Abstract

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

Architectural Overview

KeYmaera X features a minimal core that isolates soundness-critical axiomatic reasoning. Tactics built on top of this core drive automated proof search, and a modern web-based front-end provides a clean interface for both interactive and automated proving.

Core Features of KeYmaera X

- KeYmaera X provides a list of applicable tactics when a goal is selected.
- A list of previously executed tactics provides an overview of the proof history.
- User-written tactics may be applied to both entire problems and subproblems.

KeYmaera X supports both interactive and automated proof search for hybrid systems models.

- The web-based user interface (pictured above) supports interactive proving and exposes built-in general-purpose proof search tactics that suffice for many models.
- Domain or problem-specific proof search techniques are implemented using a tactic combinator library.
- An isolated soundness-critical core ensures that bugs in custom tactics cannot introduce unsoundness.

Tactical Theorem Proving for Hybrid Systems

The following dL formula describes a safety property for a car model.

\[ v \geq 0 \land A > 0 \rightarrow [(a := A \cup a := 0 ; \{p' = v, v' = a\})^*] \quad v \geq 0 \]

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:

```
ImplyRight & Loop("v\geq0".asFormula) & onLabel(
  "base\_case", Master),
("induction\_step", ImplyRight & Seq & Choice & AndRight && (Assign & ODESolve & Master,
  Assign & ODESolve & Master)),
("use\_case", Master)
```

Try KeYmaera X!

KeYmaera X is available for download at keymaerax.org