Isabelle Supports Rodin

Matthias Schmalz

Information Security Group, ETH Zurich

April 28th, 2011

Problem

Problem:
discharge more proof obligations automatically
(in Event-B / Rodin)

Approaches

1. improve one of Rodin's existing theorem provers
   - PP/ML: source code unavailable
   - NewPP: complicated design, unsoundness issues
2. develop a new theorem prover
   - duplication of effort
   - huge investment of time / late results
3. connect Rodin to some other theorem prover
   - requires (non-trivial?) translation between logics
   - take advantage of other people's work

Approaches

1. improve one of Rodin's existing theorem provers
   - PP/ML: source code unavailable
   - NewPP: complicated design, unsoundness issues
2. develop a new theorem prover
   - duplication of effort
   - huge investment of time / late results
3. connect Rodin to some other theorem prover
   - requires (non-trivial?) translation between logics
   - take advantage of other people's work

Which Theorem Prover?

First Experiments

Experiments with first-order provers (E, Vampire):

- need to implement several optimizations, e.g.:

  rewrite $\forall x \cdot x = t \Rightarrow \varphi(x)$ to $\varphi(t)$.

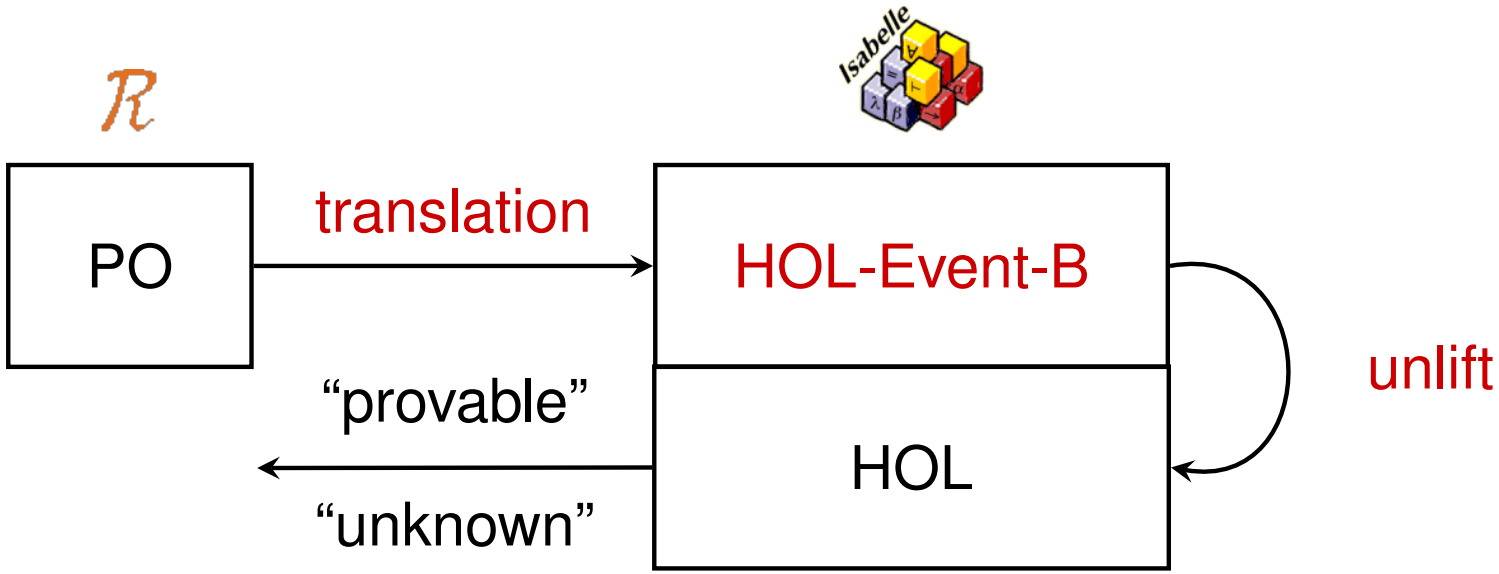
- besides, need to:
  - translate types away
  - translate from three-valued to two-valued logic

- these transformations are hard to implement (in Rodin)
- even harder to implement transformations soundly

Which Theorem Prover?

Current Approach

Current Approach: link-up to Isabelle/HOL



Benefits of Using Isabelle

Benefits of using Isabelle/HOL:

- some automatization is already available
- automatization is easy to adapt:

  e.g., easy to instruct the simplifier to rewrite $\forall x \cdot x = t \Rightarrow \varphi(x)$ to $\varphi(t)$.

- transformations are sound by construction (LCF)
- link-ups to ATPs (E, Spass, Vampire, Z3, ...)

Tasks

- Understand intended semantics of Event-B's logic
- Define "counterparts" of Event-B operators in Isabelle/HOL:
  $\lhd, \mapsto, \rightarrow, \mathrm{dom}, \mathrm{ran}, \ldots$
- Unlift: translate from three-valued to two-valued logic
- Instrument Isabelle's automated tactics:
  e.g., for reasoning about functions as relations
- Case studies / fine-tuning

Tasks

- Understand intended semantics of Event-B's logic ✓
- Define "counterparts" of Event-B operators in Isabelle/HOL:
  $\lhd, \mapsto, \rightarrow, \mathrm{dom}, \mathrm{ran}, \ldots$ ✓
- Unlift: translate from three-valued to two-valued logic (✓)
- Instrument Isabelle's automated tactics: ×
  e.g., for reasoning about functions as relations
- Case studies / fine-tuning ×

Unlifting

Limitations of State of the Art

$\vdash f(f^{-1}(x)) = x$

is “magically” valid,

Unlifting

Limitations of State of the Art

$\vdash f(f^{-1}(x)) = x$

is “magically” valid,
because it is equivalent to

$f^{-1} \in R \pfun S$,

$x \in \mathrm{dom}(f^{-1})$,

$f \in S \pfun R$,

$f^{-1}(x) \in \mathrm{dom}(f)$

$\vdash$

$f(f^{-1}(x)) = x$

Unlifting

Limitations of State of the Art

$\vdash f(f^{-1}(x)) = x$

is “magically” valid,
because it is equivalent to

$f^{-1} \in R \pfun S$,

$x \in \mathrm{dom}(f^{-1})$,

$f \in S \pfun R$,

$f^{-1}(x) \in \mathrm{dom}(f)$

$\vdash$

$f(f^{-1}(x)) = x$

Dilemma:

- extra hypotheses are needed for completeness
- subterm duplication
- redundant hypotheses

Unlifting

Limitations of State of the Art

$\vdash f(f^{-1}(x)) = x$

is “magically” valid,
because it is equivalent to

$f^{-1} \in R \pfun S$,

$x \in \mathrm{dom}(f^{-1})$,

$f \in S \pfun R$,

$f^{-1}(x) \in \mathrm{dom}(f)$

$\vdash$

$f(f^{-1}(x)) = x$

Dilemma:

- extra hypotheses are needed for completeness
- subterm duplication
- redundant hypotheses

Unlifting

Limitations of State of the Art

$\vdash f(f^{-1}(x)) = x$

is “magically” valid,
because it is equivalent to

$f^{-1} \in R \pfun S$,

$x \in \mathrm{dom}(f^{-1})$,

$f \in S \pfun R$,

$f^{-1}(x) \in \mathrm{dom}(f)$

$\vdash$

$f(f^{-1}(x)) = x$

Dilemma:

- extra hypotheses are needed for completeness
- subterm duplication
- redundant hypotheses

Results So Far

- Written specification of Event-B's logic
  (syntax, semantics, proofs, conservative extensions).
- Translation from Event-B to Isabelle/HOL
- Unlifting: translation from three-valued to two-valued logic

First application:

- Reasoning about soundness of Event-B proof rules

Summary

- Goal: enhance Rodin's theorem proving capabilities
- Approach: use Isabelle/HOL, mainly because it is easy to adapt Isabelle's automated tactics
- Results: specification of Event-B's logic, unlifting

Future work:

- fine-tuning and case studies