Modelling Software-based Systems
Lecture 2
Proof Obligation Generation
Master Informatique

Dominique Méry
Telecom Nancy,Université de Lorraine

18 septembre 2024
dominique.mery@loria.fr

General Summary

❶ Overview of machines, contexts and proof obligations

❷ Proof Obligations for Contexts and Machines
    PO thm/THM (context)
    PO thm/THM (machine)
    PO evt/inv/INV
    PO evt/act/FIS

❸ Proof Obligations for Refinement
    PO evt/grd/GRD
    PO evt/act/SIM
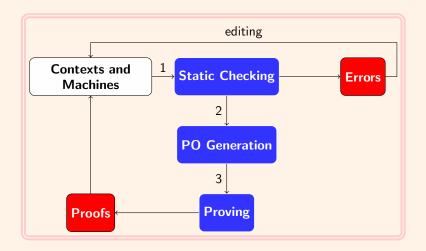   PO evt/NAT
    PO NAT
    PO evt/VAR (arithmetic)
    PO evt/VAR (set-theoretic)
    PO evt/x/WFIS

Current Summary

1 Overview of machines, contexts and proof obligations

2 Proof Obligations for Contexts and Machines

3 Proof Obligations for Refinement

Analysis of the Event-B Models

```
MACHINE
    m
REFINES
    am
SEES
    c
VARIABLES
    u
INVARIANTS
    I(s, c, u)
THEOREMS
    Q(s, c, u)
VARIANT
    exp(s, c, u)
EVENTS
    INITIALIZATION
    . . .
    e
    . . .
END
```

```
MACHINE
   m
REFINES
   am
SEES
   c
VARIABLES
   u
INVARIANTS
   I(s, c, u)
THEOREMS
   Q(s, c, u)
VARIANT
   exp(s, c, u)
EVENTS
   INITIALIZATION
   ...
   e
   ...
END
```

- $\Gamma(m)$: environment for the machine m defined by the context c and it provides a list of seen axioms $Ax(s, c)$ and a list of seen theorems $Th(s, c)$ for the sets s and constants c.

- $\Gamma(m) \vdash \forall u.\text{INIT}(s, c, u) \Rightarrow \text{I}(s, c, u)$

- For each event e in E :
  $\Gamma(m) \vdash \forall u, u'.\text{I}(s, c, u) \wedge BA(e)(u, u') \Rightarrow \text{I}(u')$

- For each event e in E :
  $\Gamma(m) \vdash \forall u.\text{I}(s, c, u) \wedge GRD(e)(s, c, u) \Rightarrow \exists u'.BA(e)(u, u')$

- $\Gamma(m) \vdash \forall u.\text{I}(s, c, u) \Rightarrow \text{Q}(s, c, u)$

- Generated proof obligations are derived from those conditions.

Current Summary

PO thm/THM

```
CONTEXTS
    c
EXTENDS
    ac
SETS
    s
CONSTANTS
    c
AXIOMS
    Ax(s, c)
THEOREMS
    th_1 : P_1(s, c)
    ...
    th_n : P_n(s, c)
    th : P(s, c)
    ...
END
```

s	*seen sets*
c	*seen constants*
$Ax(s, c)$	*seen axioms*
$Th(s, c)$	*previous proved theorems*
	$Th(s, c) = \{P_i(s, c)\|i\ 1..n\}$
$P(s, c)$	*property over s and c*

PO th/THM

$Ax(s, c), Th(s, c) \vdash P(s, c)$

PO thm/THM (machine)

MACHINE		
m		
...	s	seen sets
VARIABLES	c	seen constants
u	u	variables
INVARIANTS	$Ax(s,c)$	seen axioms
$I(s,c,u)$	$Th(s,c)$	seen theorems
THEOREMS	$I(s,c,u)$	invariants
$Q(s,c,u)$	$Q(s,c,u)$	theorems
$th : P(s,c,u)$	$P(s,c,u)$	property over s,c and u
...		
END		

PO thm/THM

$Ax(s,c), Th(s,c), I(s,c,u) \vdash P(s,c,u)$

PO evt/inv/INV

```
EVENT evt
  ANY x WHERE
    G(x, s, c, u)
  THEN
    u : |BAP(x, s, c, u, u')
  END
```

$BA(\text{evt}) \;\widehat{=}\;$

$\exists x. \left(\begin{array}{l} \wedge\; G(x, s, c, u) \\ \wedge\; BAP(x, s, c, u, u') \end{array} \right)$

$GRD(\text{evt}) \;\widehat{=}\; G(x, s, c, u)$

$ACT(\text{evt}) \;\widehat{=}\; BAP(x, s, c, u, u')$

s	*seen sets*
c	*seen constants*
u	*variables*
$Ax(s, c)$	*seen axioms*
$Th(s, c)$	*seen theorems*
$I(s, c, u)$	*invariants*
$Q(s, c, u)$	*theorems*
evt	*event name*
x	*event parameter*
$G(x, s, c, u)$	*event guard*
$BAP(x, s, c, u, u')$	*event before-after predicate*
$inv : inv(s, c, u')$	*specific modified invariant*

PO evt/inv/INV

$Ax(s, c), Th(s, c), I(s, c, u), G(x, s, c, u), BAP(x, s, c, u, u') \vdash inv(s, c, u')$

PO Q/THM $Ax(s, c), Th(s, c), I(s, c, u) \vdash Q(s, c, u)$

PO evt/act/FIS

EVENT evt
  ANY x WHERE
    $G(x, s, c, u)$
  THEN
    $u :| BAP(x, s, c, u, u')$
  END

s	*seen sets*
c	*seen constants*
u	*variables*
$Ax(s, c)$	*seen axioms*
$Th(s, c)$	*seen theorems*
$I(s, c, u)$	*invariants*
$Q(s, c, u)$	*theorems*
evt	*event name*
x	*event parameter*
$G(x, s, c, u)$	*event guard*
$BAP(x, s, c, u, u')$	*event before-after predicate*

$BA(\text{evt}) \ \widehat{=}$
$$\begin{pmatrix} \wedge\ G(x, s, c, u) \\ \wedge\ BAP(x, s, c, u, u') \end{pmatrix}$$
$GRD(\text{evt}) \ \widehat{=} \ G(x, s, c, u)$
$ACT(\text{evt}) \ \widehat{=}$
$BAP(x, s, c, u, u')$

PO evt/act/FIS

$Ax(s, c), Th(s, c), I(s, c, u), G(x, s, c, u), \vdash \exists u'. BAP(x, s, c, u, u')$

Current Summary

PO evt/grd/GRD

```
EVENT ae
  ANY x WHERE
    G(x, s, c, u)
  THEN
    u : |ABAP(x, s, c, u, u')
  END
```

```
EVENT ce
  REFINES
    ae
  ANY y WHERE
    H(y, s, c, v)
  WITH
    x : W(x, y, s, c, v)
  THEN
    v : |CBAP(y, s, c, v, v')
  END
```

s	*seen sets*
c	*seen constants*
u, v	*abstract and concrete variables*
$Ax(s, c)$	*seen axioms*
$Th(s, c)$	*seen theorems*
$I(s, c, u)$	*abstract invariants*
$J(s, c, u, v)$	*concrete invariants*
$Q(s, c, u), \ R(s, c, u, v)$	*abstract and concrete theorems*
ae, ce	*abstract and concrete event name*
x, y	*event parameters*
$G(x, s, c, u)$	*abstract event guard*
$H(y, s, c, v)$	*concrete event guard*
$ABAP(x, s, c, u, u')$	*abstract event before-after predic*
$CBAP(x, s, c, u, u')$	*concrete event before-after predic*
W(x,y,s,c,v)	*witness predicate*

PO evt/grd/GRD

$Ax(s, c), Th(s, c), I(s, c, u), J(s, c, u, v), W(x, y, s, c, v), H(y, s, c, v), \vdash$
$G(x, s, c, u')$

PO evt/act/SIM

EVENT ae
  ANY x WHERE
    $G(x, s, c, u)$
  THEN
    $u : |ABAP(x, s, c, u, u')$
  END

EVENT ce
  REFINES
    ae
  ANY y WHERE
    $H(y, s, c, v)$
  WITH
    $x : WP(x, y, s, c, v)$
    $u' : WV(y, u', s, c, v)$
  THEN
    $v : |CBAP(y, s, c, v, v')$
  END

s	*seen sets*
c	*seen constants*
u, v	*abstract and concrete variables*
$Ax(s, c)$	*seen axioms*
$Th(s, c)$	*seen theorems*
$I(s, c, u)$	*abstract invariants*
$J(s, c, u, v)$	*concrete invariants*
$Q(s, c, u), \; R(s, c, u, v)$	*abstract and concrete theorems*
ae, ce	*abstract and concrete event name*
x,y	*event parameters*
$G(x, s, c, u)$	*abstract event guard*
$H(y, s, c, v)$	*concrete event guard*
$ABAP(x, s, c, u, u')$	*abstract event before-after predic*
$CBAP(x, s, c, u, u')$	*concrete event before-after predic*
$WP(x, y, s, c, v)$	witness parameter predicate
$WV(y, u', s, c, v)$	witness variable predicate

PO evt/act/SIM

$$\begin{pmatrix} Ax(s,c), Th(s,c), I(s,c,u), J(s,c,u,v) \\ WP(x,y,s,c,v), WV(y,u',s,c,v) \\ H(y,s,c,v), CBAP(y,s,c,v,v') \end{pmatrix} \vdash ABAP(x,s,c,u,u')$$

```
EVENT ae
  ANY x WHERE
    G(x, s, c, u)
  THEN
    u :| BAP(x, s, c, u, u')
  END
...
VARIANT
    exp(s, c, u)
```

s	*seen sets*
c	*seen constants*
u, v	*abstract and concrete variables*
$Ax(s, c)$	*seen axioms*
$Th(s, c)$	*seen theorems*
$I(s, c, u)$	*abstract invariants*
$J(s, c, u, v)$	*concrete invariants*
$Q(s, c, u), R(s, c, u, v)$	*abstract and concrete theorems*
evt, ce	*event name*
x	*event parameters*
$G(x, s, c, u)$	*abstract event guard*
$BAP(x, s, c, u, u')$	*event before-after predicate*
$exp(s, c, u)$	*aritthmetic expression*

PO evt/NAT

$$Ax(s, c), Th(s, c), I(s, c, u), J(s, c, u, v), G(x, s, c, u) \vdash exp(s, c, u) \in \mathbb{N}$$

```
EVENT ae
  ANY x WHERE
    G(x, s, c, u)
  THEN
    u :| BAP(x, s, c, u, u')
  END
...
VARIANT
    exp(s, c, u)
```

s	*seen sets*
c	*seen constants*
u, v	*abstract and concrete variables*
$Ax(s, c)$	*seen axioms*
$Th(s, c)$	*seen theorems*
$I(s, c, u)$	*abstract invariants*
$J(s, c, u, v)$	*concrete invariants*
$Q(s, c, u), R(s, c, u, v)$	*abstract and concrete theorems*
evt, ce	*event name*
x	*event parameters*
$G(x, s, c, u)$	*abstract event guard*
$BAP(x, s, c, u, u')$	*event before-after predicate*
$setexp(s, c, u)$	*set expression*

PO evt/NAT $Ax(s, c), Th(s, c), I(s, c, u), J(s, c, u, v), G(x, s, c, u) \vdash$

$finite(setexp(s, c, u))$

PO evt/VAR

s	*seen sets*
c	*seen constants*
u, v	*abstract and concrete variables*
$Ax(s, c)$	*seen axioms*
$Th(s, c)$	*seen theorems*
$I(s, c, u)$	*abstract invariants*
$J(s, c, u, v)$	*concrete invariants*
$Q(s, c, u),\ R(s, c, u, v)$	*abstract and concrete theorems*
evt, ce	*event name*
x	*event parameters*
$G(x, s, c, u)$	*abstract event guard*
$BAP(x, s, c, u, u')$	*event before-after predicate*
$exp(s, c, u)$	*aritthmetic expression*

```
EVENT ae
  ANY x WHERE
    G(x, s, c, u)
  THEN
    u : |BAP(x, s, c, u, u')
  END
...
VARIANT
  exp(s, c, u)
```

PO evt/VAR

$Ax(s, c), Th(s, c), I(s, c, u), J(s, c, u, v), G(x, s, c, u), BAP(x, s, c, u, u') \vdash$
$exp(s, c, u') < exp(s, c, u)$

PO evt/VAR

```
EVENT ae
  ANY x WHERE
    G(x, s, c, u)
  THEN
    u : |BAP(x, s, c, u, u')
  END
...
VARIANT
    setexp(s, c, u)
```

s	*seen sets*
c	*seen constants*
u, v	*abstract and concrete variables*
$Ax(s, c)$	*seen axioms*
$Th(s, c)$	*seen theorems*
$I(s, c, u)$	*abstract invariants*
$J(s, c, u, v)$	*concrete invariants*
$Q(s, c, u),\ R(s, c, u, v)$	*abstract and concrete theorems*
evt, ce	*event name*
x	*event parameters*
$G(x, s, c, u)$	*abstract event guard*
$BAP(x, s, c, u, u')$	*event before-after predicate*
$setexp(s, c, u)$	*set-theoretic expression*

PO evt/VAR

$Ax(s, c), Th(s, c), I(s, c, u), J(s, c, u, v), G(x, s, c, u), BAP(x, s, c, u, u') \vdash$
$setexp(s, c, u') \subset setexp(s, c, u)$

PO evt/x/WFIS

EVENT ae
  ANY x WHERE
    $G(x, s, c, u)$
  THEN
    $u : |ABAP(x, s, c, u, u')$
  END

EVENT ce
  REFINES
    ae
  ANY y WHERE
    $H(y, s, c, v)$
  WITH
    $x : WP(x, y, s, c, v)$
    $u' : WV(y, u', s, c, v)$
  THEN
    $v : |CBAP(y, s, c, v, v')$
  END

s	seen sets
c	seen constants
u, v	abstract and concrete variables
$Ax(s, c)$	seen axioms
$Th(s, c)$	seen theorems
$I(s, c, u)$	abstract invariants
$J(s, c, u, v)$	concrete invariants
$Q(s, c, u), R(s, c, u, v)$	abstract and concrete theorems
ae, ce	abstract and concrete event name
x,y	event parameters
$G(x, s, c, u)$	abstract event guard
$H(y, s, c, v)$	concrete event guard
$ABAP(x, s, c, u, u')$	abstract event before-after predic
$CBAP(x, s, c, u, u')$	concrete event before-after predic
$WP(x, y, s, c, v)$	witness parameter predicate
$WV(y, u', s, c, v)$	witness variable predicate

PO evt/x/WFIS

$Ax(s, c), Th(s, c), I(s, c, u), J(s, c, u, v), H(y, s, c, v) \vdash$
$\exists x. WP(x, y, s, c, v)$