The KeYmaera X Theorem Prover for Hybrid Systems

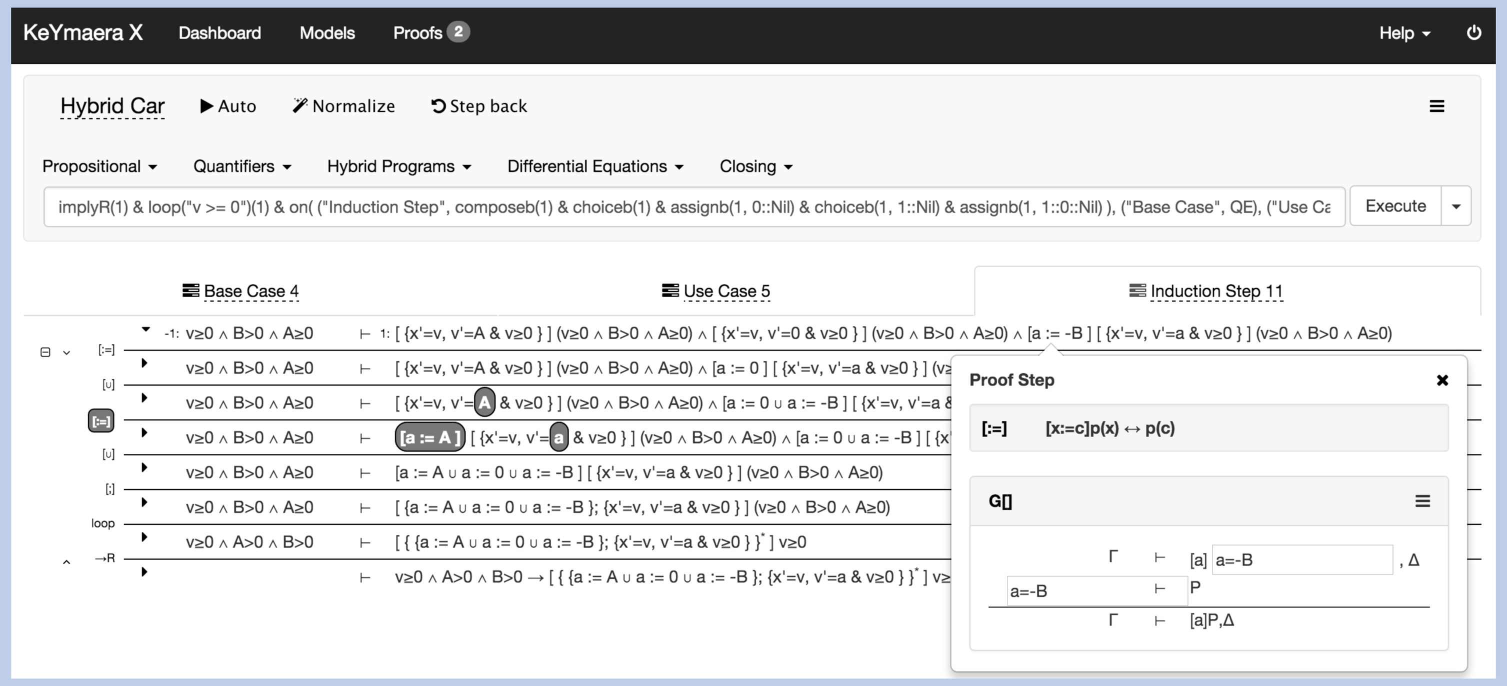
Logical Systems Lab, Carnegie Mellon University

Abstract

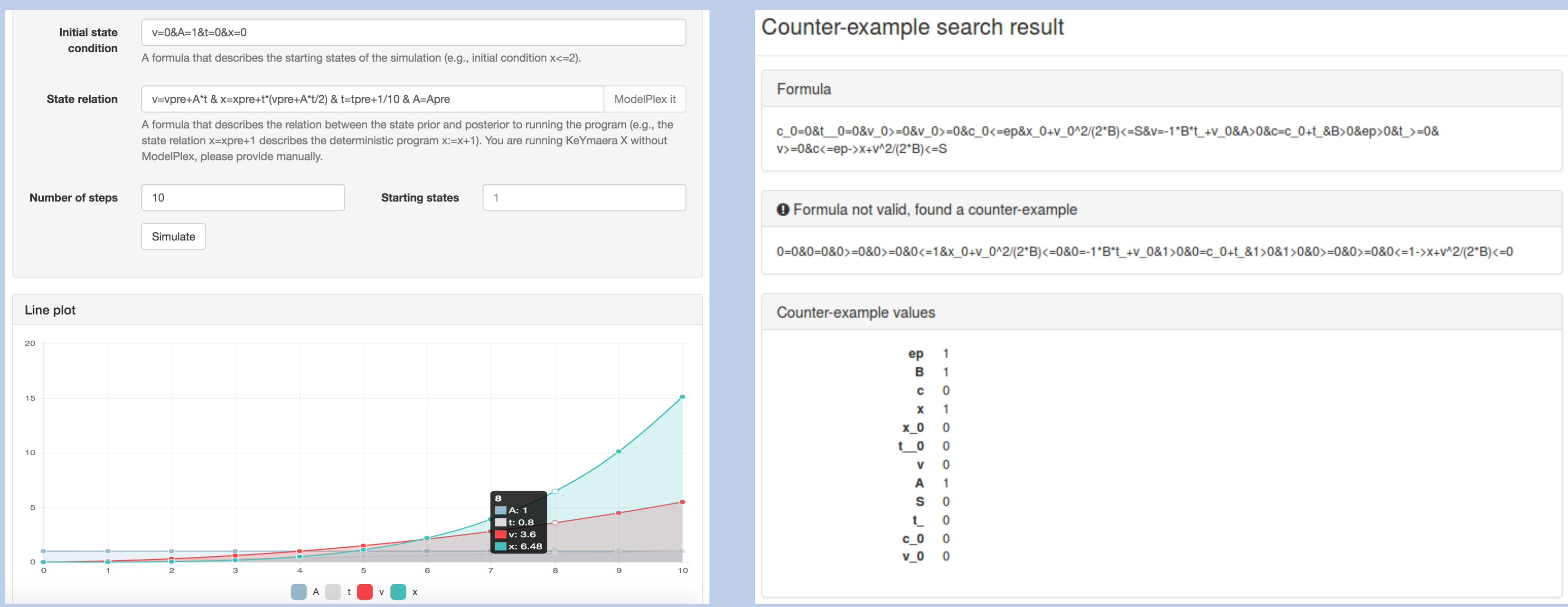
KeYmaera X is a theorem prover for specifying and verifying correctness properties of systems that mix discrete and continuous dynamics (hybrid systems). KeYmaera X implements differential dynamic logic and provides a high degree of control over automated proof search.

Overview

KeYmaera X can automatically prove safety and liveness properties for many classes of hybrid systems.

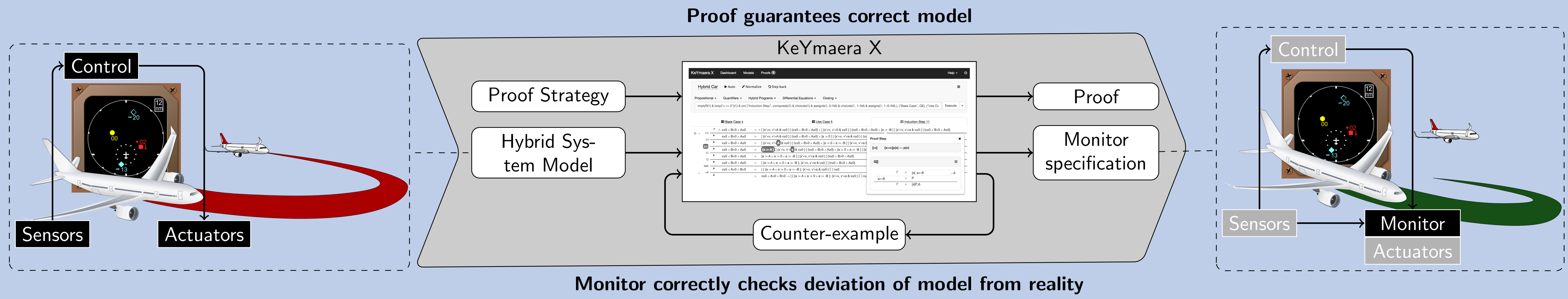


Automatic verification is not always possible so KeYmaera X assists with partially interactive proofs.



Counter-example generation and simulation support verification tasks.

Verification and Monitor Synthesis in KeYmaera X



The KeYmaera X user interface exposes tools that provide assistance during verification tasks:

- Automatic and customized proof search
- Interactive proving with suggestions
- Simulation and counter-example generation

Correct runtime monitors can be extracted after completing a verification task.

Example: Tactical Theorem Proving for a Simple Hybrid System

The following d$\mathcal{L}$ formula describes a safety property for a car model.

$$\underbrace{v \geq 0 \land A > 0}_{precondition} \rightarrow [(\underbrace{a := A \cup a := 0}_{ctrl} \; ; \; \underbrace{\{p' = v, \; v' = a\}}_{plant})^*] \; \underbrace{v \geq 0}_{postcondition}$$

The general-purpose tactics shipped with KeYmaera X will discover a proof for this model automatically. An efficient tactic specialized to this problem can be implemented using the tactic combinator library:

```
implyR(1) & loop({`v>=0`}, 1) <(
  master,
  master,
  implyR(1) & composeb(1) & choiceb(1) & andR(1) <(
    assignb(1) & diffSolve(1) & master,
    master
  )
)
```

Try KeYmaera X!

KeYmaera X is available for download at keymaeraX.org

Carnegie Mellon University