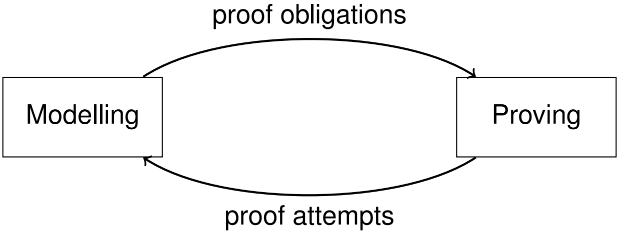
Proof Hints for Event-B

Thai Son Hoang

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

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

Developing in Event-B. Modelling and Proving



- Proof obligations are generated from formal models.
- Failed proof attempts required to the models to be fixed.
- How about successful attempts, in particular, interactive proofs?

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.

Idea

Expose more proof information in the model: "proof hints"

Existing Proof Hints in Event-B/Rodin Platform

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

Hypotheses Selection (1/2)

invariants:
inv1 : $x \in \mathbb{N}$
inv2 : $x \neq 0 \Rightarrow y \in \mathbb{N}$

set
when
grd1 : $x \in \{1, 2\}$
then
act1 : $x := y + 1$
end

inv2
inv1
grd1
$\vdash$
Modified **inv1**

$x \neq 0 \Rightarrow y \in \mathbb{N}$ $x \in \mathbb{N}$ $x \in \{1, 2\}$ $\vdash$ $y + 1 \in \mathbb{N}$	set/**inv1**/INV

- Selected hypotheses: **inv1** and **grd1**
- **inv2** is required, added as a guard theorem.

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Hypotheses Selection (1/2)

invariants:
inv1 : $x \in \mathbb{N}$
inv2 : $x \neq 0 \Rightarrow y \in \mathbb{N}$

set
when
grd1 : $x \in \{1, 2\}$
then
act1 : $x := y + 1$
end

inv2
inv1
grd1
$\vdash$
Modified **inv1**

$x \neq 0 \Rightarrow y \in \mathbb{N}$ $x \in \mathbb{N}$ $x \in \{1, 2\}$ $\vdash$ $y + 1 \in \mathbb{N}$	set/**inv1**/INV

- Selected hypotheses: **inv1** and **grd1**
- **inv2** is required, added as a guard theorem.

Hypotheses Selection (1/2)

invariants:
inv1 : $x \in \mathbb{N}$
inv2 : $x \neq 0 \Rightarrow y \in \mathbb{N}$

set
when
grd1 : $x \in \{1, 2\}$
then
act1 : $x := y + 1$
end

inv2
inv1
grd1
$\vdash$
Modified **inv1**

$x \neq 0 \Rightarrow y \in \mathbb{N}$
$x \in \mathbb{N}$
$x \in \{1, 2\}$
$\vdash$
$y + 1 \in \mathbb{N}$

set/**inv1**/INV

- Selected hypotheses: **inv1** and **grd1**
- **inv2** is required, added as a guard theorem.

Hypotheses Selection (1/2)

invariants:
inv1 : $x \in \mathbb{N}$
inv2 : $x \neq 0 \Rightarrow y \in \mathbb{N}$

set
when
grd1 : $x \in \{1, 2\}$
thm1 : $x \neq 0 \Rightarrow y \in \mathbb{N}$
then
act1 : $x := y + 1$
end

inv2
inv1
grd1
⊢
Modified **inv1**

$x \neq 0 \Rightarrow y \in \mathbb{N}$
$x \in \mathbb{N}$
$x \in \{1, 2\}$
⊢
$y + 1 \in \mathbb{N}$

set/**inv1**/INV

- Selected hypotheses: **inv1** and **grd1**
- **inv2** is required, added as a guard theorem.

ETH Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Hypotheses Selection (2/2)

set
  when
    grd1 : $x \in \{1, 2\}$
    thm1 : $x \neq 0 \Rightarrow y \in \mathbb{N}$
  then
    act1 : $x := y + 1$
  end

set
  when
    grd1 : $x \in \{1, 2\}$
  then
    act1 : $x := y + 1$
  select
    inv2
  end

Cons for using theorem

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

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Hypotheses Selection (2/2)

set
  when
    grd1 : $x \in \{1, 2\}$
    thm1 : $x \neq 0 \Rightarrow y \in \mathbb{N}$
  then
    act1 : $x := y + 1$
  end

set
  when
    grd1 : $x \in \{1, 2\}$
  then
    act1 : $x := y + 1$
  select
    inv2
  end

Cons for using theorem

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

invariants:
- **inv1** : $a \leq c$
- **inv2** : $a \neq 1 \Rightarrow b = a + 1$
- **inv3** : $a = 1 \Rightarrow b \leq c$

set
begin
$a := b - 1$
end

$a \leq c$ $a \neq 1 \Rightarrow b = a + 1$ $a = 1 \Rightarrow b \leq c$ $\vdash$ $b - 1 \leq c$	set/**inv1**/INV

- Proof by cases:
  - $a = 1$
  - $a \neq 1$

Do Case (2/3)

set_a
when
$a = 1$
then
$a := b - 1$
end

set_b
when
$a \neq 1$
then
$a := b - 1$
end

set
refines $\text{set}_a, \text{set}_b$
begin
$a := b - 1$
end

- Duplication of proof obligations.
- Artificial merging step.

Do Case (3/3)

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

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Summary

```
set
  when
    grd1 :  x ∈ {1, 2}
  then
    act1 :  x := y + 1
  select
    inv2
  end
```

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

- 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.