



# The KeYmaera X Theorem Prover for Hybrid Systems

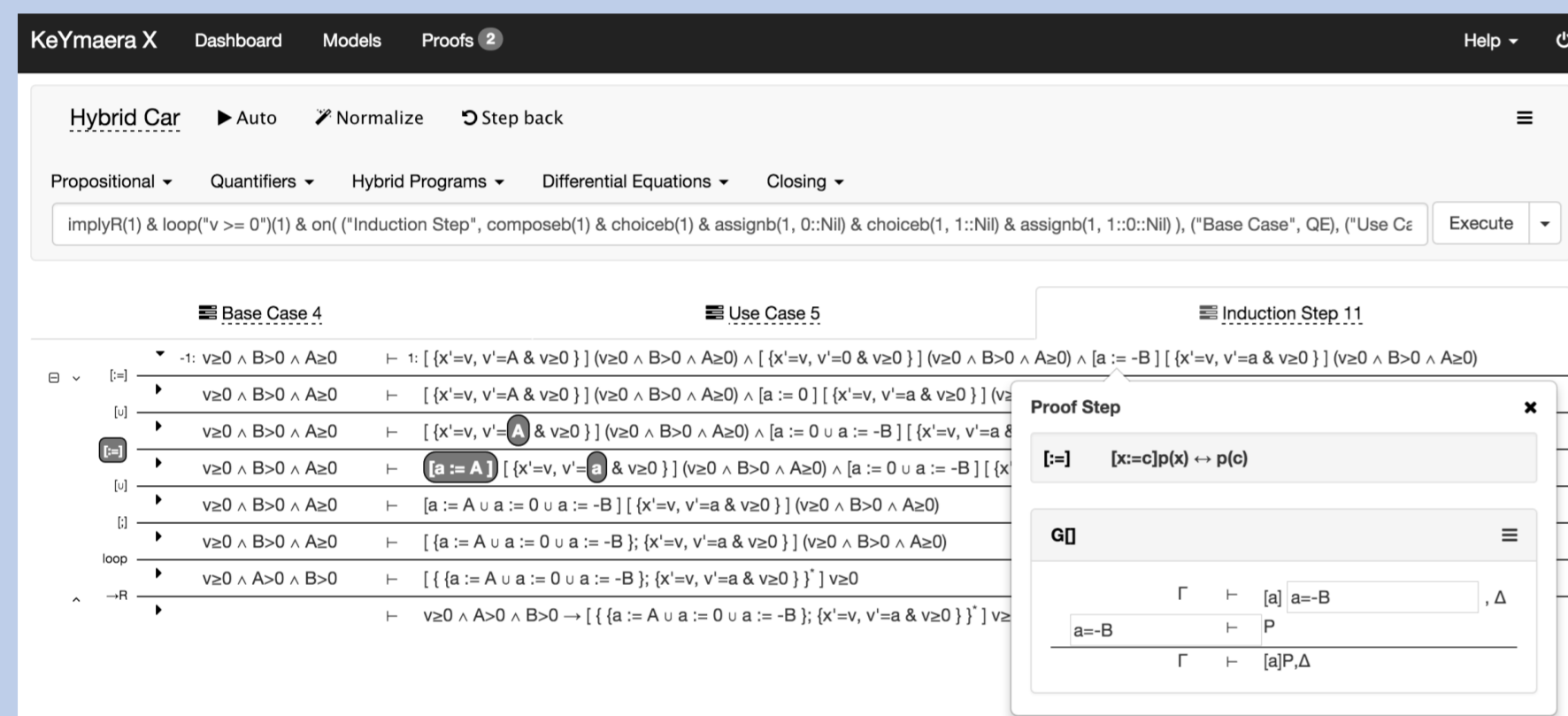
Logical Systems Lab, Carnegie Mellon University

## Abstract

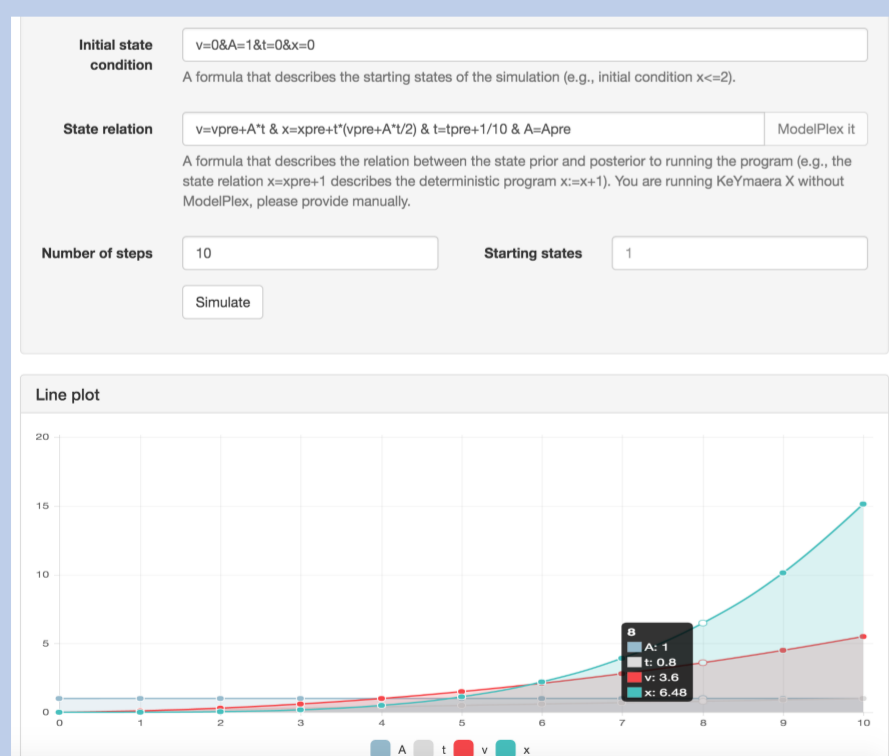
KeYmaera X is a theorem prover for specifying and verifying correctness properties of systems that mix discrete and continuous dynamics (hybrid systems). KeYmaera X implements differential dynamic logic and provides a high degree of control over automated proof search.

## 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 search result

Formula

$$c_0=0 \wedge \text{dist}_0=0 \wedge \text{dist}_1=1 \wedge \text{dist}_2=1 \wedge \text{dist}_3=1 \wedge \text{dist}_4=1 \wedge \text{dist}_5=1 \wedge \text{dist}_6=1 \wedge \text{dist}_7=1 \wedge \text{dist}_8=1 \wedge \text{dist}_9=1 \wedge \text{dist}_{10}=1 \wedge \text{dist}_{11}=1 \wedge \text{dist}_{12}=1 \wedge \text{dist}_{13}=1 \wedge \text{dist}_{14}=1 \wedge \text{dist}_{15}=1 \wedge \text{dist}_{16}=1 \wedge \text{dist}_{17}=1 \wedge \text{dist}_{18}=1 \wedge \text{dist}_{19}=1 \wedge \text{dist}_{20}=1 \wedge \text{dist}_{21}=1 \wedge \text{dist}_{22}=1 \wedge \text{dist}_{23}=1 \wedge \text{dist}_{24}=1 \wedge \text{dist}_{25}=1 \wedge \text{dist}_{26}=1 \wedge \text{dist}_{27}=1 \wedge \text{dist}_{28}=1 \wedge \text{dist}_{29}=1 \wedge \text{dist}_{30}=1 \wedge \text{dist}_{31}=1 \wedge \text{dist}_{32}=1 \wedge \text{dist}_{33}=1 \wedge \text{dist}_{34}=1 \wedge \text{dist}_{35}=1 \wedge \text{dist}_{36}=1 \wedge \text{dist}_{37}=1 \wedge \text{dist}_{38}=1 \wedge \text{dist}_{39}=1 \wedge \text{dist}_{40}=1 \wedge \text{dist}_{41}=1 \wedge \text{dist}_{42}=1 \wedge \text{dist}_{43}=1 \wedge \text{dist}_{44}=1 \wedge \text{dist}_{45}=1 \wedge \text{dist}_{46}=1 \wedge \text{dist}_{47}=1 \wedge \text{dist}_{48}=1 \wedge \text{dist}_{49}=1 \wedge \text{dist}_{50}=1 \wedge \text{dist}_{51}=1 \wedge \text{dist}_{52}=1 \wedge \text{dist}_{53}=1 \wedge \text{dist}_{54}=1 \wedge \text{dist}_{55}=1 \wedge \text{dist}_{56}=1 \wedge \text{dist}_{57}=1 \wedge \text{dist}_{58}=1 \wedge \text{dist}_{59}=1 \wedge \text{dist}_{60}=1 \wedge \text{dist}_{61}=1 \wedge \text{dist}_{62}=1 \wedge \text{dist}_{63}=1 \wedge \text{dist}_{64}=1 \wedge \text{dist}_{65}=1 \wedge \text{dist}_{66}=1 \wedge \text{dist}_{67}=1 \wedge \text{dist}_{68}=1 \wedge \text{dist}_{69}=1 \wedge \text{dist}_{70}=1 \wedge \text{dist}_{71}=1 \wedge \text{dist}_{72}=1 \wedge \text{dist}_{73}=1 \wedge \text{dist}_{74}=1 \wedge \text{dist}_{75}=1 \wedge \text{dist}_{76}=1 \wedge \text{dist}_{77}=1 \wedge \text{dist}_{78}=1 \wedge \text{dist}_{79}=1 \wedge \text{dist}_{80}=1 \wedge \text{dist}_{81}=1 \wedge \text{dist}_{82}=1 \wedge \text{dist}_{83}=1 \wedge \text{dist}_{84}=1 \wedge \text{dist}_{85}=1 \wedge \text{dist}_{86}=1 \wedge \text{dist}_{87}=1 \wedge \text{dist}_{88}=1 \wedge \text{dist}_{89}=1 \wedge \text{dist}_{90}=1 \wedge \text{dist}_{91}=1 \wedge \text{dist}_{92}=1 \wedge \text{dist}_{93}=1 \wedge \text{dist}_{94}=1 \wedge \text{dist}_{95}=1 \wedge \text{dist}_{96}=1 \wedge \text{dist}_{97}=1 \wedge \text{dist}_{98}=1 \wedge \text{dist}_{99}=1 \wedge \text{dist}_{100}=1$$

Counter-example values

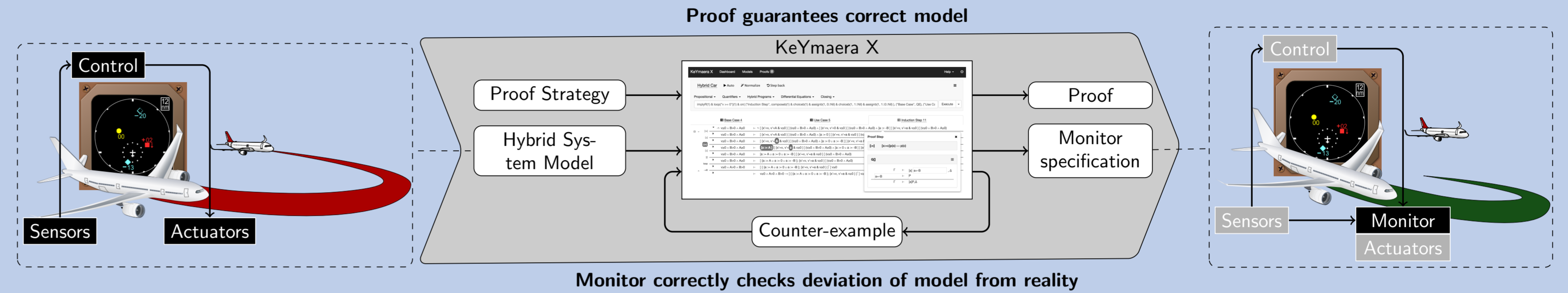
```

ep 1
B 1
c 0
x 1
x_0 0
L_0 0
v 0
A 1
B 0
L 0
c_0 0
v_0 0

```

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 dL formula describes a safety property for a car model.

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

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](http://keymaeraX.org)