Lecture 12 - February 28

Reactive System: Bridge Controller

Announcements

- Released: WrittenTest1, Lab2 solution
- To be released:
  + ProgTest1 Guide (by the end of Wednesday)
  + ProgTest1 practice questions (by Thursday class)

Recap of Previous Classes

Req. Doc.

+ Before-After Predicates
+ Example IRs

REQ2	The number of cars on bridge and island is limited.

constants: d

variables: n

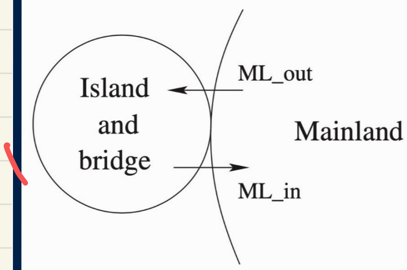
axioms:
axm0_1 : $d \in \mathbb{N}$

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

ML_out
begin
$n := n + 1$
end

$n' = n + 1$

ML_in
begin
$n := n - 1$
end



1. $A \Rightarrow C \equiv$ True

2. To prove C, it's sufficient to prove A

$$\begin{array}{c} H \\ \vdash \\ G \end{array}$$

sequent
$H \overset{?}{\Rightarrow} G$

$$\begin{array}{l} A(c) \\ I(c, v) \\ G(c, v) \\ \vdash \\ I_i(c, E(c, v)) \end{array}$$

Proof obligation

ML_out/inv0_1/INV

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

inference rule.

$$\frac{A}{\boxed{C}}\ \mathbf{L}$$

ARI : basic arithmetic

Discharging POs of original m0: Invariant Preservation

ML_out/inv0_1/INV

$d \in \mathbb{N}$
$n \in \mathbb{N}$ H1
$n \leq d$
$\vdash$
$n + 1 \in \mathbb{N}$

~~P2~~ (∵ too many hypotheses).

MON

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

ML_in/inv0_1/INV

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

$n-1 \geq 0$
$n \geq 1$ $(n > 0)$

MON

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

?? may need to add a guard to ML_in.

ML_out/inv0_2/INV

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

MON

$n \leq d \vdash n+1 \leq d$

?? may need to add a guard to ML_out

ML_in/inv0_2/INV

$d \in \mathbb{N}$
$n \in \mathbb{N}$
$n \leq d$
$\vdash$ $n-1<d \vee n-1=d$
$n - 1 \leq d$

ARI

DEC ~~X~~ (can't apply directly)

$d \in \mathbb{N}$
$n \in \mathbb{N}$
$n \leq d$
$\vdash n-1<d \vee n-1=d$

MON

$n \leq d \vdash n-1<d \vee n-1=d$

OR_R1

$n \leq d \vdash n-1<d$ DEC

$n-1 \leq d$ vs. $n-1 < m$ d

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

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

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

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

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
$n := \boxed{n+1}$ $\leq d$
end

ML_in
when $n > 0$
begin
$n := \boxed{n-1}$ $n \in \mathbb{N}$?
end

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

ML_in/inv0_1/INV

$d \in \mathbb{N}$
$n \in \mathbb{N}$
$n \leq d$ $n > 0$
$\vdash$
$\boxed{n - 1 \in \mathbb{N}}$

$n - 1 \geq 0$
$n \geq 1$ $(n > 0)$

MON
$\boxed{n \in \mathbb{N}}$
$\vdash$
$n - 1 \in \mathbb{N}$
??

ML_out/inv0_2/INV

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

MON
$\boxed{n \leq d}$
$\vdash$
$n+1 \leq d$
??

Exercise

Discharging POs of revised m0: Invariant Preservation

ML_out/inv0_1/INV

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

ML_in/inv0_1/INV

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

ML_out/inv0_2/INV

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

ML_in/inv0_2/INV

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

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

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

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

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

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

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

Model

↳ static : constants, axioms

↳ dynamic : variables, invariants

Q: Is this model correct (w.r.t. inv. preservation)

sequents formulating the POs of inv. preservation

↳ any unprovable sequents

↳ fix model →

re-generate sequents

↳ prove again.

Lecture

Reactive System: Bridge Controller

Initial Model: Invariant Establishment

Initializing the System

diff pre-states for evt. occurrence

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

resulting post states

Analogy to Induction:

Base Cases ≈ Establishing Invariants

$\xrightarrow{\text{init}}$ c = ? v = ?

right after vars init.

only a single state to prove.

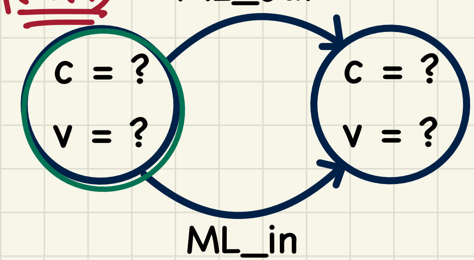
e.g. $n := n + 1$

not appropriate

Analogy to Induction:

Inductive Cases ≈ Preserving Invariants

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



The Initialization Event

no pre-state ← init → post-state

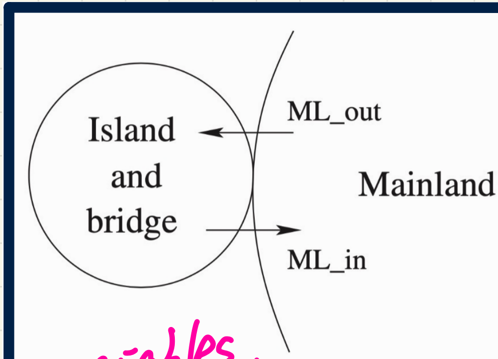
```
init
begin
  n := 0
end
```

name of evt.

variables only

when this evt occurs, none of the variables have been initialized

↳ RHS of := should not refer to variables.



PO of Invariant Establishment

Compare with effect of a non-init event: $E(c, \underline{\underline{v}})$

constants: d

variables: n

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

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

init
begin
$n := 0$
end

$n' = 0$

Components

$\boxed{K(c):}$ effect of init's actions

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

Rule of Invariant Establishment

$$\dfrac{A(c) \vdash I_i(c, K(c))}{} \quad \text{INV}$$

axioms

Exercise:

Generate Sequents from the INV rule.

$$\boxed{\begin{array}{l} d \in \mathbb{N} \\ \vdash \\ \cancel{n'} \in \mathbb{N} \end{array}}$$
0

init/ INV0_1/ INV

$$\boxed{\begin{array}{l} d \in \mathbb{N} \\ \vdash \\ \cancel{n'} \leq d \end{array}}$$
0

init/ INV0_2/ INV

Discharging PO of Invariant Establishment

$$d \in \mathbb{N} \vdash 0 \in \mathbb{N}$$

init/inv0_1/INV

MON

$$\vdash 0 \in \mathbb{N}$$

P1

$$d \in \mathbb{N} \vdash 0 \leq d$$

init/inv0_2/INV

P3

where n is instantiated by d

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

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

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

Lecture

Reactive System: Bridge Controller

Initial Model: Deadlock Freedom

want to prove:
system is deadlock-free : $G(ML\_out) \vee G(ML\_in)$

REACTIVE SYSTEMS

↳ deadlocks

↳ $\boxed{\text{no reaction}}$ to the user/env.

↳ no events can occur

↳ $\boxed{\text{None of events' guards is satisfied.}}$

deadlock cond.

$$\boxed{\neg\left(G(ML\_out) \vee G(ML\_in)\right)}$$

not the case that some event is enabled.

$\equiv \neg G(ML\_out) \wedge \neg G(ML\_in)$