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

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

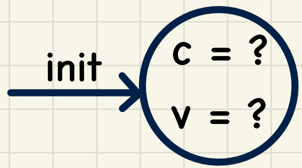
$d \in \mathbb{N}$, $n \in \mathbb{N}$, $n \leq d$, $n > 0$ $\vdash$ $n-1 \in \mathbb{N}$

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

Initializing the System

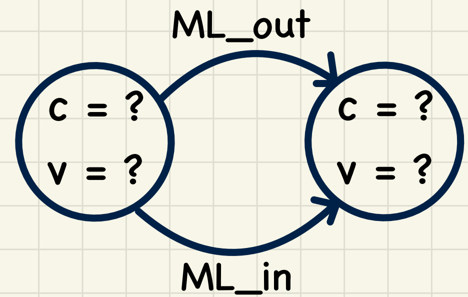
Analogy to Induction:

Base Cases ≈ Establishing Invariants



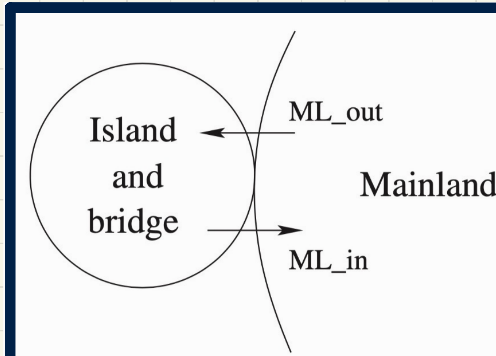
Analogy to Induction:

Inductive Cases ≈ Preserving Invariants



The Initialization Event

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



PO of Invariant Establishment

constants: d

variables: n

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

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

init
begin
$n := 0$
end

Components

K(c): effect of init's actions

v′ = K(c): BAP of init's actions

Rule of Invariant Establishment

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

$A(c)$
$\vdash$
$I_i(c, K(c))$ — 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

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

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

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

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

$$\begin{array}{l} A(c) \\ I(c, \mathbf{v}) \\ \vdash \\ G_1(c, \mathbf{v}) \vee \cdots \vee G_m(c, \mathbf{v}) \end{array} \quad \underline{\text{DLF}}$$

- c: list of ***constants*** $\langle d \rangle$
- $A(c)$: list of ***axioms*** $\langle \mathbf{axm0\_1} \rangle$
- $\mathbf{v}$ and $\mathbf{v'}$: list of ***variables*** in ***pre***- and ***post***-states $\mathbf{v} \mathrel{\widehat{=}} \langle n \rangle$, $\mathbf{v'} \mathrel{\widehat{=}} \langle n' \rangle$
- $I(c, v)$: list of ***invariants*** $\langle \mathbf{inv0\_1}, \mathbf{inv0\_2} \rangle$
- $G(c, v)$: 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

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

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

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

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

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

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

Discharging PO of DLF: First Attempt

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

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

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

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

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

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