Recent KIV developments

Castellon, September 17th, 2002

Michael Balser, Christoph Duelli

Overview

Jaundice application gave rise to a lot of improvements

KIV improvements

- Support for complex operators
- More comfortable proofs ($\Rightarrow$ high level rules)
- Automation (heuristics)

Complex operators

Requirements

- Modular
- Sound
- Complete

Calculus

- Strategy: Symbolic execution of operators

$\Rightarrow$ More complete set of (basic) rules

High Level Rules

Use of basic rules not suitable for large applications

Concurrent goals

- Understandability
- Efficiency

Heuristics

Automatic application of rules

- In theory: Automation of symbolic execution possible
- Important for large proofs
- In practice: Implementation effort

Example

Lemma `pti-no-tsb-readings`

July: Manual proof with roughly 100 proof steps

September: Fully automatic proof

Lemma `rt-indicator-7`

- Lemma far more complex
- Automation essential
- Manual repetition of proof not possible $\Rightarrow$ Reuse
- Analysis of proof attempt requires fine tuned complex rules
- Strategy of generalization gives rise to lemmas

Demonstration

Lemma `pti-no-tsb-readings`

Heuristics 1

- simplifier
- tl apply induction
- tl induction simple
- tl step

Heuristics 2

- tl simple
- simplifier
- tl apply induction
- tl induction simple
- tl case distinction
- itl case distinction
- tl unwind
- tl step

Conclusion

- Tool support more complex than expected
- Asbru application gave push to development
- Potential improvements
  - ⋆ More comfortable rules
  - ⋆ Fine tuned heuristics
  - ⋆ Generalization
  - ⋆ Reuse of proofs

Thank you for trying to do proofs!