Lecture 13 - Oct. 24

Bridge Controller

Proof Obligation of Inv. Preservation
Inference Rule: Syntax and Semantics

Announcements/Reminders

- ProgTest1 & WT1 results to be released next Monday.
- Lab4 released (ProgTest2 on November 6)
  + Try to complete Part 1 ASAP.
  + Follow the proof steps in Part 2 & collect questions.
  + Scheduled lab session on October 30.

↓
- Demo of Lab4 Part2
- Q&A -

PO/VC Rule of Invariant Preservation

verification condition

proof obligation

ML_out

pre I → post I'

constants: d

variables: n

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

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

model no

indices of INV

ML_out when True

begin
$n := n + 1$
end

BAP:

ML_in

begin
$n := n - 1$
end

(A) $n' \in \mathbb{N} \wedge n' \leq d$

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

Inv at post-state

(B) $n' = n+1$

$\equiv d \in \mathbb{N} \wedge n \in \mathbb{N} \wedge n \leq d \wedge \text{True}$

(new true in hypothesis section is implicitly a conjunction)

$d \in \mathbb{N}$, $n \in \mathbb{N}$, $n \leq d$, True ⊢ $n' \in \mathbb{N} \wedge n' \leq d$ *

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

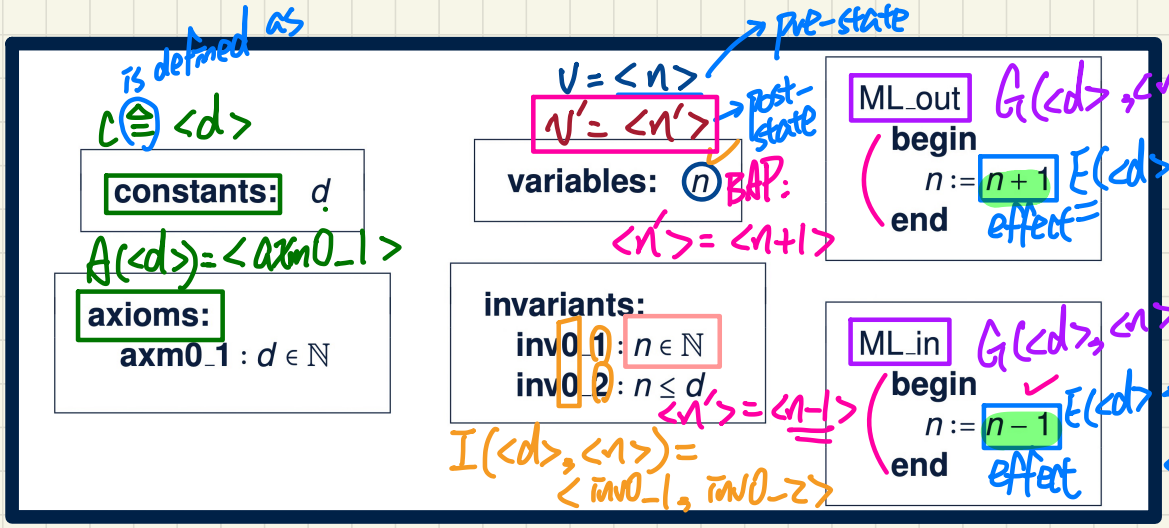
Axioms
Invariants Satisfied at *Pre-State*
Guards of the Event
ML_out
⊢
Invariants Satisfied at *Post-State*

INV

P.O. for INV. preservation

main-formed

PO/VC Rule of Invariant Preservation: Components



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

choice by predicate

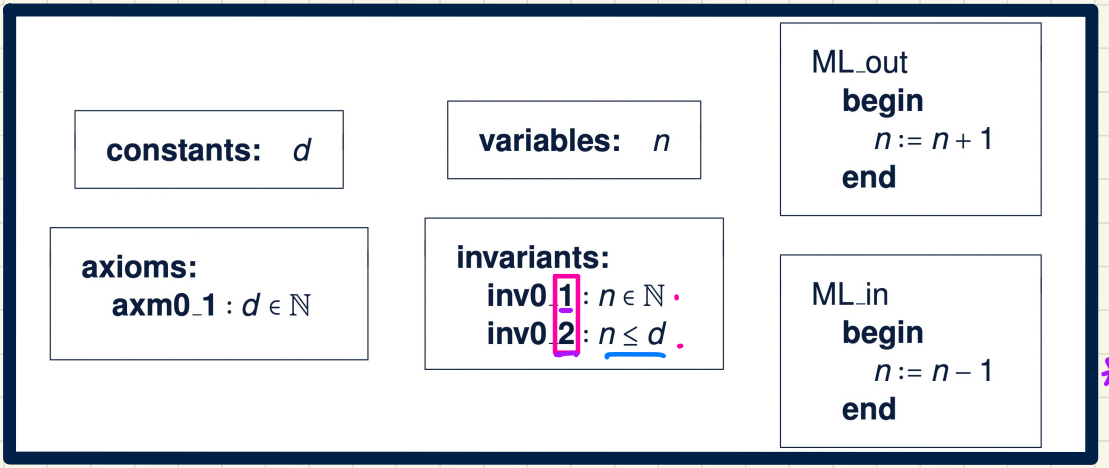
Swap.

$x, y :| x' = y \wedge y' = x$

change list of variables

post-state characterization (as a predicate)

PO/VC Rule of Invariant Preservation: Sequents



$A(c)$

$I(c, v)$ ← pre-state values

* $G(c, v)$

$\vdash$ effect of event

** $I_i(c, E(c, v))$ ← i=1, i=2

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

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

** Some all invariant conditions : inv0_1 or inv0_2 (2)

Total # of POs : 2 * 2 = 4.

PO1 : ML_out / inv0_1 / INV
(evt / inv. cond / nature of PO.)

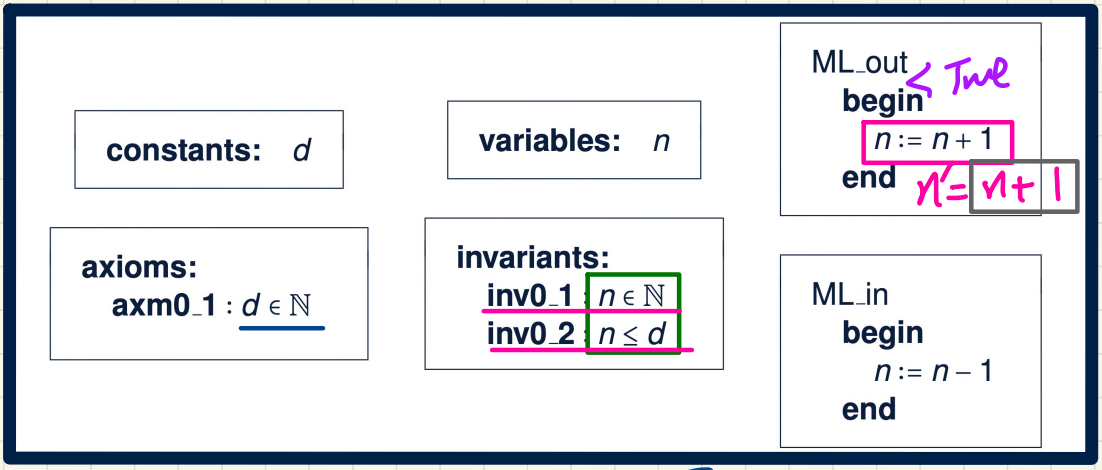
PO2 : ML_out / inv0_2 / INV

EXERCISE : PO3 & PO4 ?

M2_out / inv0_1 / INV

P.O. is related to whether or not taking a state transition of event M2_out can preserve/maintain inv0_1

PO/VC Rule of Invariant Preservation: Sequents



$A(c)$

$I(c, v)$

$G(c, v)$

$\vdash$

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

PO1 ML_out/INV0_1/INV

$d \in \mathbb{N}$

$n \in \mathbb{N}$

$n \leq d$

$\top$

$\vdash$

$n' \in \mathbb{N}$

$n+1$

PO2 ML_out/INV0_2/INV

$d \in \mathbb{N}$

$n \in \mathbb{N}$

$n \leq d$

$\top$

$\vdash$

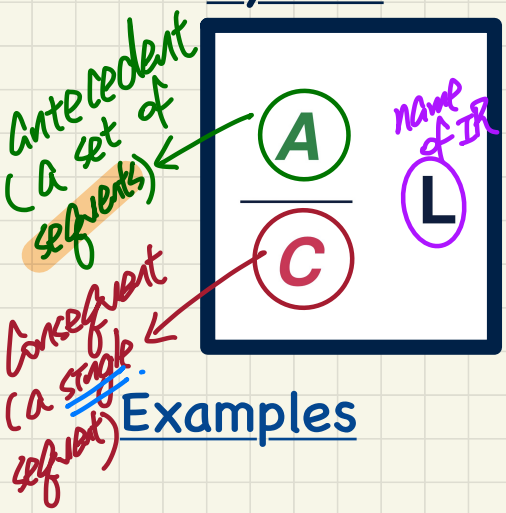
$n' \leq d$

$n+1$

Exercise : PO3 PO4

Inference Rule: Syntax and Semantics

Syntax



Semantics

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

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

Examples

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

MON = monotonicity.

To prove $H_1, H_2 \vdash G$

it's sufficient to prove

$H_1 \vdash G$