Lecture 18 - Nov 11

Bridge Controller

Guard Strengthening: Review
INV Preservation: POs
INV Preservation: Commuting Diagram

Announcements/Reminders

- Today's class: notes template posted
- **WrittenTest2** Wednesday (November 12)

Refinement: Guard Strengthening

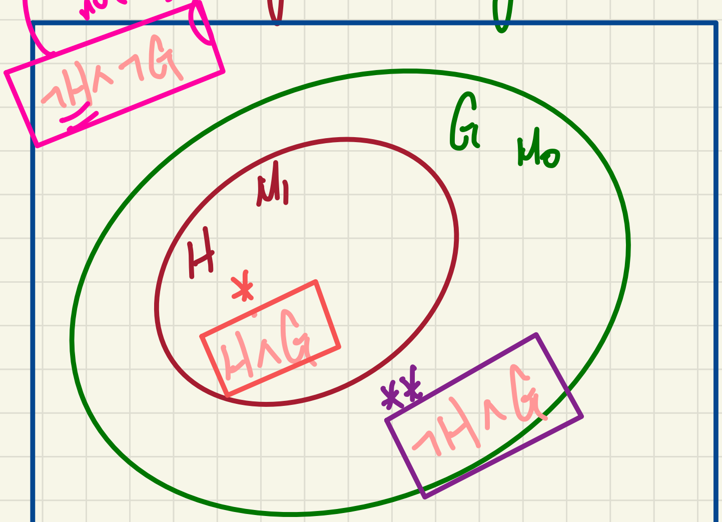
$\neg G \Rightarrow \neg H$

$H \Rightarrow G$

H: concrete guard

G: abstract guard

what's not allowed by M_0 is also not allowed by M_1.



* what's enabled in M_1 is also enabled in M_0.

** some scenarios allowed by M_0 is not allowed by M_1.

(ok ∵ no new scenarios created by M_1).

M_0 $\boxed{\begin{array}{l}\text{ML\_out}\\ \quad n < d\end{array}}$ (G)

M_1 $\boxed{\begin{array}{l}\text{ML\_out}\\ \quad a+b < d\end{array}}$ (H)

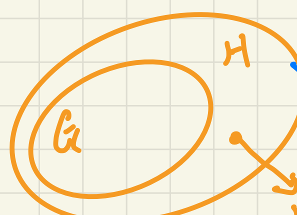
$a+b+c=n$

$c=0$

change this to $\leq$

Q. guard strengthening?

A. $\underbrace{\cancel{a+b}}_{n} \leq d \Rightarrow n < d$



$n=d$

in M_1, ML_out is enabled when $n=d$, but it is disabled in M_0.

Discharging POs of m1: Guard Strengthening in Refinement

ML_out/GRD

$$
\begin{array}{l}
d \in \mathbb{N} \\
d > 0 \\
n \in \mathbb{N} \\
n \leq d \\
a \in \mathbb{N} \\
b \in \mathbb{N} \\
c \in \mathbb{N} \\
a + b + c = n \\
a = 0 \lor c = 0 \\
a + b < d \\
c = 0 \\
\vdash \\
n < d
\end{array}
$$

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

$$\frac{}{H, P \vdash P}\ \textbf{HYP}$$

$$\frac{H(F), E = F \vdash P(F)}{H(E), E = F \vdash P(E)}\ \textbf{EQ\_LR}$$

Discharging POs of m1: Guard Strengthening in Refinement

ML_in/GRD

$$
\begin{array}{l}
d \in \mathbb{N} \\
d > 0 \\
n \in \mathbb{N} \\
n \leq d \\
a \in \mathbb{N} \\
b \in \mathbb{N} \\
c \in \mathbb{N} \\
a + b + c = n \\
a = 0 \lor c = 0 \\
c > 0 \\
\vdash \\
n > 0
\end{array}
$$

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

$$\frac{}{H, P \vdash P}\ \textbf{HYP}$$

$$\frac{}{\bot \vdash P}\ \textbf{FALSE\_L}$$

$$\frac{H(F), E = F \vdash P(F)}{H(E), E = F \vdash P(E)}\ \textbf{EQ\_LR}$$

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

PO/VC Rule of Invariant Preservation: Sequents

Abstract m0

$* \cancel{a} + \cancel{b} + \cancel{c} = \cancel{n}\ n+1$
$a+1 \quad b \quad c$

variables: n

invariants:
$\boxed{\begin{array}{l}\textbf{inv0\_1}: n \in \mathbb{N} \\ \textbf{inv0\_2}: n \le d\end{array}}$

ML_out
when
$n < d$
then
$\boxed{n := n + 1}$ $n' = n+1$
end

ML_in
when
$n > 0$
then
$\boxed{n := n - 1}$
end
$n' = n-1$

pre-state

$\boxed{A(c)}$ axioms
$\boxed{I(c, \mathbf{v})}$ abst. Inv.
$\boxed{J(c, \mathbf{v}, \mathbf{w})}$ conc. Inv.
$\boxed{H(c, \mathbf{w})}$ concrete guard
$\vdash$
$J_i(c, E(c, \mathbf{v}), F(c, \mathbf{w}))$

concrete inv. sat in post state

Concrete m1

$** \cancel{a} = 0 \vee \cancel{c} = 0$
$a \quad c-1$

variables: a, b, c

invariants:
$\boxed{\begin{array}{l}\textbf{inv1\_1}: a \in \mathbb{N} \\ \textbf{inv1\_2}: b \in \mathbb{N} \\ \textbf{inv1\_3}: c \in \mathbb{N} \\ \textbf{inv1\_4}: a + b + c = n \\ \textbf{inv1\_5}: a = 0 \vee c = 0\end{array}}$

ML_out
when
$\boxed{\begin{array}{l}a + b < d \\ c = 0\end{array}}$
then
$\boxed{a := a + 1}$
end
$a' = a+1 \wedge b' = b \wedge c' = c$

ML_in
when
$\boxed{c > 0}$
then
$\boxed{c := c - 1}$
end
$c' = c-1 \wedge a' = a \wedge b' = b$

2 con. evts * 5 con. inv.
$=$
10 POs.

Q. How many PO/VC rules for model m1?

ML_out/inv1_4/INV

$d \in \mathbb{N}$
$d > 0$
$n \in \mathbb{N}$
$n \le d$
$a \in \mathbb{N}$ $b \in \mathbb{N}$ $c \in \mathbb{N}$
$a+b+c = n$
$a = 0 \vee c = 0$
$a+b < d \quad c = 0$
$\vdash *$
$\boxed{(a+1)+b+c = n+1}$

ML_in/inv1_5/INV

$d \in \mathbb{N}$
$d > 0$
$n \in \mathbb{N}$
$n \le d$
$a \in \mathbb{N}$ $b \in \mathbb{N}$ $c \in \mathbb{N}$
$a+b+c = n$
$a = 0 \vee c = 0$
$c > 0$
$\vdash **$
$\boxed{a = 0 \vee (c-1) = 0}$

Visualizing Invariant Preservation in Refinement

linking invariant:

(1) defined in the concrete model

(2) involves both abst. & concrete variables

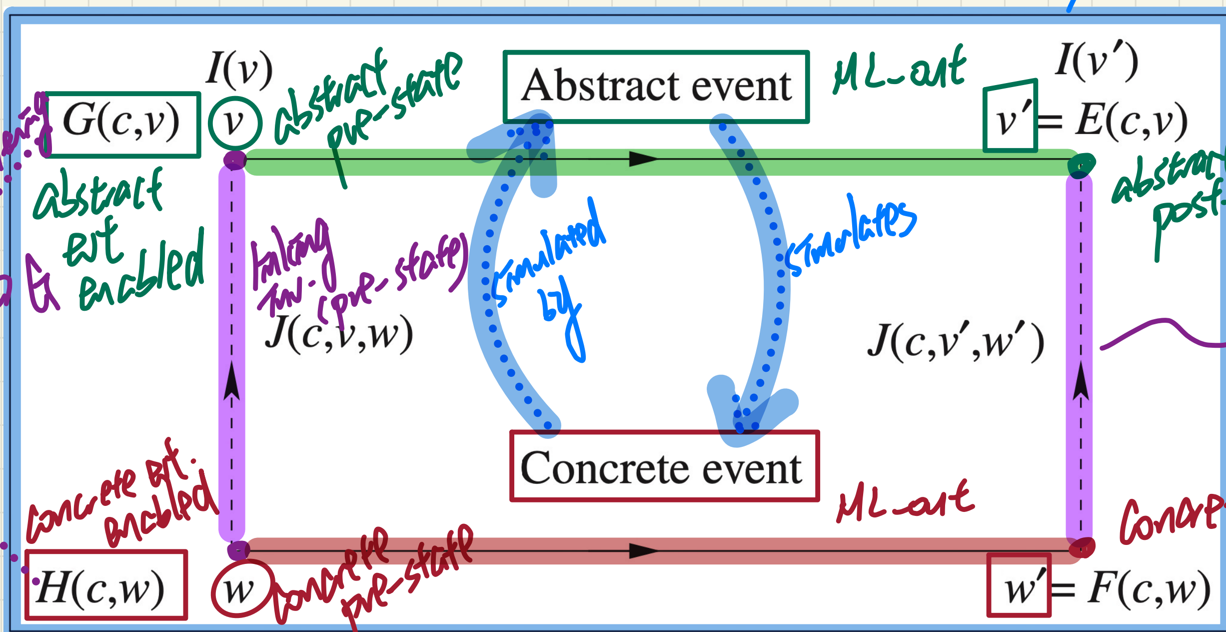
Each concrete state transition (from w to w′) should be simulated by an abstract state transition (from v to v′)

ML_out

→ found correspondence to.

ML_out

commuting diagram



Discharging POs of m1: Invariant Preservation in Refinement

ML_out/inv1_4/INV

$$
\begin{array}{l}
d \in \mathbb{N} \\
d > 0 \\
n \in \mathbb{N} \\
n \leq d \\
a \in \mathbb{N} \\
b \in \mathbb{N} \\
c \in \mathbb{N} \\
a + b + c = n \\
a = 0 \lor c = 0 \\
a + b < d \\
c = 0 \\
\vdash \\
(a + 1) + b + c = (n + 1)
\end{array}
$$

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

$$\frac{}{P \vdash E = E} \ \textbf{EQ}$$

$$\frac{H(\mathbf{F}), \mathbf{E} = \mathbf{F} \vdash P(\mathbf{F})}{H(\mathbf{E}), \mathbf{E} = \mathbf{F} \vdash P(\mathbf{E})} \ \textbf{EQ\_LR}$$

Discharging POs of m1: Invariant Preservation in Refinement

ML_in/inv1_5/INV

$d \in \mathbb{N}$
$d > 0$
$n \in \mathbb{N}$
$n \leq d$
$a \in \mathbb{N}$
$b \in \mathbb{N}$
$c \in \mathbb{N}$
$a + b + c = n$
$a = 0 \lor c = 0$
$c > 0$
$\vdash$
$a = 0 \lor (c - 1) = 0$

$$\frac{}{H, P \vdash P} \quad \textbf{HYP}$$

$$\frac{}{\bot \vdash P} \quad \textbf{FALSE\_L}$$

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

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

$$\frac{H(F), E = F \vdash P(F)}{H(E), E = F \vdash P(E)} \quad \textbf{EQ\_LR}$$

$$\frac{H, P \vdash R \qquad H, Q \vdash R}{H, P \lor Q \vdash R} \quad \textbf{OR\_L}$$

PO of Invariant Establishment in Refinement

constants: d

axioms:
axm0_1 : $d \in \mathbb{N}$
axm0_2 : $d > 0$

variables: a, b, c

invariants:
inv1_1 : $a \in \mathbb{N}$
inv1_2 : $b \in \mathbb{N}$
inv1_3 : $c \in \mathbb{N}$
inv1_4 : $a + b + c = n$
inv1_5 : $a = 0 \lor c = 0$

init
begin
$a := 0$
$b := 0$
$c := 0$
end

Components

K(c): effect of abstract init

L(c): effect of concrete init

Rule of Invariant Establishment

$$A(c) \vdash J_i(c, K(c), L(c))$$

Exercise:

Generate Sequents from the INV rule.

5

Q. How many PO/VC rules for model m1?

Discharging PO of Invariant Establishment in Refinement

$$\boxed{\begin{array}{l} d \in \mathbb{N} \\ d > 0 \\ \vdash \\ 0 + 0 + 0 = 0 \end{array}}$$

init/inv1_4/INV

$$\boxed{\begin{array}{l} d \in \mathbb{N} \\ d > 0 \\ \vdash \\ 0 = 0 \lor 0 = 0 \end{array}}$$

init/inv1_5/INV

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

$$\boxed{\frac{}{P \ \vdash \ \top} \quad \text{TRUE\_R}}$$