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.

Example: Tactical Theorem Proving for a Simple Hybrid System

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

\[ v \geq 0 \land A > 0 \rightarrow \left[ \{ a := A \cup a := 0 ; \{ p = v, v' = a \} \} \right] \]

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:

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

Try KeYmaera X!

KeYmaera X is available for download at keymaeraX.org