Lecture 13 - March 2

Reactive System: Bridge Controller

model

const. var.

Axioms Inv.

evt.

generate

Proof obligations (POs)

(sequents)

⋮

⊢

⋮

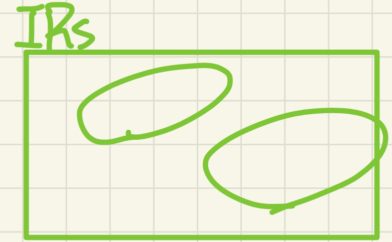
not necessarily provable.

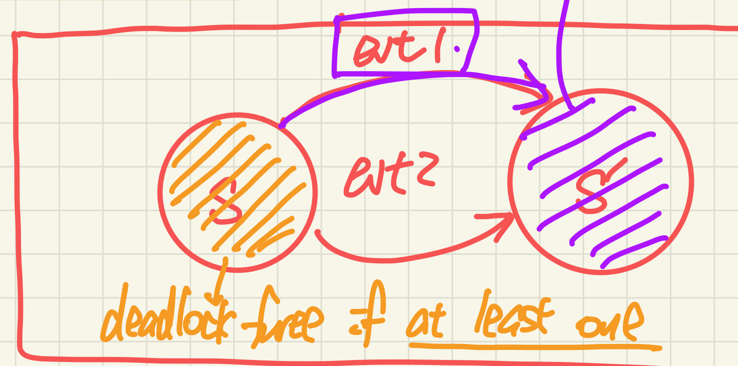
↳ Inv. establishment

Inv. preservation

not provable ⇒ fix model

after re-generating seq.; try again





deadlock-free if at least one evt is enabled.

after the evt's action takes effect, inv. should be preserved.

PO Rule: Deadlock Freedom

REQ4	Once started, the system should work for ever.

constants: d

variables: n

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

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

$m = 2$

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

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

$A(c)$ axioms
$I(c, \mathbf{v})$ invariant held at pre-state
$\vdash$
$G_1(c, \mathbf{v}) \vee \cdots \vee G_m(c, \mathbf{v})$ pre-state

DLF

- c: list of ***constants*** $\langle d \rangle$
- $A(c)$: list of ***axioms*** $\langle$**axm0_1**$\rangle$
- $\mathbf{v}$ and $\mathbf{v'}$: list of ***variables*** in ***pre***- and ***post***-states $\mathbf{v} \mathrel{\widehat{=}} \langle n \rangle$, $\mathbf{v'} \mathrel{\widehat{=}} \langle n' \rangle$
- $I(c, v)$: list of ***invariants*** $\langle$**inv0_1**, **inv0_2**$\rangle$
- $G(c, v)$: the event's ***guard***

$G(\langle d \rangle, \langle n \rangle)$ of $ML\_out \mathrel{\widehat{=}} n < d$, $G(\langle d \rangle, \langle n \rangle)$ of $ML\_in \mathrel{\widehat{=}} n > 0$

↳ disjunction of guards of all events held True

Exercise: Generate Sequent from the DLF rule.

$$\begin{array}{l} d \in \mathbb{N} \\ n \in \mathbb{N} \\ n \leq d \end{array} \vdash \underbrace{n < d}_{G_{ML\_out}} \vee \underbrace{n > 0}_{G_{ML\_in}}$$

PO	(v) pre-state	(v') post-state
INV est.	✗	✓
INV pre.	✓	✓
DLF	✓	✗

Example Inference Rules

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

appears to the Left of $\vdash$

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

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

H(E) replaced for free occurrences of E by F

application from L to R

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

$P \Rightarrow (E = E)$

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

application from R to L

$$\frac{H(\underset{L}{E}), E = F \vdash P(\underset{L}{E})}{H(\underset{R}{F}), \underset{L}{E} = \underset{R}{F} \vdash P(\underset{R}{F})}\ \textbf{EQ\_RL}$$

$$\frac{H(E),\, E = F \;\vdash\; P(E)}{H(F),\, \underset{F}{\cancel{E}} = \underset{E}{\cancel{F}} \;\vdash\; P(F)}\ \mathbf{EQ\_}\cancel{\mathbf{RL}}\ \mathrm{LR}$$

Discharging PO of DLF: First Attempt

$$\frac{H1 \vdash G}{H1, H2 \vdash G}\ \textbf{MON} \qquad \frac{H, P \vdash R \qquad H, Q \vdash R}{H, P \lor Q \vdash R}\ \textbf{OR\_L} \qquad \frac{H \vdash P}{H \vdash P \lor Q}\ \textbf{OR\_R1}$$

$$\frac{}{H, P \vdash P}\ \textbf{HYP} \qquad \frac{H(F), E = F \vdash P(F)}{H(E), E = F \vdash P(E)}\ \textbf{EQ\_LR} \qquad \frac{H \vdash Q}{H \vdash P \lor Q}\ \textbf{OR\_R2}$$

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

$n<d \lor n=d$

$$\begin{array}{l} d \in \mathbb{N} \\ n \in \mathbb{N} \\ n<d \lor n=d \\ \vdash \\ n<d \lor n>0 \end{array} \xrightarrow{\text{ARI}}$$

$$\xrightarrow{\text{MON}} \quad n<d \lor n=d \vdash n<d \lor n>0 \quad \xrightarrow{\text{OR\_L}}$$

$$n<d \vdash n<d \lor n>0 \quad \xrightarrow{\text{OR\_R1}} \quad n<d \vdash n<d \quad \text{HYP}$$

$$\underbrace{n}_{E}=\underbrace{d}_{F} \vdash n<d \lor n>0 \quad \xrightarrow{\text{EQ\_LR}} \quad n=d \vdash d<d \lor d>0 \quad \xrightarrow{\text{OR\_R2}} \quad \vdash d>0$$

MON

unprovable

Understanding the Failed Proof on DLF

constants: d

variables: n

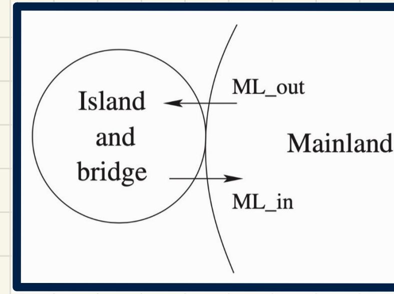
axioms:
axm0_1 : $\boxed{d \in \mathbb{N}}$ ✓

fix: axm0_2: $\boxed{d > 0}$

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

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

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



Unprovable Sequent: $\vdash \boxed{d > 0}$ may be violated

↳ its negation may be true

$\neg(d > 0)$ is allowed by the current model

↳ ① $d \leq 0$ ✓

② $d \in \mathbb{N}$ $(d \geq 0)$ ✓

↳ $\boxed{d = 0}$.

0

Say $d = 0$,

after init: $n = 0$ $\quad 0 < 0$

deadlock free: $[\cancel{n}_0 < \cancel{d}_0 \vee \cancel{n}_0 > 0]$ $\quad 0 > 0 \equiv F$

Discharging PO of DLF: Second Attempt

$$\boxed{\begin{array}{l} d \in \mathbb{N} \quad < d>0 \\ n \in \mathbb{N} \\ n \leq d \\ \vdash \\ n < d \lor n > 0 \end{array}}$$

$\equiv$

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

MON

$d > 0$

$$\boxed{\begin{array}{l} n < d \lor n = d \\ \vdash \\ n < d \lor n > 0 \end{array}} \ \textbf{OR\_L} \left\{ \begin{array}{l} \boxed{\begin{array}{l} n < d \\ \vdash \\ n < d \lor n > 0 \end{array}} \ \textbf{OR\_R1} \ \boxed{\begin{array}{l} n < d \\ \vdash \\ n < d \end{array}} \ \textbf{HYP} \\ d > 0 \\ \boxed{\begin{array}{l} n = d \\ \vdash \\ n < d \lor n > 0 \end{array}} \ \textbf{EQ\_LR, MON} \ \boxed{\begin{array}{l} d > 0 \\ \vdash \\ d < d \lor d > 0 \end{array}} \ \textbf{OR\_R2} \ \boxed{\begin{array}{l} d > 0 \\ \vdash \\ d > 0 \end{array}} \ \textbf{?} \end{array} \right.$$

HYP.

Discharging PO of DLF: Second Attempt

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

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

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

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

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

$d \in \mathbb{N}$
$d > 0$
$n \in \mathbb{N}$
$n \leq d$
$\vdash$
$n < d \lor n > 0$

Summary of the Initial Model: Provably Correct

static

dynamic

constants: d

axioms:
axm0_1 : $d \in \mathbb{N}$
$\boxed{\textbf{axm0\_2} : d > 0}$

deadlock freedom

variables: n

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

init
begin
$n := 0$
end

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

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

INV-Preservation

Correctness Criteria:

+ Invariant Establishment
+ Invariant Preservation
+ Deadlock Freedom