Lecture 11 - February 14

Reactive System: Bridge Controller

Announcements

- Lab2 released
- WrittenTest1 guide released
  - \+ Verify EECS account on a WSC machine
  - \+ Verify PPY account and Duo Mobile on eClass
- Review Session at 7pm, Wednesday? (Zoom)

- No Rodin
- given Rodin syntax → answer
- written Rodin syntax
-

Confirmed

PO/VC Rule of Invariant Preservation: Components

θ : event parameters ?

$c \triangleq \langle d \rangle$ is defined as

constants: d

$A(\langle d \rangle) = \langle axm0\_1 \rangle$

axioms:
axm0_1 : $d \in \mathbb{N}$

$v \triangleq \langle n \rangle$ → pre-state value

$v' \triangleq \langle n' \rangle$ → post-state value

variables: n

$I(\langle d \rangle, \langle n \rangle) = \langle inv0\_1, inv0\_2 \rangle$

invariants:
inv0_1 : $n \in \mathbb{N}$
inv0_2 : $n \le d$

indices of inv.

$I_1(\langle d \rangle, \langle n \rangle) \triangleq n \in \mathbb{N}$

ML_out $G(\langle d \rangle, \langle v \rangle) \triangleq True$
begin
$n := n + 1$ → $n' = n + 1$ effect
end

$E(\langle d \rangle, \langle n \rangle) = \langle n + 1 \rangle$

ML_in $G(\langle d \rangle, \langle v \rangle) \triangleq True$
begin
$n := n - 1$
end

$E(\langle d \rangle, \langle n \rangle) = \langle n - 1 \rangle$

c: list of constants

A(c): list of axioms

v and v′: variables in pre- and post-state

I(c, v): list of invariants
(c → constants, v → variables)

G(c, v): guards of an event's

E(c, v): effect of an event's actions

v′ = E(c, v): BAP of an event's actions

BAP of ML_out:
$\langle n' \rangle = \langle n + 1 \rangle$

PO/VC Rule of Invariant Preservation: Sequents

all invariant conditions

constants: d	variables: n	ML_out **begin** $n := n + 1$ **end**
axioms: **axm0_1** : $d \in \mathbb{N}$	**invariants:** **inv0_1** : $n \in \mathbb{N}$ **inv0_2** : $n \leq d$	ML_in **begin** $n := n - 1$ **end**

$\boxed{A(c)}$ axioms

$\boxed{I(c, v)}$ → invariant in pre-state

$* \boxed{G(c, v)}$ guard of some event is evaluated true in pre-state

$\vdash$

$** \; I_i(c, \boxed{E(c, v)})$

index of invariants (1 or 2)

invariant i should be expr. using the effect of the event.

Q. How many PO/VC rules for model m0?

* guard of some event → # of events (2)

** some invariant condition → # of invariant conditions. (2)

Overall: 2 * 2 = 4 POs

PO_1 : ML_out / inv0_1 / INV

evt name   inv. cond.   nature of PO

PO_2 : ML_out / inv0_2 / INV

PO_3, PO_4 : Exercise!

constants: d

variables: n

axioms:
axm0_1 : $d \in \mathbb{N}$

invariants:
inv0_1 : $n \in \mathbb{N}$
inv0_2 : $n \leq d$

ML_out
begin
$n := \boxed{n + 1}$
end

ML_in
begin
$n := n - 1$
end

$A(c)$
$I(c, v)$
$G(c, v)$
$\vdash$
$I_i(c, \boxed{E(c, v)})$

effect of an event only occurs if event is enabled

effect of ML_out

$d \in \mathbb{N}$
$n \in \mathbb{N}$
$n \leq d$
True
$\vdash$
$\underbrace{\cancel{n}}_{n+1} \in \mathbb{N}$

ML_out/inv0_1/INV

Exercise: Formulate PO3, PO4

$d \in \mathbb{N}$
$n \in \mathbb{N}$
$n \leq d$
True
$\vdash$
$\underbrace{\cancel{n}}_{n+1} \leq d$

ML_out/inv0_2/INV

Inference Rule: Syntax and Semantics

Sequent

$$\boxed{H \vdash G}$$

$H \Rightarrow G$ provable or not.

Inference Rule

$$\boxed{\frac{A}{C}}$$

$A \Rightarrow C \equiv \text{True}.$

Syntax

antecedent ↳ a set of sequents

$$\boxed{\frac{A}{C} \quad L}$$

L: name

consequent ↳ a single sequent

Semantics

$$A \overset{T①}{\Rightarrow} \underset{T②}{C} \equiv \text{True}$$

③ must be true

Q. What does it mean when A is empty/absent?

$$\boxed{\frac{}{C}}$$

$\text{True} \Rightarrow C \equiv \text{True}$

↳ $C \equiv \text{True}$

the consequent itself is an axiom.

Examples

IR1

$$\frac{H_1 \vdash G}{H_1, H_2 \vdash G}$$

To prove $H_1, H_2 \vdash G$,

it's sufficient to prove (by dropping a hypothesis):

$H_1 \vdash G$

$$\frac{H_1 \vdash G}{\boxed{H_1, H_2 \vdash G}}$$

$$\frac{A}{C}\ \underline{\text{MON}}$$

monotonicity.

→ To prove C, it's sufficient to prove A

$$\boxed{\frac{}{n \in \mathbb{N} \vdash n+1 \in \mathbb{N}}}\ \text{P2}$$

nothing to prove for the consequent.

$$\frac{\boxed{\begin{array}{l} d \in \mathbb{N} \\ n \in \mathbb{N} \\ n \le d \\ \text{True} \\ \vdash n+1 \in \mathbb{N} \end{array}}}{}\ \text{MON}\ \frac{\boxed{\begin{array}{l} n \in \mathbb{N} \\ \vdash \\ n+1 \in \mathbb{N} \end{array}}}{}\ \text{P2}$$

Justifying Inference Rule: OR_L

$$\frac{\boxed{\cancel{H}, P \vdash R \qquad \cancel{H}, Q \vdash R}\ A}{\boxed{\cancel{H}, P \vee Q \vdash R}\ C}\ \textbf{OR\_L}$$

$$\boxed{A \Rightarrow C \equiv True}$$

$$((P \Rightarrow R) \wedge (Q \Rightarrow R)) \Rightarrow (P \vee Q \Rightarrow R) \equiv \underline{\underline{True}}.$$

(demo video).

Example Inference Rules

terminating rules.

$$\frac{}{\vdash 0 \in \mathbb{N}}\ \textbf{P1}$$

$$\frac{}{n \in \mathbb{N} \vdash n+1 \in \mathbb{N}}\ \textbf{P2}$$

n m

$$\frac{}{n < m \vdash n+1 \leq m}\ \textbf{INC}$$

$$\frac{}{0 < n \vdash n-1 \in \mathbb{N}}\ \textbf{P2'}$$

n n, m

$$\frac{}{n \leq m \vdash n-1 < m}\ \textbf{DEC}$$

$$\frac{}{n \in \mathbb{N} \vdash 0 \leq n}\ \textbf{P3}$$

non-terminating.

$$\frac{H, P \vdash R \qquad H, Q \vdash R}{H, \boxed{P \vee Q} \vdash R}\ \textbf{OR\_L}$$

to the L of ⊢

$(H \Rightarrow P) \Rightarrow (H \Rightarrow P \vee Q)$

$$\frac{H \vdash P}{H \vdash P \vee Q}\ \textbf{OR\_R1}$$

to the R of ⊢

disjunction

$$\frac{H \vdash Q}{H \vdash P \vee Q}\ \textbf{OR\_R2}$$

$$\frac{H1 \vdash G}{H1, H2 \vdash G}\ \textbf{MON}$$