Lecture 2

Part C

Case Study on Reactive Systems - Bridge Controller

Initial Model: Invariant Preservation

Design of Events: **Invariant** Preservation

variables: n

dynamic part
↳ values might change via actions of events

ML_out
begin
$n := n + 1$
end

ML_in
begin
$n := n - 1$
end

always enabled

guard: true

guard: true

enabled
↳ guards evaluating to true

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

✓ important properties of the system that must always hold true

$\forall s \bullet s \in StateSpace$
$\Rightarrow invariants(s)$
$\equiv$
$\neg(\exists s \bullet s \in StateSpace$
$\wedge \neg invariants(s))$

witness for disproving

the state space being consistent

may or may not be consistent

✓ State space: configurations
↳ variable values
constant values
invariants

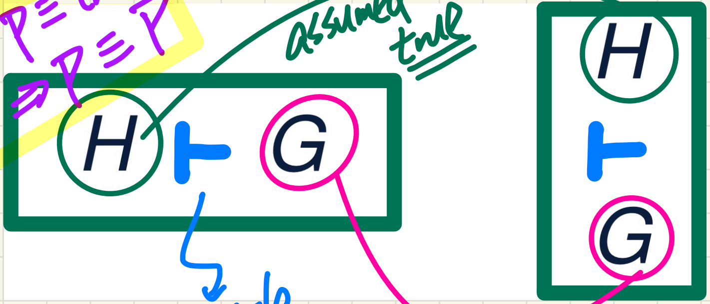
inconsistent s.s. if some ✓ combination of var. and c. violates the invariant.

Sequents: Syntax and Semantics

Syntax

zero of ⇒: false ⇒ P ≡ true

identity of ⇒: true ⇒ P ≡ P



assumed true

turnstile

hypotheses/assumptions (a set of predicates)

↳ might be empty

provable assuming H

goal (a set of predicates)

↳ should not be empty.

Semantics

$\boxed{H \vdash G}$ → a predicate → proved or disproved.

✓

$\boxed{H \vdash G \iff H \Rightarrow G}$

Q. What does it mean when **H** is empty/absent?

$\boxed{\vdash G}$ $\boxed{\begin{matrix}\vdash \\ G\end{matrix}}$ $\overset{?}{\equiv}$ ✗ $\boxed{false \vdash G}$ ✓ $\boxed{true \vdash G}$

↳ false ⇒ G ≡ true

↳ true ⇒ G ≡ G

PO/VC Rule of Invariant Preservation

Identity of $\land$: $P \land true \equiv P$

zero of $\land$: $P \land false \equiv false$

model m0

constants: d

substitute n' by expression on n according to the BAP

axioms:

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

Pre-State

$n \in \mathbb{N} \land n \le d$

variables: n

invariants:

→ **inv0_1** : $n \in \mathbb{N}$

→ **inv0_2** : $n \le d$

→ Post-State

$\underset{n+1}{n'} \in \mathbb{N} \land \underset{n-1}{n'} \le d$

guard: true

ML_out

begin

$n := n + 1$

end

BAP: $n' = n+1$

guard: true

ML_in

begin

$n := n - 1$

end

BAP: $n' = n-1$

Variable

n before-state

n' after-state

$$\begin{array}{c} H1 \\ \cancel{H2}\ \text{True} \\ \vdash \\ G \end{array} \equiv H1 \land \cancel{H2}^{\text{True}} \Rightarrow G$$

Axioms

Invariants Satisfied at *Pre-State*

↳ before state transition occurs

Guards of the Event

↳ true

⊢

Invariants Satisfied at *Post-State*

INV

↳ name of rule

PO/VC rule of invariant preservation

↳ for a single event

PO/VC Rule of Invariant Preservation: Components

$c \triangleq \langle d \rangle$

pre-state → $v \triangleq \langle n \rangle$

post-state → $v' \triangleq \langle n' \rangle$

constants: d

variables: n

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

$A(\langle d \rangle) \triangleq \langle axm0\_1 \rangle$

$A_1(\langle d \rangle) \triangleq axm0\_1$

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

$I(\langle d \rangle, \langle n \rangle) = \langle inv0\_1, inv0\_2 \rangle$

$I_1(\langle d \rangle, \langle n \rangle) = inv0\_1$

$I_2(\langle d \rangle, \langle n \rangle) = inv0\_2$

$G(\langle d \rangle, \langle n \rangle) \triangleq true$

ML_out $E(\langle d \rangle, \langle n \rangle) \triangleq \langle n+1 \rangle$
begin
$n := n + 1$
end

BAP: $n' = n+1$

$\langle n' \rangle = \langle n+1 \rangle$

$G(\langle d \rangle, \langle n \rangle) \triangleq true$

ML_in $E(\langle d \rangle, \langle n \rangle) \triangleq \langle n-1 \rangle$
begin
$n := n - 1$
end

BAP: $n' = n-1$ → $\langle n' \rangle = \langle n-1 \rangle$

Each PO rule should be instantiated for every event.

c: list of constants

A(c): list of axioms

v and v′: variables in pre- and post-state

I(c, v): list of invariants

G(c, v): guards of an event

↳ determines enabledness of event

E(c, v): effect of an event's actions

↳ values of variables in post-state i.t.o pre-state exp.

$v' = E(c, v)$: BAP of an event's actions

PO/VC Rule of Invariant Preservation: Sequents

for a single inv. condition, for a single event

Rule of PO (I.P.).

m0

constants: d

variables: n

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

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

Post-state:
$n' \in \mathbb{N}$
$n+1 \in \mathbb{N}$

$n' \leq d$
$n+1 \leq d$

ML_out
begin
$n := n + 1$
end

true guard

all invariants

ML_in
begin
$n := n - 1$
end

true guard

event enabled

hypotheses

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

pre-state

guard & effect of the event under consideration

goal

index of an inv. condition

post-state value i.t.o pre-state exp. specified in the event's actions.
↳ BAP.

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

* 1. # of events (state transitions)
2. # of invariant conditions

$|\{ML\_out, ML\_in\}| \times |\{inv0\_1, inv0\_2\}| = ④$

event / inv. cond. / kind of PO

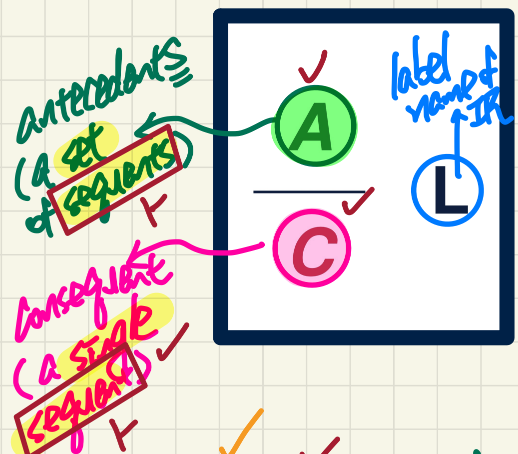
① ML_out/inv0_1/INV
② ML_out/inv0_2/INV

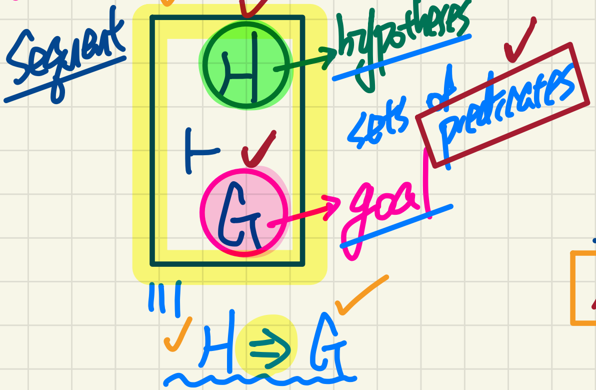
①
$d \in \mathbb{N}$
$n \in \mathbb{N}$
$n \leq d$
$\vdash n+1 \in \mathbb{N}$

②
$d \in \mathbb{N}$
$n \in \mathbb{N}$
$n \leq d$
$\vdash n+1 \leq d$

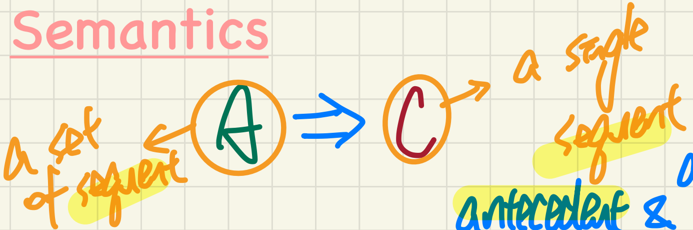
Inference Rule: Syntax and Semantics

Syntax



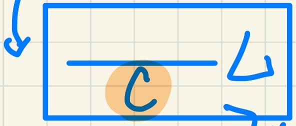


Semantics



Think of an IR is stating that an implication whose antecedent & consequence are both sets of predicates and that implication is an axiom ready to use

Q. What does it mean when **A** is empty/absent?



to prove C, nothing else to prove

Examples

IR1

$(H_1 \Rightarrow G)$

$\Rightarrow (H_1 \land H_2 \Rightarrow G)$

$H_1 \Rightarrow G$

$$\frac{H_1 \vdash G}{H_1 , H_2 \vdash G} \; MON$$

$\land$

monotonicity

$H_1 \land H_2 \Rightarrow G$

IR2

True

$\Rightarrow (n \in N \Rightarrow n+1 \in N)$

axiom $\equiv (n \in N \Rightarrow n+1 \in N)$

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

$n \in N \Rightarrow n+1 \in N$

Proof of Sequent: Steps and Structure

Outstanding Sequent to Prove

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

ML_out/inv0_1/INV

Known Inference Rules

Ⓐ

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

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

Ⓒ

$$\begin{array}{l} d \in \mathbb{N} \\ n \in \mathbb{N} \quad H1 \\ n \leq d \\ \vdash \\ n + 1 \in \mathbb{N} \end{array}$$

H2

MON

Ⓐ

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

P2

↑

to prove the original, outstanding sequent, it's sufficient to prove this instead.

Justifying Inference Rule: OR_L

$$\frac{\overset{\wedge}{\boxed{\cancel{H}, P \vdash R \qquad \cancel{H}, Q \vdash R}}}{\cancel{H}, P \vee Q \vdash R} \checkmark \ \textbf{OR\_L}$$

$$\boxed{(P \Rightarrow R) \wedge (Q \Rightarrow R)} \overset{\checkmark}{\Rightarrow} ((P \vee Q) \Rightarrow R)$$

$(p \Rightarrow R) \wedge (Q \Rightarrow R)$

$\equiv$ < def. of imp: $p \Rightarrow q \equiv \neg p \vee q$ >

$(\neg p \vee \underline{\underline{R}}) \wedge (\neg Q \vee \underline{\underline{R}})$

$\equiv$ < def. of dist. $\vee$ over $\wedge$: $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ >

$R \vee (\neg p \wedge \neg q)$ Q

$\equiv$ < de morgan : $\neg(p \vee q) \equiv \neg p \wedge \neg q$ >

$\neg(\underline{p \vee \overset{Q}{q}}) \vee \underline{R}$ $\equiv$ < def. of imp. > $p \vee \overset{Q}{q} \Rightarrow R$

Example Inference Rules

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

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

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

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

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

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

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

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

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

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

Discharging POs of original m0: Invariant Preservation

ML_out/inv0_1/INV

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

MON

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

PZ

ML_in/inv0_1/INV

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

MON

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

?

ML_out/inv0_2/INV

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

MON

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

?

ML_in/inv0_2/INV

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

MON

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

OR_R1

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

DEC

$\downarrow$

$\underline{n-1<d} \vee n-1=d$

Discharging POs of revised m0: Invariant Preservation

ML_out/inv0_1/INV

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

Exercise

ML_in/inv0_1/INV

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

MON

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

P2′

Conclusion

m0 as is is correct w.r.t Invariant Preservation

ML_out/inv0_2/INV

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

MON

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

INC

ML_in/inv0_2/INV

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

Exercise