Lecture 15 - Oct 30

Bridge Controller

Revising M0: Adding Event Guards
Initializing System, Establishing Inv.
Deadlock Free: Intro, PO, 1st Attempt

PO/VC Rule of Invariant Preservation: Revised M0

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 when $n < d$
begin
$n := n + 1$
end

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

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

Q. How many PO/VC rules for model m0? 4

Discharging POs of revised m0: Invariant Preservation

ML_out/inv0_1/INV

Ex.

$$\begin{array}{l} d \in \mathbb{N} \\ n \in \mathbb{N} \\ n \leq d \\ n < d \\ \vdash \\ n + 1 \in \mathbb{N} \end{array}$$

ML_in/inv0_1/INV

$$\begin{array}{l} d \in \mathbb{N} \\ n \in \mathbb{N} \\ n \leq d \\ n > 0 \\ \vdash \\ n - 1 \in \mathbb{N} \end{array}$$

new guard for ML_in

MON

$$\boxed{\begin{array}{l} n > 0 \\ \vdash \\ n - 1 \in \mathbb{N} \end{array}}$$

P2'

ML_out/inv0_2/INV

$$\begin{array}{l} d \in \mathbb{N} \\ n \in \mathbb{N} \\ n \leq d \\ n < d \\ \vdash \\ n + 1 \leq d \end{array}$$

new guard for ML_out

MON

$$\boxed{\begin{array}{l} n < d \\ \vdash \\ n + 1 \leq d \end{array}}$$

INC

ML_in/inv0_2/INV

Ex.

$$\begin{array}{l} d \in \mathbb{N} \\ n \in \mathbb{N} \\ n \leq d \\ n > 0 \\ \vdash \\ n - 1 \leq d \end{array}$$

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

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

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

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

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

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

Initializing the System

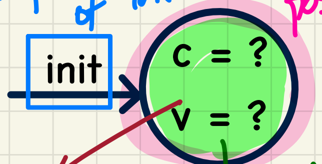
$d \in \mathbb{N}$, $n \in \mathbb{N}$, $n \leq d$, $n < d$ $\vdash$ $n+1 \in \mathbb{N}$	$d \in \mathbb{N}$, $n \in \mathbb{N}$, $n \leq d$, $n < d$ $\vdash$ $n+1 \leq d$	$d \in \mathbb{N}$, $n \in \mathbb{N}$, $n \leq d$, $n > 0$ $\vdash$ $n-1 \in \mathbb{N}$	$d \in \mathbb{N}$, $n \in \mathbb{N}$, $n \leq d$, $n > 0$ $\vdash$ $n-1 \leq d$

Analogy to Induction:

Base Cases ≈ Establishing Invariants

no pre-state of init

post-state of init



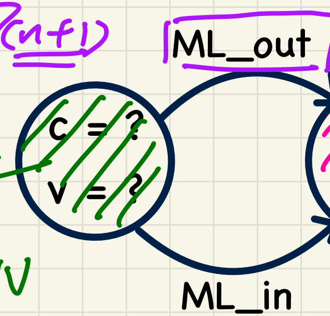
post-state of event (primed version of variables)

establishing INV for the first time.

Analogy to Induction:

Inductive Cases ≈ Preserving Invariants

$P(n) \Rightarrow P(n+1)$



pre-state assumed to satisfy INV

show that it's provable for the event to preserve INV

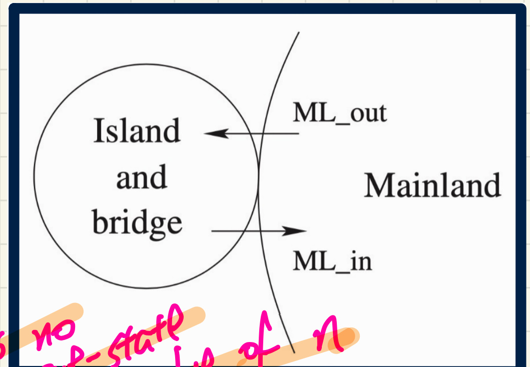
The Initialization Event

init
begin
$n := 0$
end

the only event that should be unguarded (initialization is always possible)

constants

$n := n + 1$ not valid init action ∵ there's no pre-state value of n



PO of Invariant Establishment

constants: d	variables: n	init begin $\boxed{n := 0}$ end
axioms: axm0_1 : $d \in \mathbb{N}$	invariants: inv0_1 : $n \in \mathbb{N}$ inv0_2 : $n \leq d$	

BAP: $n' = 0$

$E(c, v)$ → regular evt can ref. variables

effect of non-init event

Components

$K(c)$: effect of init's actions

$v' = K(c)$: BAP of init's actions

init evt can only ref. constants (no v).

Rule of Invariant Establishment

$$\frac{\begin{array}{c} \boxed{A(c)} \\ \vdash \\ I_i(c, K(c)) \end{array}}{} \quad \text{INV}$$

axioms

no invariants assumed ∵ not established yet.

index of INV

Exercise:

Generate Sequents from the INV rule.

$$\frac{\text{init/inv0\_1/INV}}{\begin{array}{c} d \in \mathbb{N} \\ \vdash \\ n' \in \mathbb{N} \\ 0 \in \mathbb{N} \end{array}} \qquad \frac{\text{init/inv0\_2/INV}}{\begin{array}{c} d \in \mathbb{N} \\ \vdash \\ n' \leq d \\ 0 \leq d \end{array}}$$

Discharging PO of Invariant Establishment

$$\boxed{\begin{array}{l} d \in \mathbb{N} \\ \vdash \\ 0 \in \mathbb{N} \end{array}} \quad \underline{\text{init/inv0\_1/INV}}$$

P_1 ✗

MON

$$\boxed{\begin{array}{l} \vdash \\ 0 \in \mathbb{N} \end{array}}$$

P_1

$$\boxed{\begin{array}{l} d \in \mathbb{N} \\ \vdash \\ 0 \leq d \end{array}} \quad \underline{\text{init/inv0\_2/INV}}$$

P_3

where n is instantiated by d

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

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

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

Bridge Controller : REACTIVE SYSTEM

↳ $\boxed{\text{there's always at least one event enabled for the system to progress}}$

unacceptable : $\boxed{\text{deadlock}}$ no event enabled to occur

$$\neg G(ML\_out) \land \neg G(ML\_in)$$ [deadlock condition]

$$\text{''} \quad \neg(G(ML\_out) \lor G(ML\_in))$$

$$G(ML\_out) \lor G(ML\_in)$$ [deadlock freedom cond.]

PO Rule: Deadlock Freedom

event enableness in pre-state

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 : $n \leq d$

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

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

$$\begin{array}{l} A(c) \quad \text{axioms} \\ I(c, \mathbf{v}) \quad \text{invariants} \\ \vdash \\ G_1(c, \mathbf{v}) \vee \cdots \vee G_m(c, \mathbf{v}) \end{array} \quad \text{DLF}$$

at least one of the m events is enabled.

DLF ≅ deadlock freedom

- 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 $ML\_in \mathrel{\widehat{=}} n > 0$

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	(n) pre-state	(n') post-state
inv. est.	✗	✓
inv. pre.	✓	✓
DLF	✓	✗

Example Inference Rules

$\top$ true
$\bot$ false

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

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

false $\Rightarrow P \equiv$ True

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

$P \Rightarrow$ True $\equiv$ True

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

L R

replace every free occurrence of E by F

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

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

L R

Discharging PO of DLF: First Attempt

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

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

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

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

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

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

$\mathbf{E}$: n, $\mathbf{F}$: d

$\cancel{n} < d \lor \cancel{n} > 0$

d   d

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

DLF

$\equiv$

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

MON

$n < d \lor n = d \vdash n < d \lor n > 0$ **OR_L**

L   R

- $n < d \vdash n < d \lor \boxed{n > 0}$ **OR_R1** $n < d \vdash \boxed{n < d}$ **HYP**
- $n = d \vdash \boxed{n < d \lor n > 0}$ **EQ_LR, MON** $\vdash \boxed{\underbrace{d < d}_{\text{false}} \lor d > 0}$ **OR_R2** $\vdash d > 0$ **?**

unprovable given no additional hypo-theses

alt. $\boxed{\vdash d < d \lor d > 0}$ ORI $\boxed{\vdash \text{false} \lor d > 0}$ ORI $\boxed{\vdash d > 0}$

$d < d \equiv \text{false}$

$\text{false} \lor P \equiv P$