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

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

$$\frac{H1 \vdash G}{H1, H2 \vdash G}\ \textbf{MON} \qquad \frac{}{H, P \vdash P}\ \textbf{HYP} \qquad \frac{}{\bot \vdash P}\ \textbf{FALSE\_L}$$

$$\frac{H(F), E = F \vdash P(F)}{H(E), E = F \vdash P(E)}\ \textbf{EQ\_LR} \qquad \frac{H, P \vdash R \quad H, Q \vdash R}{H, P \lor Q \vdash R}\ \textbf{OR\_L}$$

PO/VC Rule of Invariant Preservation: Sequents

Abstract m0

variables: n

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

ML_out
when
$n < d$
then
$n := n + 1$
end

ML_in
when
$n > 0$
then
$n := n - 1$
end

$$A(c)$$
$$I(c, v)$$
$$J(c, v, w)$$
$$H(c, w)$$
$$\vdash$$
$$J_i(c, E(c, v), F(c, w))$$

Concrete m1

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 : $a = 0 \vee c = 0$

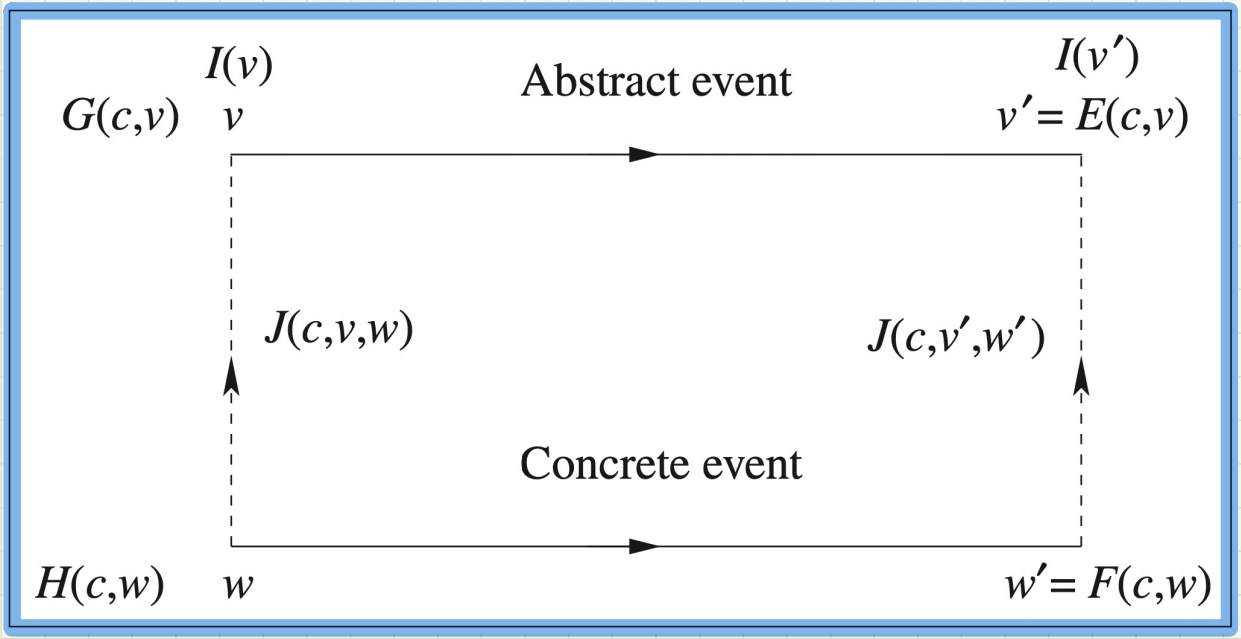
ML_out
when
$a + b < d$
$c = 0$
then
$a := a + 1$
end

ML_in
when
$c > 0$
then
$c := c - 1$
end

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

Visualizing Invariant Preservation in Refinement

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



Discharging POs of m1: Invariant Preservation in Refinement

ML_out/inv1_4/INV

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

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

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

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

Discharging POs of m1: Invariant Preservation in Refinement

ML_in/inv1_5/INV

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

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

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

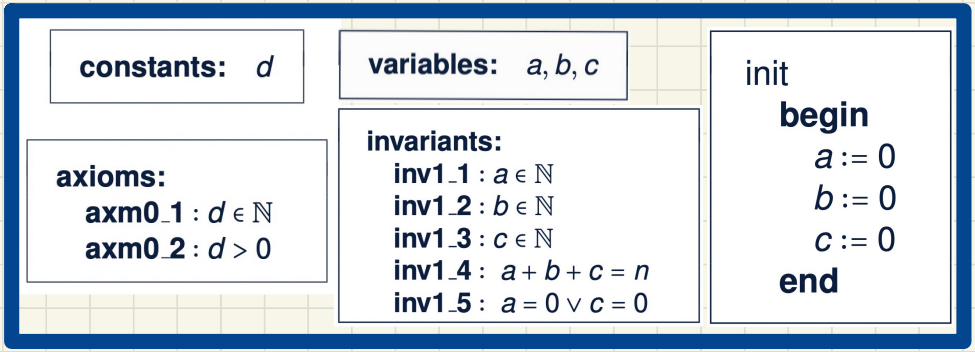
$$\frac{H1 \vdash G}{H1, H2 \vdash G}\ \text{MON}$$

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

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

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

PO of Invariant Establishment in Refinement



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.

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

Discharging PO of Invariant Establishment in Refinement

$$d \in \mathbb{N}$$
$$d > 0$$
$$\vdash$$
$$0 + 0 + 0 = 0$$

init/inv1_4/INV

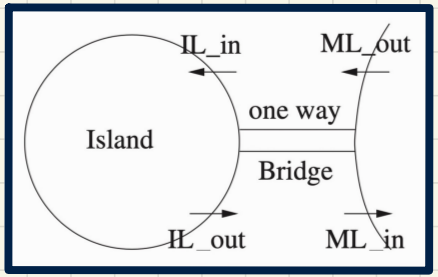
$$\frac{H1 \vdash G}{H1, H2 \vdash G}\ \text{MON}$$

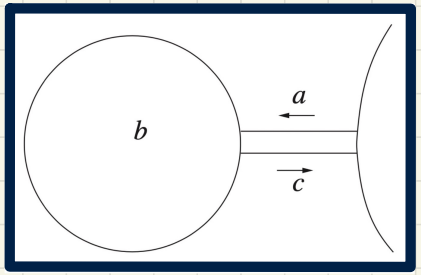
$$\frac{}{P \vdash \top}\ \text{TRUE\_R}$$

$$d \in \mathbb{N}$$
$$d > 0$$
$$\vdash$$
$$0 = 0 \lor 0 = 0$$

init/inv1_5/INV

Bridge Controller: Guarded Actions of "new" Events in 1st 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 : $a = 0 \vee c = 0$

IL_in: A car enters **island** (getting off the **bridge**).

IL_in
when
??
then
??
end

IL_out: A car exits **island** (getting on the **bridge**).

IL_out
when
??
then
??
end

Before-After Predicates of Event Actions: 1st Refinement

IL_in
when
$a > 0$
then
$a := a - 1$
$b := b + 1$
end

IL_out
when
$b > 0$
$a = 0$
then
$b := b - 1$
$c := c + 1$
end

- Pre-State
- Post-State
- Sate Transition

Concrete State Space