Synthesis for Nonlinear Robots: Abstractions and Revisions

Jonathan DeCastro
Hadas Kress-Gazit

Matthias Rungger
Ayca Balkan
Paulo Tabuada

Rüdiger Ehlers

Cornell University

UCLA

University of Bremen

ExCAPE-ARISE Spring Meeting
Berkeley, CA March 10-11 2014
Open issues:

– Finding an abstraction
– Restricting the environment behaviors

Visit laundry and bedroom infinitely often. If the door is closed, avoid the door region. Infinitely often, the door must be open. The door cannot be closed if you are in the door region.
Abstractions

• Quantized input, state, time
• Non-deterministic
Abstractions

• Quantized input, state, time
• Non-deterministic
• Continuous guarantees
  – Region inflation/deflation
Synthesis for Nonlinear Robots

\[ \dot{\xi}(t) = f(\xi(t), \nu(t)) \]
Effects of the Dynamics

• Inevitable Collisions
Preventing Inevitable Collisions

Existing Sys Safety:

\(\Box(\text{door\_closed} \implies \Diamond \neg\text{door\_reg})\)
Preventing Inevitable Collisions

Add Env Safety:
\[ \Box (\neg \text{door\_closed} \land \Diamond \text{buffered\_door\_reg} \implies \Diamond \neg \text{door\_closed}) \]

Existing Sys Safety:
\[ \Box (\text{door\_closed} \implies \Diamond \neg \text{door\_reg}) \]
Effects of the Dynamics

- *Inevitable Collisions*

- *Environment Falsification:*
  - Robot can force a violation of the environment assumptions
Preventing Environment Falsification

Visit U and R while avoiding the obstacle.

If a given door is closed, avoid that door region.

If in a given door region, do not close that door.

DoorU is closed if and only if DoorR is open.

Add Sys Safety:  □  → Red
Under-Actuated Unicycle Example
Thank You!

jad455@cornell.edu
hadaskg@cornell.edu
verifiablerobotics.com