Lecture 13 - Oct 23

Bridge Controller

Proof Obligation Rule: Inv. Preservation
Inference Rule: Syntax and Semantics
Sequent Proofs via Inference Rules

Announcements/Reminders

- Today's class: notes template posted
- ProgTest results to be released by next Tuesday's class
- WrittenTest1 results to be released by early Monday

PO/VC Rule of Invariant Preservation: Sequents

assume: all invariants hold in pre-state

constants: d	variables: n	✓ ML_out begin $n := n + 1$ end
axioms: axm0_1 : $d \in \mathbb{N}$	invariants: inv0_1 ✓: $n \in \mathbb{N}$ inv0_2 ✓: $n \leq d$	✓ ML_in begin $n := n - 1$ end

$A(c)$ axioms

$I(c, v)$ pre-state version of invariant

* $G(c, v)$ guards of some event

$\vdash$

** $I_i(c, E(c, v))$

post-state version of invariant

effect of the event's action

as a goal, prove invariant at index i: 1, 2.

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

* Guards of some events: ML_out or ML_in (2)

** Some invariant condition: inv0_1 or inv0_2 (2)

Total # of POs (sequents): 2 * 2 = 4

constants: d	variables: n

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

invariants:
inv0_1 : $n \in \mathbb{N}$
inv0_2 : $n \le d$
inv0_3 : ...

ML_out
begin
$n := n + 1$
end

ML_in
begin
$n := n - 1$
end

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

PO1: ML_out/inv0_1/INV invariant preservation

PO2: ML_out/inv0_2/INV

PO3: ML_in/inv0_1/INV

PO4: ML_in/inv0_2/INV

PO5: ML_out/inv0_3/INV

PO6: ML_in/inv0_3/INV

ML_out / $\overline{\text{inv}}$0_1 / $\boxed{\text{INV}}$

P.O. is related to whether or not taking a state transition via some event action can preserve/maintain inv0_1.

PO/VC Rule of Invariant Preservation: Sequents

constants: d

variables: n

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

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

ML_out ≤ true
begin
$n := n + 1$
end

BAP: $n' = n+1$

ML_in ≤ true
begin
$n := n - 1$
end

BAP: $n' = n-1$

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

PO1 : ML_out/inv0_1/INV

$d \in \mathbb{N}$
$n \in \mathbb{N}$
$n \leq d$
$\boxed{true}$
$\vdash$
$\cancel{n}^{\,n+1} \in \mathbb{N}$

PO2 : ML_in/inv0_2/INV

$d \in \mathbb{N}$
$n \in \mathbb{N}$
$n \leq d$
$\boxed{true}$
$\vdash$
$\cancel{n}^{\,n-1} \leq d$

Exercises

PO3 : ML_out/inv0_2/INV

PO4 : ML_in/inv0_1/INV

1. copy the inv.
2. adapt it to post-state
3. substitute each primed var. using BAP

Inference Rule: Syntax and Semantics

Syntax

antecedent
(a set of sequents)

$$\frac{A}{C}\; L$$

name of the inference rule

consequent
(a single sequent)

Semantics

$A \Rightarrow C \equiv True.$

$\boxed{\frac{}{C}}\; L$

$\equiv$

$\boxed{\frac{True}{C}}$ means C is an axiom

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

without any proof.

To prove the consequent C,
it's sufficient to prove the antecedent A instead.

rewriting

Examples

singleton set of sequents

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

MON
by monotonicity

a single sequent.

To prove $H_1, H_2 \vdash G$
it's sufficient to prove $\boxed{H_1 \vdash G}$

we can drop hypothesis.

Sequent

$$\boxed{\begin{array}{c} H \\ \vdash G \end{array}} \qquad H \Rightarrow G$$

(subject to prove)

e.g.

$$\boxed{\begin{array}{c} H_1 \\ H_2 \\ \vdash G \end{array}} \ \text{MON} \ \boxed{\begin{array}{c} H_1 \\ \vdash G \end{array}}$$

Inference Rule

$$\frac{A}{C}$$

may be used as a proof step.

↳ to make progress in proofs, rewrite C as A

$$A \Rightarrow C \equiv \text{True}$$

↳ (assumed to be true)

Proof of Sequent: Steps and Structure

Outstanding Sequent to Prove

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

ML_out/inv0_1/INV

Known Inference Rules

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

rewriting

relevant, useful

can be dropped

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

base case

$d \in \mathbb{N}$ → not relevant

$n \in \mathbb{N}$

$n \le d$ → not useful for arguing $n+1 \in \mathbb{N}$

$\vdash$

$n + 1 \in \mathbb{N}$ goal

MON

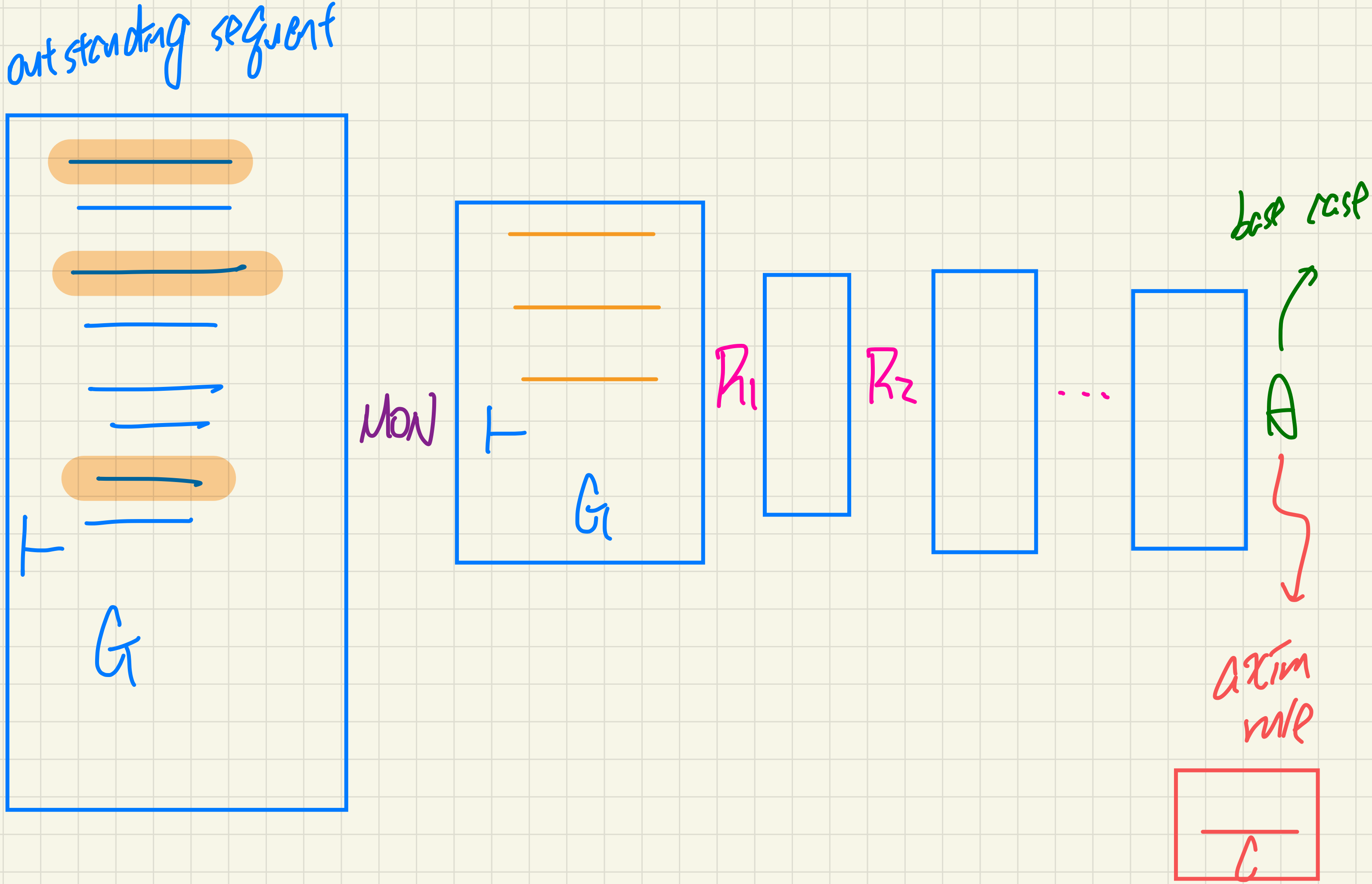
$n \in \mathbb{N}$
$\vdash$
$n+1 \in \mathbb{N}$

P2

* Analyze the goal predicate to prove:

Q1. what are the relevant vars?

Q2. what hypotheses are useful?


outstanding sequent
G
MON
G1
R1
R2
base case
axiom rule

Understanding Inference Rule: OR_L

OR_L
OR_R
AND_L

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

disjunction

OR appears to the L of $\vdash$

$$\frac{A}{C}$$

To prove C, sufficient to prove A

Q. Does OR_L help us: AND_R

$\boxed{\text{(A)}}$ split one sequent to prove into two sequents to prove

(B) Combine two sequents to prove into one sequent to prove.

$$\boxed{H,\ P \lor Q \vdash R} \quad \text{OR\_L} \quad \left\{ \begin{array}{l} \boxed{H,\ P \vdash R} \\[2ex] \boxed{H,\ Q \vdash R} \end{array} \right.$$

$$\frac{\checkmark H_2 \vdash G}{\boxed{H_1, H_2 \vdash G}}\ \text{MON}$$

to prove the L, sufficient to prove R.

$$\boxed{\begin{array}{l} H_1 \\ H_2 \\ \vdash G \end{array}} \quad \text{MON} \quad \boxed{\begin{array}{l} H_2 \\ \vdash G \end{array}}$$

$R \Rightarrow L$