Developing in Event-B. Modelling and Proving

Proof Hints for Event-B

Thai Son Hoang

Institute of Information Security
Swiss Federal Institute of Technology Zürich (ETH Zürich)

Rodin Workshop, Fontainebleau, France
28th-29th February 2012

Interactive Proofs v.s Automatic Proofs

- Maintenance of interactive proofs is difficult.
- Better rate of automatic proofs
  - Better automatic provers (Isabelle, SMT)
  - Better proof profiles.
  - This talk: “Improve” the existing model.

Existing Proof Hints in Event-B/Rodin Platform

- Theorems (add hypothesis)
- Witnesses (existential instantiation)
- Guard selection (select hypotheses)

Idea

Expose more proof information in the model: “proof hints”
Hypotheses Selection (1/2)

**inv1**: \( x \in \mathbb{N} \)

**inv2**: \( x \neq 0 \Rightarrow y \in \mathbb{N} \)

**Modified inv1**

\[ \vdash x \neq 0 \Rightarrow y \in \mathbb{N} \]

\[ x \in \mathbb{N} \]

\[ x \in \{1, 2\} \]

\[ y + 1 \in \mathbb{N} \]

**Cons for using theorem**

- Copy/paste.
- An extra proof obligation (trivially discharged).

Selected hypotheses: **inv1** and **grd1**

**inv2** is required, added as a guard theorem.

Hypotheses Selection (2/2)

**inv2**

**inv1**

**grd1**

Cons for using theorem

- Copy/paste.
- An extra proof obligation (trivially discharged).

Do Case (1/3)

**inv1**: \( a \leq c \)

**inv2**: \( a \neq 1 \Rightarrow b = a + 1 \)

**inv3**: \( a = 1 \Rightarrow b \leq c \)

**Proof by cases**:

- \( a = 1 \)
- \( a \neq 1 \)

Do Case (2/3)

**set_a**

**set_b**

**set**

Refines **set_a**, **set_b**

Duplication of proof obligations.

Artificial merging step.
Do Case (3/3)

```
set
begin
a := b
case-split
a = 1 for inv1
end
```

Summary

- Using information of interactive proofs to “improve” the model.
- Hints (proof information) help with proof automation.
- Hints help to understand model better.
- How far should we go in terms of exposing proof information in the model?
- A plug-in (a reasoner) that “interprete” proof hints.