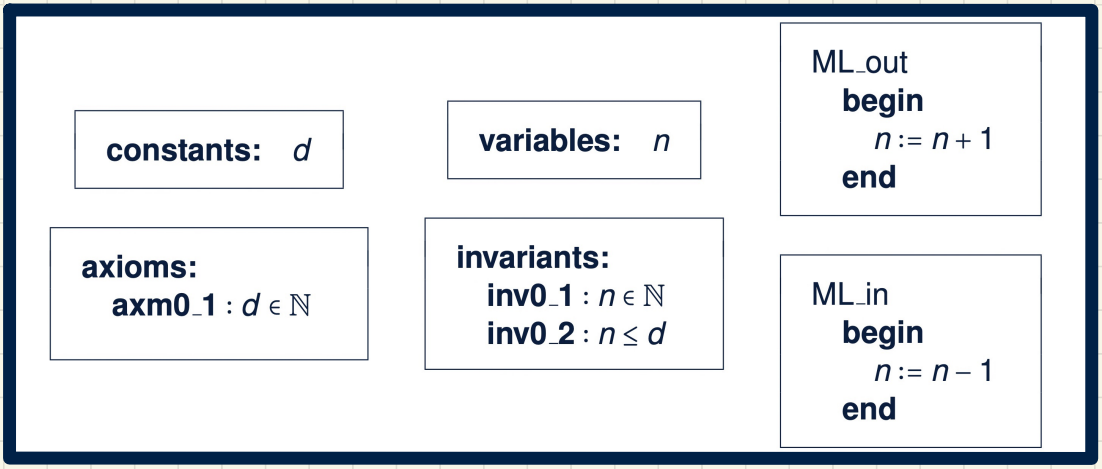
PO/VC Rule of Invariant Preservation: Revised M0



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

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

Discharging POs of revised m0: Invariant Preservation

ML_out/inv0_1/INV

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

ML_in/inv0_1/INV

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

ML_out/inv0_2/INV

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

ML_in/inv0_2/INV

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

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

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

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

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

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

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

Initializing the System

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

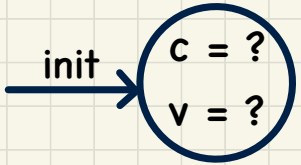
$d \in \mathbb{N}$ $n \in \mathbb{N}$ $n \le d$ $n < d$ ⊢ $n+1 \le d$

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

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

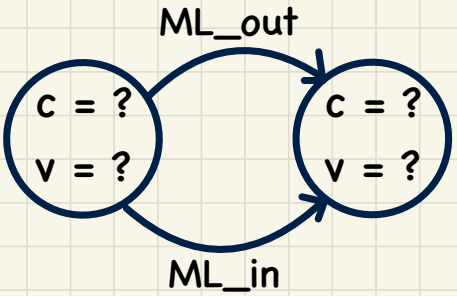
Analogy to Induction:

Base Cases ≈ Establishing Invariants



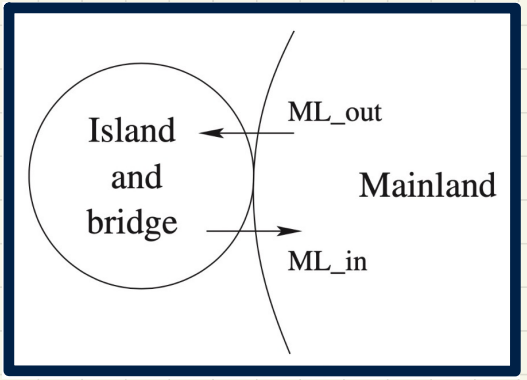
Analogy to Induction:

Inductive Cases ≈ Preserving Invariants

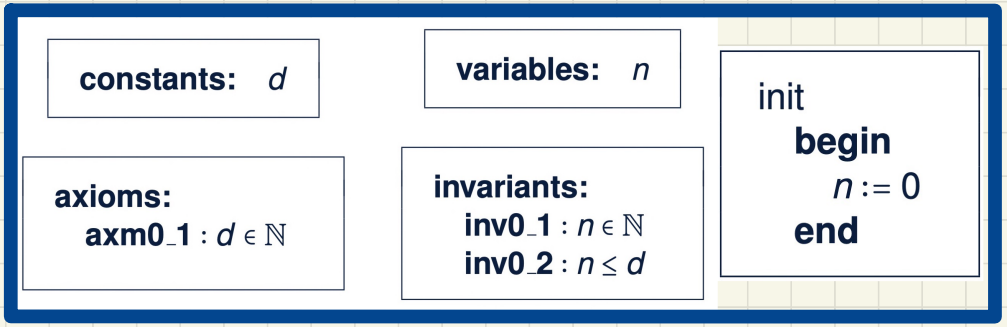


The Initialization Event

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



PO of Invariant Establishment



Components

K(c): effect of init's actions

v′ = K(c): BAP of init's actions

Rule of Invariant Establishment

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

Exercise:

Generate Sequents from the INV rule.

Discharging PO of Invariant Establishment

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

init/inv0_1/INV

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

init/inv0_2/INV

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

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

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

PO Rule: Deadlock Freedom

REQ4	Once started, the system should work for ever.

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
$n < d$
then
$n := n + 1$
end

ML_in
when
$n > 0$
then
$n := n - 1$
end

$$A(c)$$
$$I(c, v)$$
$$\vdash$$
$$G_1(c, v) \lor \cdots \lor G_m(c, v)$$

DLF

- c: list of ***constants*** $\langle d \rangle$
- $A(c)$: list of ***axioms*** $\langle$**axm0_1**$\rangle$
- v and v': list of ***variables*** in ***pre***- and ***post***-states $v \mathrel{\widehat{=}} \langle n \rangle$, $v' \mathrel{\widehat{=}} \langle n' \rangle$
- $I(c, v)$: list of ***invariants*** $\langle$**inv0_1**, **inv0_2**$\rangle$
- $G(c, v)$: the event's ***guard***

$G(\langle d \rangle, \langle n \rangle)$ of *ML_out* $\mathrel{\widehat{=}}$ $n < d$, $G(\langle d \rangle, \langle n \rangle)$ of *ML_in* $\mathrel{\widehat{=}}$ $n > 0$

Exercise: Generate Sequent from the **DLF rule**.

Example Inference Rules

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

$$\frac{}{\bot \vdash P}\ \textbf{FALSE\_L}$$

$$\frac{}{P \vdash \top}\ \textbf{TRUE\_R}$$

$$\frac{H(F), E = F \vdash P(F)}{H(E), E = F \vdash P(E)}\ \textbf{EQ\_LR}$$

$$\frac{}{P \vdash E = E}\ \textbf{EQ}$$

$$\frac{H(E), E = F \vdash P(E)}{H(F), E = F \vdash P(F)}\ \textbf{EQ\_RL}$$

Discharging PO of DLF: First Attempt

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

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

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

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

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

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