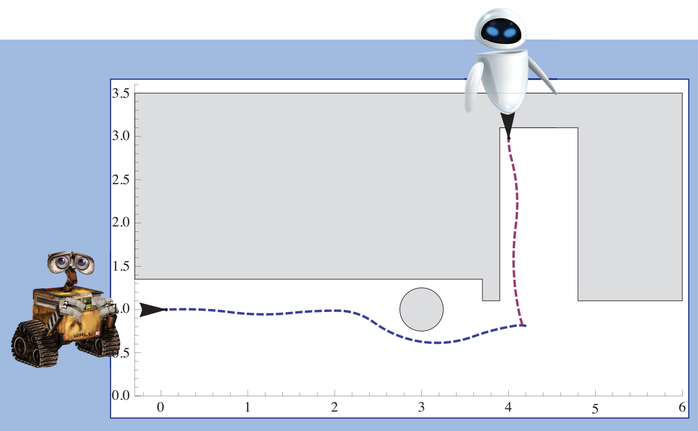
Design & verify controller for a robot avoiding obstacles
- Accel / brake / steer
  (discrete dynamics)
- 2D motion
  (continuous dynamics)

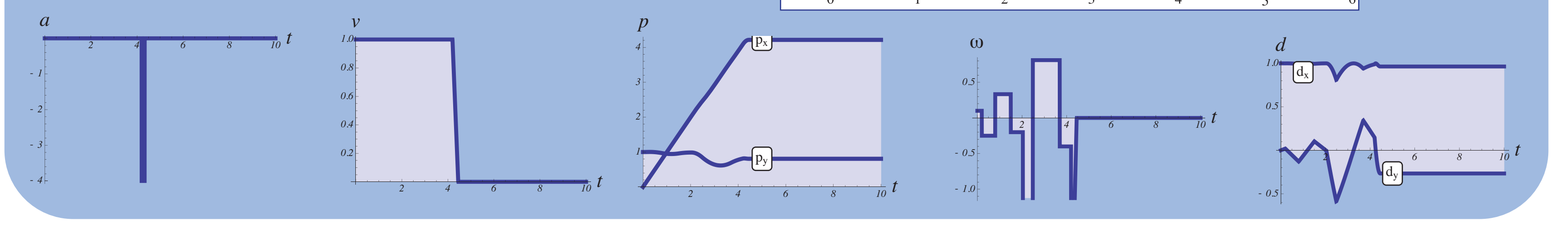




Lab 3

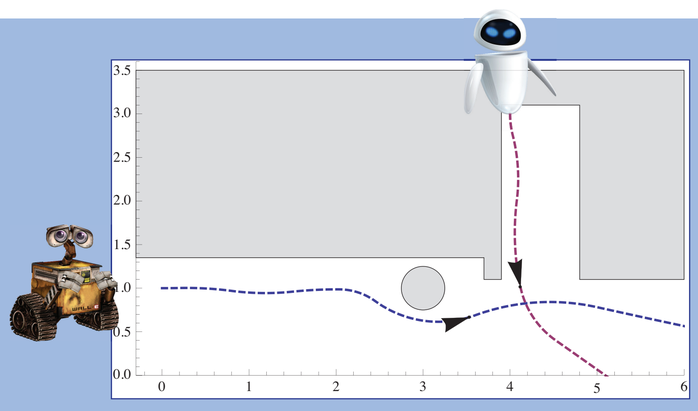
Design & verify controller for a robot avoiding obstacles
- Dynamic obstacles
  (other agents)
- Avoid collisions
  (define safety)

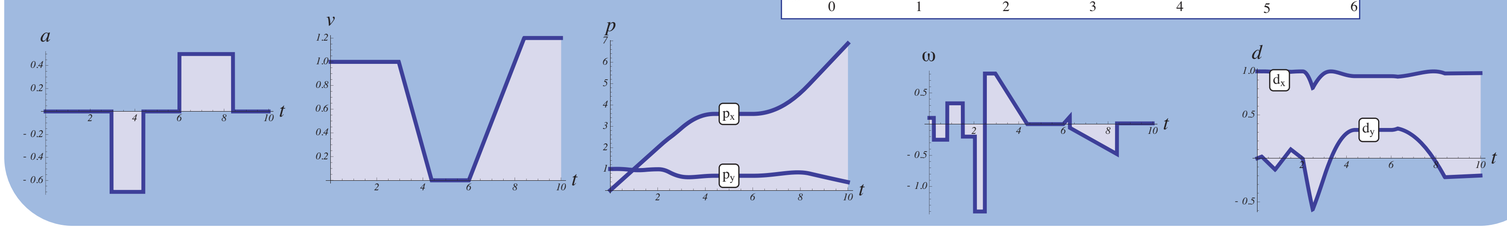




Lab 4

Design & verify controller for a robot avoiding obstacles
- Control robot
  (respect delays)
- Environment interaction
  (obstacles, agents, uncertainty)





pre-/post condition

rigorous reasoning

operational effects

core principles

HP Reveal in layers

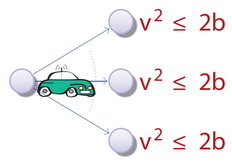
Contracts Reason about CPS

```
@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

differential dynamic logic
dL = FOL_R + DL + HP



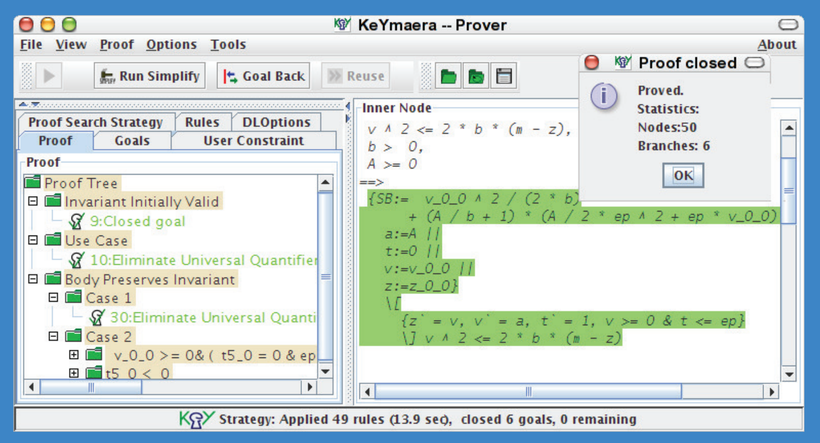
$C \rightarrow [\text{if } (z > SB)\ a := -b;\ z'' = a]\ v^2 \le 2b$

hybrid program

Initial condition

System dynamics

Post condition



http://symbolaris.com/course/fcps13.html