Summary of Event-B Proof Obligations

Jean-Raymond Abrial (ETHZ)

March 2008

Various Kinds of Proof Obligations

- Invariant preservation (INV slide 8)

- Non-deterministic action feasibility (FIS slide 13)

- Guard strengthening in a refinement (GRD slide 17)

- Simulation (SIM slide 21)

- Numeric variant (NAT slide 25)

- Set variant (FIN slide 29)

Various Kinds of Proof Obligations (cont'd)

- Variant decreasing (VAR slide 33)

- Feasibility of a non-deterministic witness (WFIS slide 41)

- Proving theorems (THM slide 45)

- Well-definedness (WD slide 53)

- Guard strengthening when merging abstract events (MRG slide 57)

Purpose of Invariant Preservation PO (INV)

- Ensuring that each invariant is preserved by each event.

- For an event "evt" and an invariant "inv" the name of this PO is:

evt/inv/INV

Formal Definition of Invariant Preservation (INV)

evt
  any x **where**
    $G(x, s, c, v)$
  then
    $v :\mid BAP(x, s, c, v, v')$
  end

s	:	seen sets
c	:	seen constants
v	:	variables
$A(s, c)$	:	seen axioms and thms
$I(s, c, v)$	:	invariants and thms.
evt	:	specific event
x	:	event parameters
$G(x, s, c, v)$	:	event guards
$BAP(x, s, c, v, v')$	:	event before-after predicate
$inv(s, c, v')$	:	modified specific invariant

Axioms Invariants Guards of the event Before-after predicate of the event $\vdash$ Modified Specific Invariant	$evt/inv/$INV

$$
\begin{array}{l}
A(s, c) \\
I(s, c, v) \\
G(x, s, c, v) \\
BAP(x, s, c, v, v') \\
\vdash \\
inv(s, c, v')
\end{array}
$$

- In case of the initialization event, $I(s, c, v)$ is removed from the hypotheses

Purpose of the Feasibility PO (FIS)

- Ensuring that each non-deterministic action is feasible.

- For an event "evt" and a non-deterministic action "act" in it,
  the name of this PO is:

evt/act/FIS

Formal Definition of the Feasibility PO (FIS)

evt
  any x **where**
    $G(x, s, c, v)$
  then
    $v :| BAP(x, s, c, v, v')$
  end

s	:	seen sets
c	:	seen constants
v	:	variables
$A(s, c)$	:	seen axioms and thms
$I(s, c, v)$	:	invariants and thms.
evt	:	specific event
x	:	event parameters
$G(x, s, c, v)$	:	event guards
$BAP(x, s, c, v, v')$	:	event action

Axioms Invariants Guards of the event $\vdash$ $\exists v' \cdot$ Before-after predicate	$evt/act/$FIS

$$A(s, c)$$
$$I(s, c, v)$$
$$G(x, s, c, v)$$
$$\vdash$$
$$\exists v' \cdot BAP(x, s, c, v, v')$$

Purpose of the Guard Strengthening PO (GRD)

- Ensuring that each abstract guard is stronger than the concrete ones in the refining event.

- This ensures that when a concrete event is enabled then so is the corresponding abstract one.

- For a concrete event "evt" and an abstract guard "grd" in the corresponding abstract event, the name of this PO is:

evt/grd/FIS

Formal Definition of the Guard Strengthening PO (GRD)


```
evt0
  any
    x
  where
    g(x, s, c, v)
    ...
  then
    ...
  end
```

```
evt
  refines
    evt0
  any
    y
  where
    H(y, s, c, w)
  with
    x : W(x, y, s, c, w)
  then
    ...
  end
```

s	:	seen sets
c	:	seen constants
v	:	abstract variables
w	:	concrete variables
$A(s,c)$	:	seen axioms and thms
$I(s,c,v)$	:	abs. invts. and thms.
$J(s,c,v,w)$	:	conc. invts. and thms.
evt	:	specific concrete event
x	:	abstract event parameter
y	:	concrete event parameter
$g(x,s,c,v)$	:	abstract event specific guard
$H(y,s,c,w)$	:	concrete event guards

Axioms Abstract invariants and thms. Concrete invariants and thms. Concrete event guards witness predicate $\vdash$ Abstract event specific guard	$evt/grd/$GRD

$A(s,c)$
$I(s,c,v)$
$J(s,c,v,w)$
$H(y,s,c,w)$
$W(x,y,s,c,w)$
$\vdash$
$g(x,s,c,v)$

- It is simplified when there are no parameters

Purpose of the Simulation PO (SIM)

- Ensuring that each action in a concrete event simulates the corresponding abstract action

- This ensures that when a concrete event is "executed" then what it does is not contradictory with what the corresponding abstract event does.

- For a concrete event "evt" and an action "act" in both concrete and abstract events, the name of this PO is:

evt/act/SIM

Formal Definition of the Simulation PO (SIM)

evt0
any
x
where
$\dots$
then
$v :\mid BA1(v, v', \dots)$
end

evt
refines
evt0
any
y
where
$H(y, s, c, w)$
with
$x : W1(x, y, s, c, w)$
$v' : W2(y, v', s, c, w)$
then
$w :\mid BA2(w, w', \dots)$
end

s	:	seen sets
c	:	seen constants
v	:	abstract vrbls
w	:	concrete vrbls
$A(s, c)$	:	seen axioms and thms
$I(s, c, v)$	:	abs. invts. and thms.
$J(s, c, v, w)$	:	conc. invts. and thms.
evt	:	concrete event
x	:	abstract prm
y	:	concrete prm
$H(y, s, c, w)$	:	concrete guards
$BA1(v, v')$	:	abstract action
$BA2(w, w')$	:	concrete action

Axioms Abstract invariants and thms. Concrete invariants and thms. Concrete event guards witness predicate witness predicate Concrete before-after predicate $\vdash$ Abstract before-after predicate	$evt/act/$SIM

$A(s, c)$
$I(s, c, v)$
$J(s, c, v, w)$
$H(y, s, c, w)$
$W1(x, y, s, c, w)$
$W2(y, v', s, c, w)$
$BA2(w, w', \dots)$
$\vdash$
$BA1(v, v', \dots)$

Purpose of the Numeric Variant PO (NAT)

- Ensuring that under the guards of each convergent event a proposed numeric variant is indeed a natural number

- For a convergent event "evt", the name of this PO is:

evt/NAT

Formal Definition of the Numeric Variant PO (NAT)

machine
  m
refines
  $\ldots$
sees
  $\ldots$
variables
  v
invariants and thms.
  $I(s,c,v)$
theorems
  $\ldots$
events
  $\ldots$
variant
  $n(s,c,v)$
end

evt
  status
    convergent
  any x **where**
    $G(x,s,c,v)$
  then
    A
  end

s	:	seen sets
c	:	seen constants
v	:	variables
$A(s,c)$	:	seen axioms and thms
$I(s,c,v)$	:	abs. invts. and thms.
$J(s,c,v,w)$	:	conc. invts. and thms.
evt	:	specific event
x	:	event parameters
$G(x,s,c,v)$	:	event guards
$n(s,c,v)$	:	numeric variant

Axioms Abstract invariants and thms. Concrete invariants and thms. Event guards $\vdash$ a numeric variant is a natural number	evt/NAT

$$\begin{array}{l} A(s,c) \\ I(s,c,v) \\ J(s,c,v,w) \\ G(x,s,c,v) \\ \vdash \\ n(s,c,v) \in \mathbb{N} \end{array}$$

Purpose of the Set Variant PO (FIN)

- Ensuring that a proposed set variant is indeed a finite set

- The name of this PO is:

FIN

Formal Definition of the Set Variant (FIN)

```
machine
   m
refines
   ...
sees
   ...
variables
   v
invariants and thms.
   J(s, c, v, w)
theorems
   ...
events
   ...
variant
   t(s, c, v)
end
```

s	:	seen sets
c	:	seen constants
v	:	variables
$A(s,c)$	:	seen axioms and thms
$I(s,c,v)$	:	abs. invts. and thms.
$J(s,c,v,w)$	:	conc. invts. and thms.
$t(s,c,v)$	:	set variant

Axioms Abstract invariants and thms. Concrete invariants and thms. $\vdash$ Finiteness of set variant	FIN

$$
\begin{array}{l}
A(s,c) \\
I(s,c,v) \\
J(s,c,v,w) \\
\vdash \\
\mathrm{finite}(t(s,c,v))
\end{array}
$$

Purpose of the Numeric Variant Decreasing PO (VAR)

- Ensuring that each convergent event decreases the proposed numeric variant

- For a convergent event "evt", the name of this PO is:

evt/VAR

Numeric Variant Decreasing (VAR)

evt
  status
    convergent
  any x **where**
    $G(x, s, c, w)$
  then
    $v :| BAP(x, s, c, w, w')$
  end

s	:	seen sets
c	:	seen constants
v	:	variables
$A(s, c)$	:	seen axioms and thms
$I(s, c, v)$	:	abs. invts. and thms.
$J(s, c, v, w)$	:	conc. invts. and thms.
evt	:	specific event
x	:	event parameters
$G(x, s, c, v)$	:	event guards
$BAP(x, s, c, w, w')$	:	event before-after predicate
$n(s, c, w)$	:	numeric variant

Axioms Abstract invariants and thms. Concrete invariants and thms. Guards of the event Before-after predicate of the event ⊢ Modified variant smaller than variant	evt/VAR

$A(s, c)$
$I(s, c, v)$
$J(s, c, v, w)$
$G(x, s, c, w)$
$BAP(x, s, c, w, w')$
$\vdash$
$n(s, c, w') < n(s, c, w)$

Purpose of the Set Variant Decreasing PO (VAR)

- Ensuring that each convergent event decreases the proposed set variant

- For a convergent event "evt", the name of this PO is:

evt/VAR

Formal Definition of the Set Variant Decreasing PO (VAR)

evt
  status
    convergent
  any x **where**
    $G(x, s, c, w)$
  then
    $v :| \ BAP(x, s, c, w, w')$
  end

s	:	seen sets
c	:	seen constants
v	:	variables
$A(s, c)$	:	seen axioms and thms
$I(s, c, v)$	:	abs. invts. and thms.
$J(s, c, v, w)$	:	conc. invts. and thms.
evt	:	specific event
x	:	event parameters
$G(x, s, c, v)$	:	event guards
$BAP(x, s, c, w, w')$	:	event before-after predicate
$t(s, c, w)$	:	set variant

Axioms Abstract Invariants Concrete Invariants Guards of the event Before-after predicate of the event $\vdash$ Modified variant strictly included in variant	evt/VAR

$A(s, c)$
$I(s, c, v)$
$J(s, c, v, w)$
$G(x, s, c, v)$
$BAP(x, s, c, w, w')$
$\vdash$
$t(s, c, w') \subset t(s, c, w)$

Purpose of the Witness Feasibility PO (WFIS)

- Ensuring that each witness proposed in the witness predicate of a concrete event indeed exists

- For a concrete event "evt", and an abstract parameter x the name of this PO is:

$$\text{evt}/x/\text{WFIS}$$

Formal Definition of the Witness Feasibility PO (WFIS)

evt
  refines
    evt0
  any
    y
  where
    $H(y,s,c,w)$
  with
    $x : W(x,y,s,c,w)$
  then
    $\ldots$
  end

s	:	seen sets
c	:	seen constants
v	:	abstract variables
w	:	concrete variables
$A(s,c)$	:	seen axioms and thms
$I(s,c,v)$	:	abs. invts. and thms.
$J(s,c,v,w)$	:	conc. invts. and thms.
evt	:	specific concrete event
x	:	abstract event parameter
y	:	concrete event parameter
$H(y,s,c,w)$	:	concrete event guards
$W(x,y,s,c,w)$	:	witness predicate

Axioms Abstract invariants and thms. Concrete invariants and thms. Concrete event guards $\vdash$ $\exists x \cdot$ Witness	$evt/x/$WFIS

$$
\begin{array}{l}
A(s,c) \\
I(s,c,v) \\
J(s,c,v,w) \\
H(y,s,c,w) \\
\vdash \\
\exists x \cdot W(x,y,s,c,w)
\end{array}
$$

Purpose of a Context Theorem PO (THM)

- Ensuring that a proposed context theorem is indeed provable

- Theorems are important in that they might simplify some proofs

- For a theorem "thm" in a context, the name of this PO is:

thm/THM

Formal Definition of the Context Theorem PO (THM)

context
  ctx
extends
  $\ldots$
sets
  s
constants
  c
axioms
  $A(s,c)$
theorems
  $\ldots$
  $thm: \quad P(s,c)$
  $\ldots$
end

s	:	seen sets
c	:	seen constants
$A(s,c)$	:	seen axioms and previous thms
$P(s,c)$	:	specific theorem

Axioms $\vdash$ Theorem	thm/THM

$$\begin{array}{l} A(s,c) \\ \vdash \\ P(s,c) \end{array}$$

Purpose of a Machine Theorem PO (THM)

- Ensuring that a proposed machine theorem is indeed provable

- Theorems are important in that they might simplify some proofs

- For a theorem "thm" in a machine, the name of this PO is:

thm/THM

Formal Definition of the Machine Theorem PO (THM)

machine
  $m0$
refines
  $\dots$
sees
  $\dots$
variables
  v
invariants and thms.
  $I(s, c, v)$
theorems
  $\dots$
  $thm: \quad P(s, c, v)$
  $\dots$
events
  $\dots$
end

s	:	seen sets
c	:	seen constants
v	:	variables
$A(s, c)$	:	seen axioms and thms
$I(s, c, v)$	:	invariants and previous thms.
$P(s, c, v)$	:	specific theorem

Axioms Invariants $\vdash$ Theorem	thm/THM

$$\begin{array}{l} A(s, c) \\ I(s, c, v) \\ \vdash \\ P(s, c, v) \end{array}$$

Purpose of a Well-definedness PO (WD)

- Ensuring that a potentially ill-defined axiom, theorem, invariant, guard, action, variant, or witness is indeed well-defined

- For a given modeling element (axm, thm, inv, grd, act), or a variant, or a witness x in an event evt, the names are:

axm/WD, thm/WD, inv/WD, grd/WD, act/WD, VWD, evt/x/WWD

Formal Definition of the Well-definedness PO (WD)

- It depends on the potentially ill-defined expression

$\mathrm{inter}\,(S)$	$S \neq \varnothing$
$\bigcap\, x \cdot x \in S \;\land\; P(x) \mid T(x)$	$\exists\, x \cdot x \in S \;\land P(x)$
$f(E)$	f is a partial function $E \in \mathrm{dom}(f)$
E/F	$F \neq 0$
$E \bmod F$	$F \neq 0$
$\mathrm{card}(S)$	$\mathrm{finite}(S)$
$\min(S)$	$S \subseteq \mathbb{Z}$ $\exists x \cdot x \in \mathbb{Z} \;\land\; (\forall n \cdot n \in S \;\Rightarrow\; x \leq n)$
$\max(S)$	$S \subseteq \mathbb{Z}$ $\exists x \cdot x \in \mathbb{Z} \;\land\; (\forall n \cdot n \in S \;\Rightarrow\; x \geq n)$

evt01 **any** x **where** $G1(x,s,c,v)$ **then** A **end**
evt02 **any** x **where** $G2(x,s,c,v)$ **then** A **end**

evt **refines** evt01 evt02 **any** x **where** $H(x,s,c,v)$ **then** A **end**

s	:	seen sets
c	:	seen constants
v	:	abstract vrbls
$A(s,c)$	:	seen axioms and thms
$I(s,c,v)$	:	abs. invts. and thms.
evt	:	concrete event
x	:	similar prm
$H(x,s,c,v)$	:	concrete guards
$G1(x,s,c,v)$	:	abstract event guards
$G2(x,s,c,v)$	:	abstract event guards
A	:	similar abs. and cnc. actions

Axioms Abstract invariants and thms. Concrete event guards $\vdash$ Disjunction of abstract guards	evt/MRG

$$
\begin{array}{l}
A(s,c) \\
I(s,c,v) \\
H(x,s,c,v) \\
\vdash \\
G1(x,s,c,v) \lor G2(x,s,c,v)
\end{array}
$$