Discharging PO of DLF: Revisiting First Attempt

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

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

$$\boxed{\begin{array}{l} d \in \mathbb{N} \\ n \in \mathbb{N} \\ n \leq d \\ \vdash \\ n < d \lor n > 0 \end{array}}$$

$\equiv$

$$\boxed{\begin{array}{l} d \in \mathbb{N} \\ n \in \mathbb{N} \\ n < d \lor n = d \\ \vdash \\ n < d \lor n > 0 \end{array}}$$

MON

$$\boxed{\begin{array}{l} n < d \lor n = d \\ \vdash \\ n < d \lor n > 0 \end{array}}\ \textbf{OR\_L} \left\{ \begin{array}{l} \boxed{\begin{array}{l} n < d \\ \vdash \\ n < d \lor n > 0 \end{array}}\ \textbf{OR\_R1}\ \boxed{\begin{array}{l} n < d \\ \vdash \\ n < d \end{array}}\ \textbf{HYP} \\ \\ \boxed{\begin{array}{l} n = d \\ \vdash \\ n < d \lor n > 0 \end{array}}\ \textbf{EQ\_LR}, \textbf{MON}\ \boxed{\begin{array}{l} \vdash \\ d < d \lor d > 0 \end{array}}\ \textbf{OR\_R2}\ \boxed{\begin{array}{l} \vdash \\ d > 0 \end{array}}\ \textbf{?} \end{array} \right.$$

what if EQ_RL was used?

Understanding the Failed Proof on DLF

constants: d

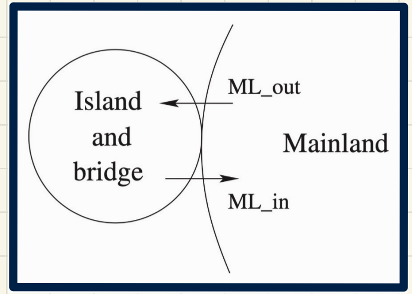
variables: n

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



Unprovable Sequent: $\vdash d > 0$

Discharging PO of DLF: Second Attempt

$$\begin{array}{l} d \in \mathbb{N} \\ n \in \mathbb{N} \\ n \leq d \\ \vdash \\ n < d \lor n > 0 \end{array}$$

$\equiv$

$$\begin{array}{l} d \in \mathbb{N} \\ n \in \mathbb{N} \\ n < d \lor n = d \\ \vdash \\ n < d \lor n > 0 \end{array}$$

MON

$$\boxed{\begin{array}{l} n < d \lor n = d \\ \vdash \\ n < d \lor n > 0 \end{array}} \quad \textbf{OR\_L} \left\{ \begin{array}{l} \boxed{\begin{array}{l} n < d \\ \vdash \\ n < d \lor n > 0 \end{array}} \quad \textbf{OR\_R1} \quad \boxed{\begin{array}{l} n < d \\ \vdash \\ n < d \end{array}} \quad \textbf{HYP} \\ \\ \boxed{\begin{array}{l} n = d \\ \vdash \\ n < d \lor n > 0 \end{array}} \quad \textbf{EQ\_LR, MON} \quad \boxed{\begin{array}{l} \\ \vdash \\ d < d \lor d > 0 \end{array}} \quad \textbf{OR\_R2} \quad \boxed{\begin{array}{l} \vdash \\ d > 0 \end{array}} \quad \textbf{?} \end{array} \right.$$

Discharging PO of DLF: Second Attempt

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

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

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

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

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

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

Summary of the Initial Model: Provably Correct

constants: d

axioms:
- **axm0_1** : $d \in \mathbb{N}$
- **axm0_2** : $d > 0$

variables: n

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

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

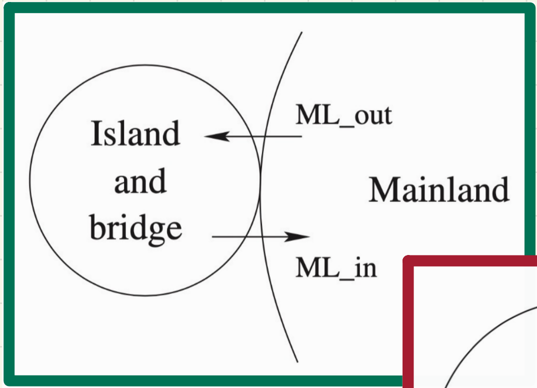
```
ML_out
  when
    n < d
  then
    n := n + 1
  end
```

```
ML_in
  when
    n > 0
  then
    n := n − 1
  end
```

Correctness Criteria:

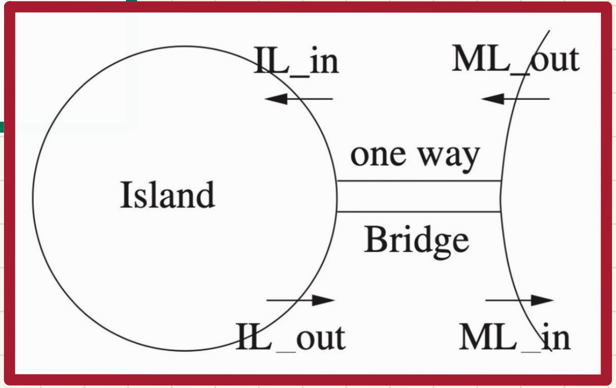
+ Invariant Establishment
+ Invariant Preservation
+ Deadlock Freedom

Bridge Controller: Abstraction in the 1st Refinement



m0:

initial, most abstract



m1:

second, more concrete

REQ1	The system is controlling cars on a bridge connecting the mainland to an island.
REQ3	The bridge is one-way or the other, not both at the same time.

Bridge Controller: State Space of the 1st Refinement

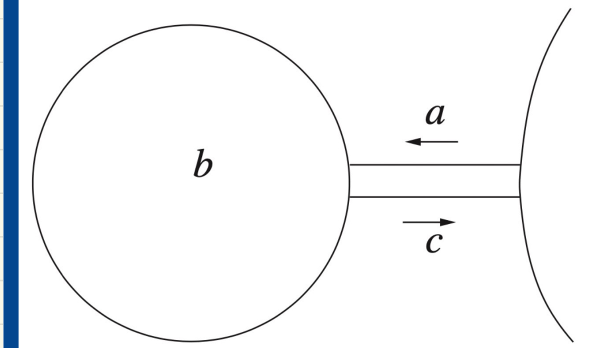
REQ1	The system is controlling cars on a bridge connecting the mainland to an island.
REQ3	The bridge is one-way or the other, not both at the same time.

Dynamic Part of Model

variables: a, b, c

invariants:

inv1_1 : $a \in \mathbb{N}$
inv1_2 : $b \in \mathbb{N}$
inv1_3 : $c \in \mathbb{N}$
inv1_4 : ??
inv1_5 : ??



Static Part of Model

constants: d

axioms:

axm0_1 : $d \in \mathbb{N}$
axm0_2 : $d > 0$

Exercises

inv1_4: linking abstract & concrete states
inv1_5: bridge is one-way