Understanding the Failed Proof on DLF

constants: d

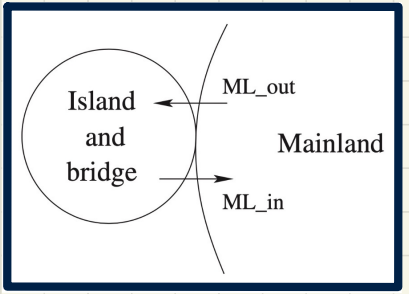
variables: n

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

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

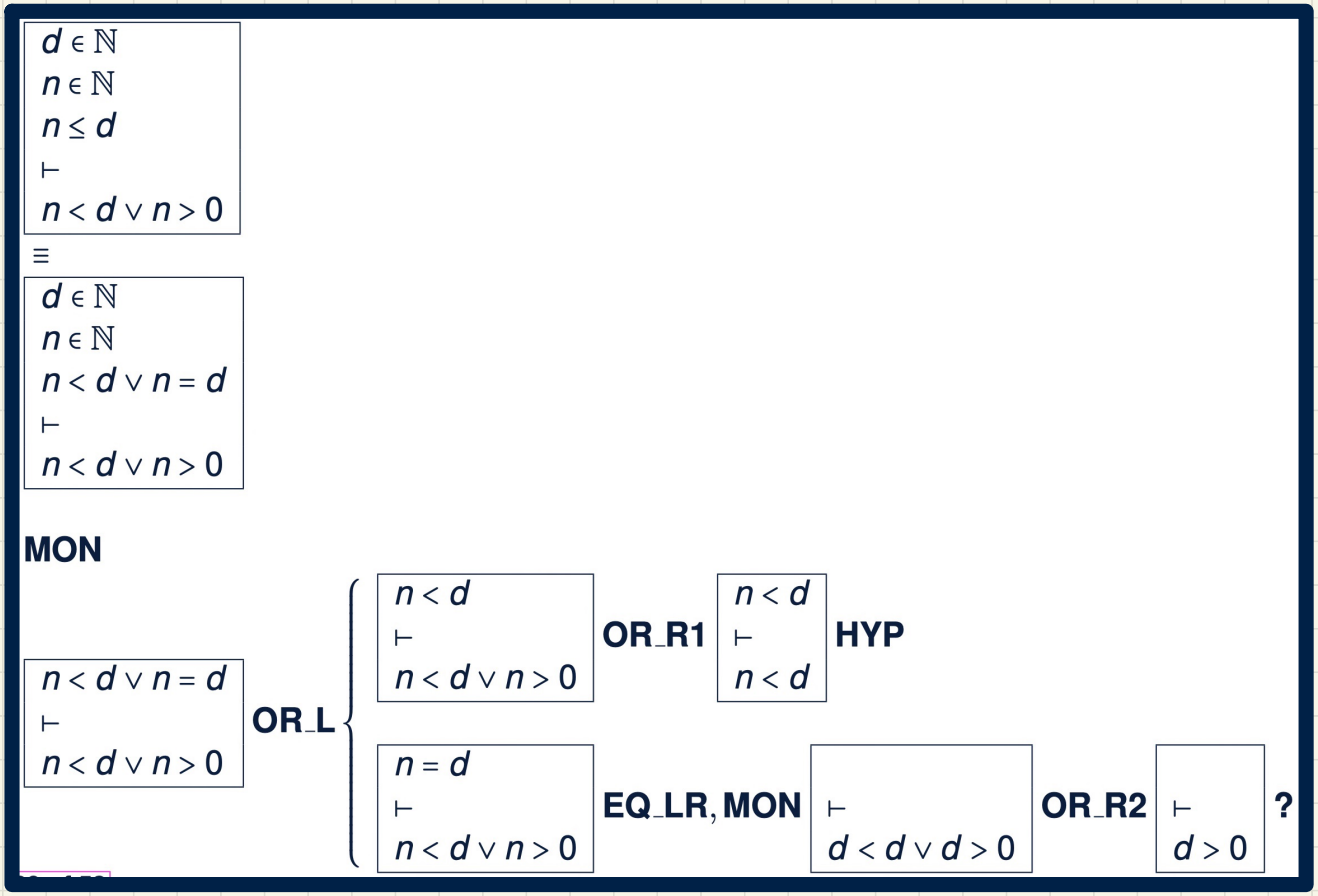
ML_out
when
$n < d$
then
$n := n + 1$
end

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

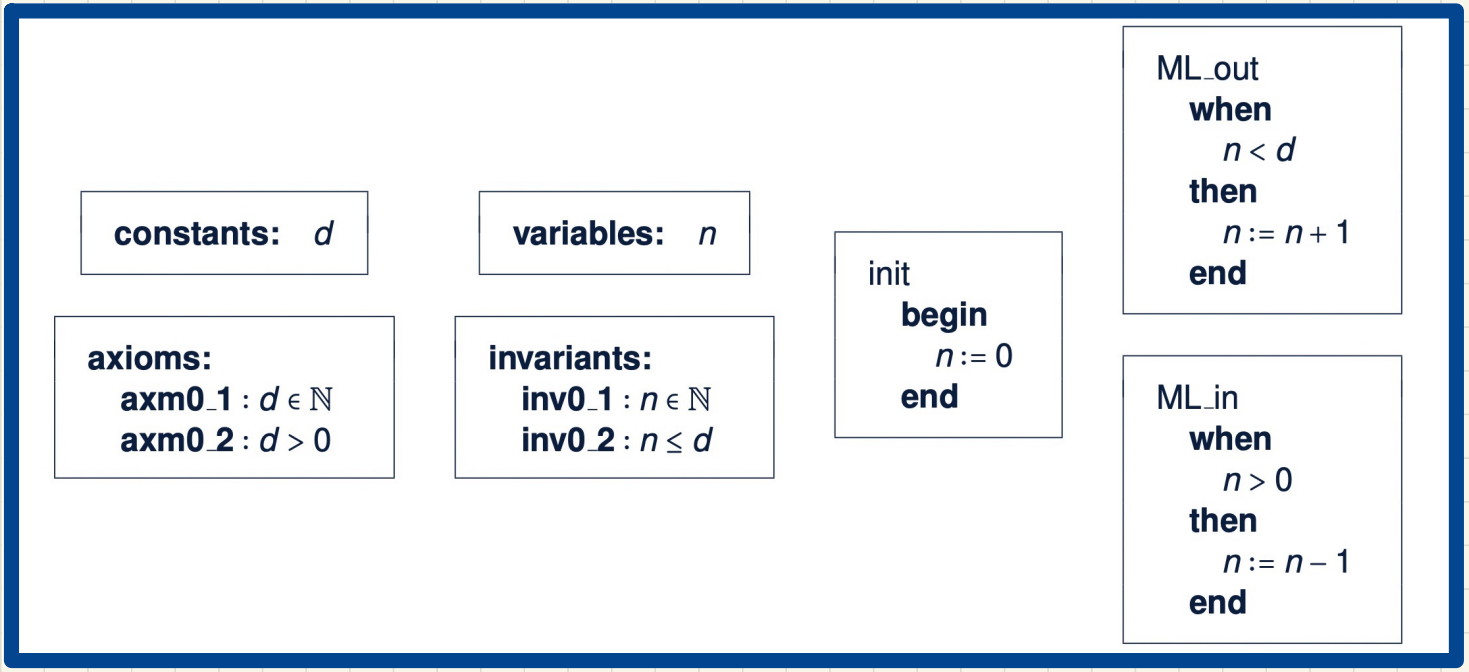


Unprovable Sequent: $\vdash d > 0$

Discharging PO of DLF: Second Attempt



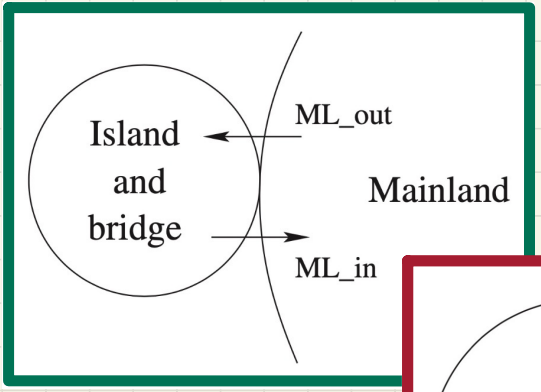
Summary of the Initial Model: Provably Correct



Correctness Criteria:

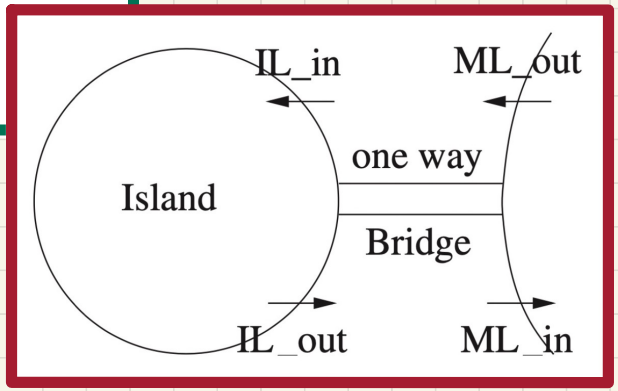
+ Invariant Establishment
+ Invariant Preservation
+ Deadlock Freedom

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

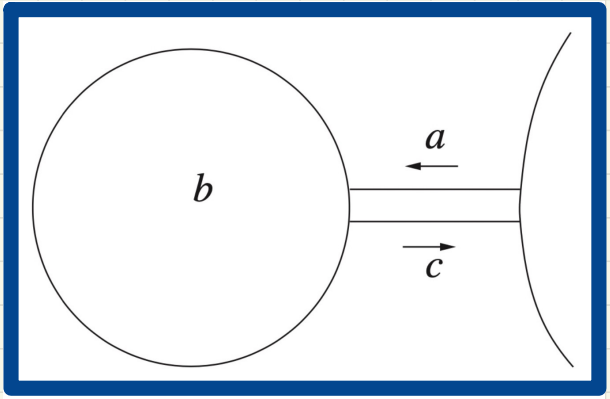
REQ1	The system is controlling cars on a bridge connecting the mainland to an island.
REQ3	The bridge is one-way or the other, not both at the same time.

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:

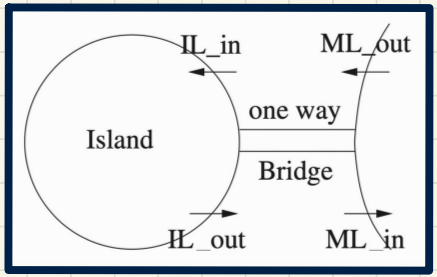
axm0_1 : $d \in \mathbb{N}$
axm0_2 : $d > 0$

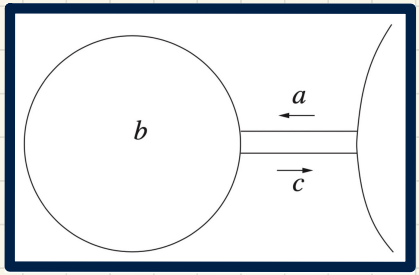
Exercises

inv1_4: linking abstract & concrete states

inv1_5: bridge is one-way

Bridge Controller: Guards of "old" Events 1st Refinement





ML_out: A car exits **mainland** (getting on the **bridge**).

ML_out
when
??
then
$a := a + 1$
end

constants: d

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

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 : $a + b + c = n$
inv1_5 : $a = 0 \lor c = 0$

ML_in: A car enters **mainland** (getting off the **bridge**).

ML_in
when
??
then
$c := c - 1$
end