Lecture 15 - Oct. 31

Bridge Controller

Revising M0: Adding Event Guards
Re-Generating/Re-Proving PO Sequents

Announcements/Reminders

- Lab4 due tomorrow at **noon**
- ProgTest2 next Wednesday, November 6

* $n \le d \vdash n-1 < d$ DEC

Discharging POs of original m0: Invariant Preservation

ML_out/inv0_1/INV

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

✗ P2 ∵ too many irrelevant hypotheses.

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

ML_in/inv0_1/INV

$d \in \mathbb{N}$
$n \in \mathbb{N}$
$n \le d$
$\vdash$
$n-1 \in \mathbb{N}$ ← True guard of ML_tr

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

unprovable

new guard for ML_tr: $n > 0$

One possible resolution: add some guard condition of ML_tr, so that the extra hypotheses can make this seq. provable.

ML_out/inv0_2/INV

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

MON → $n \le d \vdash n < d \;\vee\; n+1 \le d$

new guard for ML_out: not provable ∵ n might be equal to d.

ML_in/inv0_2/INV

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

DEC ✗ → ARI $p \le q \equiv p < q \vee p = q$ → $d \in \mathbb{N}, n \in \mathbb{N}, n \le d \vdash n-1 < d \vee n-1 = d$

OR_R1 → $d \in \mathbb{N}, n \in \mathbb{N}, n \le d \vdash n-1 < d$ MON*

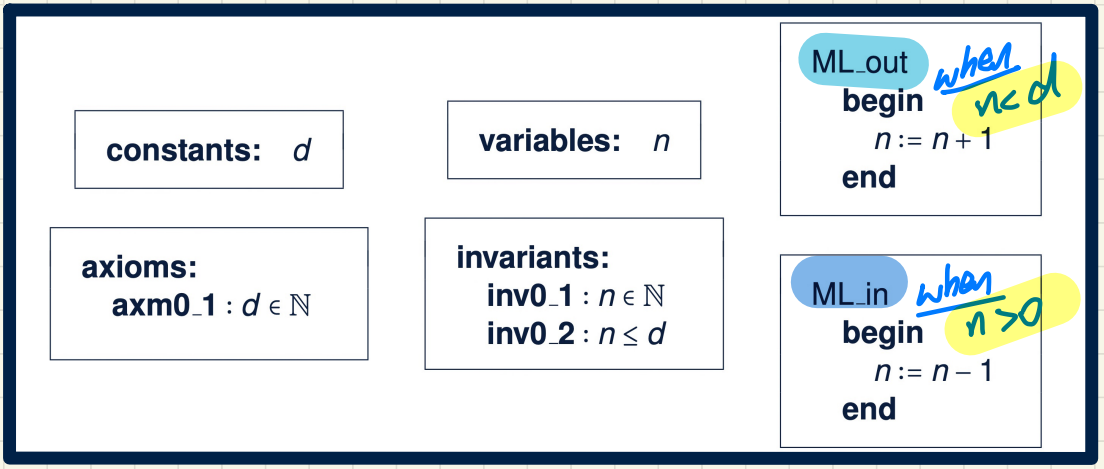
OR_R1: $\dfrac{H \vdash P}{H \vdash P \vee Q}$

MON: $\dfrac{H1 \vdash G}{H1, H2 \vdash G}$

DEC: $\dfrac{}{n \le m \vdash n-1 < m}$

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

PO/VC Rule of Invariant Preservation: Revised M0



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

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

Discharging POs of revised m0: Invariant Preservation

ML_out/inv0_1/INV — Ex.

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

ML_in/inv0_1/INV

$d \in \mathbb{N}$
$n \in \mathbb{N}$
$n \le d$
$n > 0$ — new guard for ML_in
$\vdash$
$n - 1 \in \mathbb{N}$

MON:
$n > 0$
$\vdash$
$n - 1 \in \mathbb{N}$
P2

ML_out/inv0_2/INV

$d \in \mathbb{N}$
$n \in \mathbb{N}$
$n \le d$
$n < d$ — new guard for ML_out
$\vdash$
$n + 1 \le d$

MON:
$n < d$
$\vdash$
$n + 1 \le d$
INC

ML_in/inv0_2/INV — Ex.

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

$$\frac{H \vdash P}{H \vdash P \vee Q}\ \text{OR\_R1} \qquad \frac{H1 \vdash G}{H1, H2 \vdash G}\ \text{MON}$$

$$\frac{}{n \le m \vdash n - 1 < m}\ \text{DEC} \qquad \frac{}{n < m \vdash n + 1 \le m}\ \text{INC}$$

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

Discharging PO of DLF: Second Attempt

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

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

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

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

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

$d \in \mathbb{N}$
$d > 0$
$n \in \mathbb{N}$
$n \le d$ ($n < d \vee n = d$)
$\vdash$
$n < d \vee n > 0$

ARI

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

MON

$n < d \vee n = d$
$\vdash$
$n < d \vee n > 0$

OR_L

$n < d$
$\vdash$
$n < d \vee n > 0$

OR_R1

$n < d$
$\vdash$
$n < d$

HYP

$n = d$
$\vdash$
$n < d \vee n > 0$