

Lecture 11 - February 14

Reactive System: Bridge Controller

Announcements

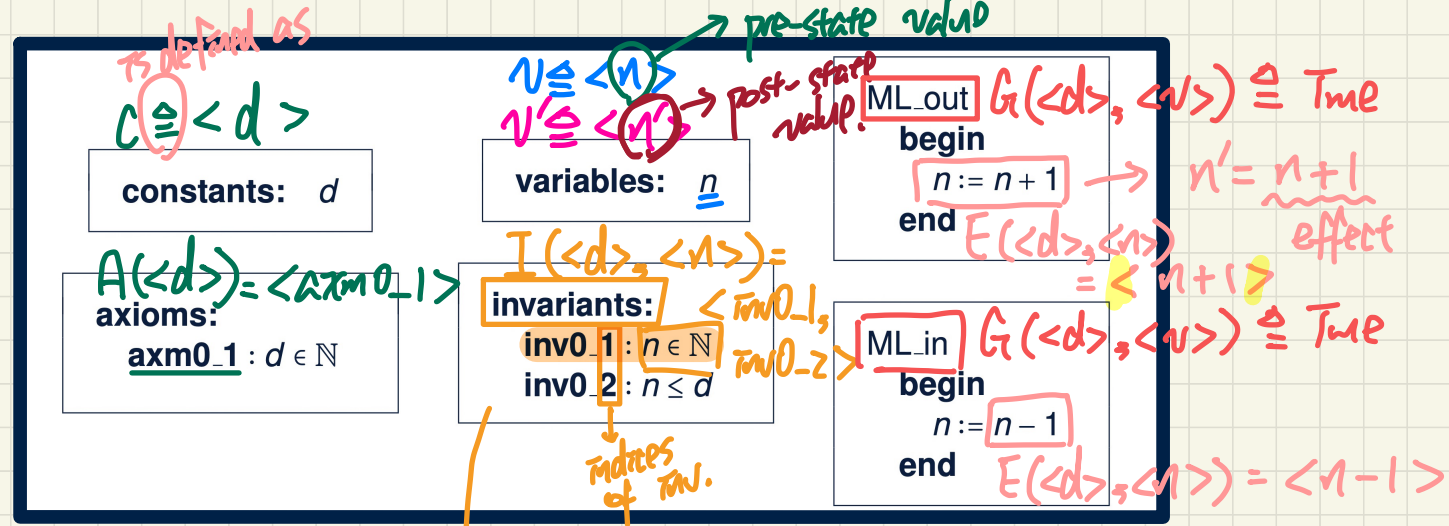
- Lab2 released
- WrittenTest1 guide released
 - + Verify EECS account on a WSC machine
 - + Verify PPY account and Duo Mobile on eClass
- Review Session at 7pm, Wednesday? (Zoom)

- No Router
- given Router syntax → answer
- written Router syntax

Confirmed

θ : event parameters?

PO/VC Rule of Invariant Preservation: Components



$\langle c \rangle$: list of constants

$A(\langle c \rangle)$: list of axioms

$\langle v \rangle$ and $\langle v' \rangle$: variables in pre- and post-state

$I(\langle c \rangle, \langle v \rangle)$: list of invariants

constants variables

$G(\langle c \rangle, \langle v \rangle)$: guards of an event's

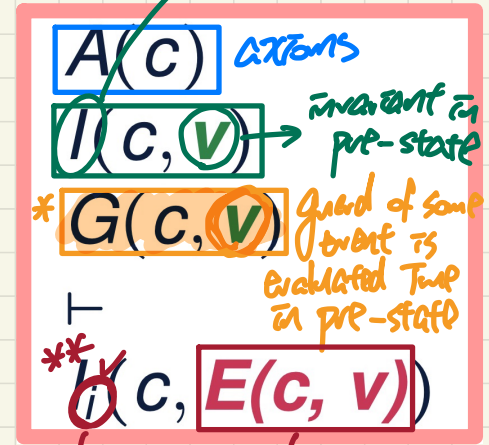
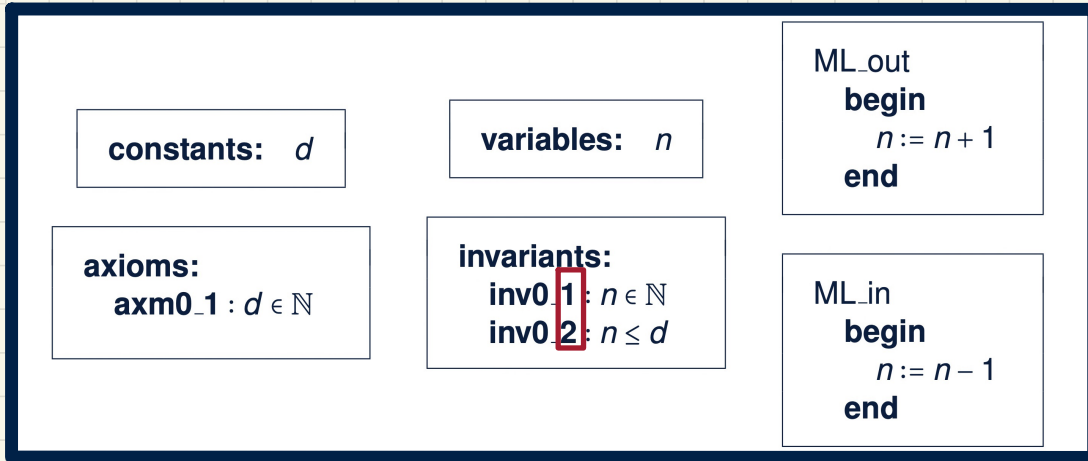
$E(\langle c \rangle, \langle v \rangle)$: effect of an event's actions

BAP of ML.out:
 $\langle v' \rangle = \langle n + 1 \rangle$

$\langle v' \rangle = E(\langle c \rangle, \langle v \rangle)$: BAP of an event's actions

PO/VC Rule of Invariant Preservation: Sequents

all invariant conditions



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

↓ index of invariants (1 or 2)
 ↓ invariant I should be expr. using the effect of the event.

* guard of some event \rightarrow # of events (2)
 ** some invariant condition \rightarrow # of invariant conditions. (2)

Overall: $2 * 2 = 4$ POs
 $PO_1: ML_out / INV_1 / INV$
 but none inv. cond. notation of PO
 $PO_2: ML_out / INV_2 / INV$
 $PO_3, PO_4: Exercise!$

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

$A(c)$
 $\vdash I(c, v)$
 $G(c, v)$
 $\vdash I_j(c, E(c, v))$

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
 ~~$n \in \mathbb{N}$~~
 $n + 1$

ML_out / inv0_1 / INV

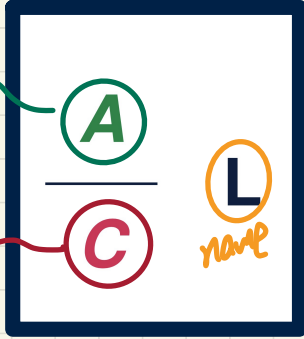
Exercise: Formulate P_3 , P_4

$d \in \mathbb{N}$
 $n \in \mathbb{N}$
 $n \leq d$
 True
 \vdash
 ~~$n \leq d$~~
 $n + 1$

ML_out / inv0_2 / INV

Inference Rule: Syntax and Semantics

Syntax

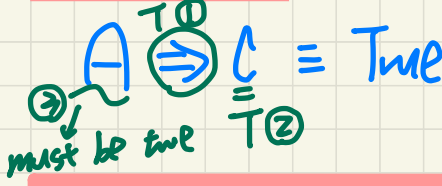


Antecedent
↳ a set of sequents

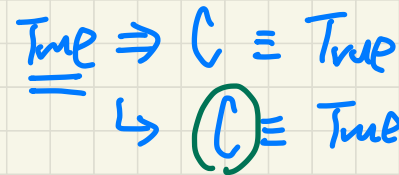
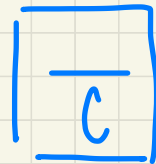
Consequent
↳ a single sequent

Examples

Semantics

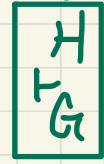


Q. What does it mean when A is empty/absent?



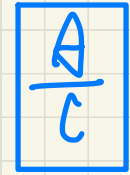
the consequent itself is an axiom.

Sequent



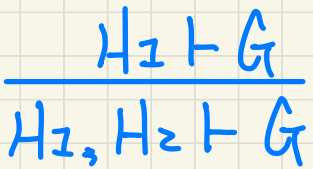
$H \Rightarrow G$
provide or not.

Inference Rule



$A \Rightarrow C \equiv True.$

IR1



To prove $H1 \rightarrow H2 \vdash G$,
it's sufficient to prove (by dropping a hypothesis):
 $H1 \vdash G$

$H_1 \vdash G$

$H_1, H_2 \vdash G$

A
Mon \rightarrow monotonicity

\rightarrow To prove C , it's sufficient to prove A

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

Mon

$n \in \mathbb{N}$
 \vdash
 $n+1 \in \mathbb{N}$

P_2

$n \in \mathbb{N} \vdash n+1 \in \mathbb{N}$ P_2

nothing to prove for the consequent.

Justifying Inference Rule: OR_L

$$\frac{\boxed{H, P \vdash R} \quad \boxed{H, Q \vdash R}}{\boxed{H, P \vee Q \vdash R}} \text{OR_L} \quad A$$

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

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

(demo video).

Example Inference Rules

terminating rules.

$$\frac{}{\vdash 0 \in \mathbb{N}} \quad \text{P1}$$

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

$$\frac{\begin{array}{c} \text{---} \\ \quad \bullet \quad \bullet \\ \quad n \quad m \end{array}}{n < m \vdash n+1 \leq m} \quad \text{INC}$$

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

$$\frac{\begin{array}{c} \text{---} \\ \quad \bullet \quad \bullet \\ \quad n \quad n, m \end{array}}{n \leq m \vdash n-1 < m} \quad \text{DEC}$$

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

$$\frac{H, P \vdash R \quad H, Q \vdash R}{H, P \vee Q \vdash R} \quad \text{OR}_L$$

to the L of \vdash

non-terminating

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

$(H \Rightarrow P) \Rightarrow (H \Rightarrow P \vee Q)$
to the R of \vdash
disjunction

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

$$\frac{H1 \vdash G}{H1, H2 \vdash G} \quad \text{MON}$$