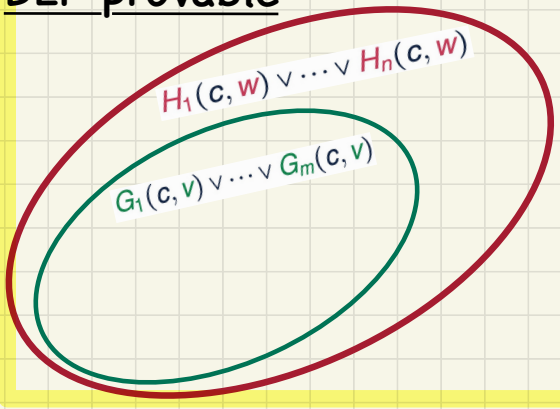
Idea of Relative Deadlock Freedom

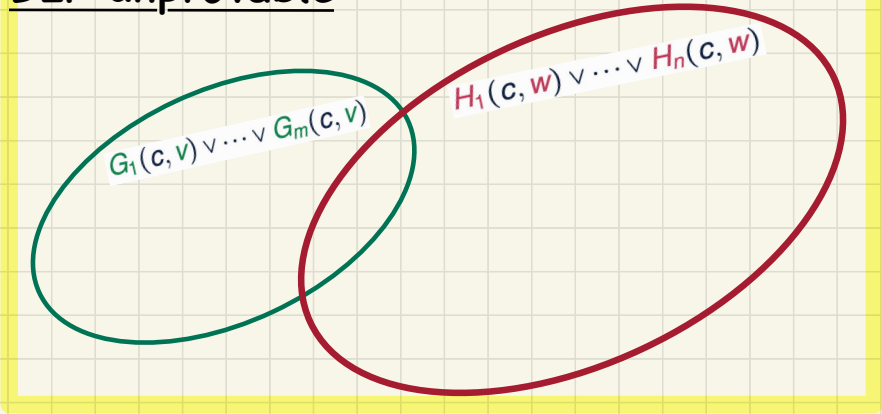
$$
\begin{array}{l}
A(c) \\
I(c, v) \\
J(c, v, w) \\
G_1(c, v) \vee \cdots \vee G_m(c, v) \\
\vdash \\
H_1(c, w) \vee \cdots \vee H_n(c, w)
\end{array}
$$

DLF

DLF provable



DLF unprovable



PO of Relative Deadlock Freedom

Abstract m0

variables: 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

Concrete m1

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 : $a = 0 \vee c = 0$

ML_out
when $a + b < d$ $c = 0$
then $a := a + 1$
end

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

IL_in
when $a > 0$
then $a := a - 1$ $b := b + 1$
end

IL_out
when $b > 0$ $a = 0$
then $b := b - 1$ $c := c + 1$
end

$$A(c)$$
$$I(c, v)$$
$$J(c, v, w)$$
$$G_1(c, v) \vee \cdots \vee G_m(c, v)$$
$$\vdash$$
$$H_1(c, w) \vee \cdots \vee H_n(c, w)$$

DLF

Discharging POs of m1: Relative Deadlock Freedom

Part 1

$$\frac{H1 \vdash G}{H1, H2 \vdash G}\ \textbf{MON} \qquad \frac{H(F), E = F \vdash P(F)}{H(E), E = F \vdash P(E)}\ \textbf{EQ\_LR} \qquad \frac{H, \neg P \vdash Q}{H \vdash P \vee Q}\ \textbf{OR\_R}$$

$d \in \mathbb{N}$
$d > 0$
$n \in \mathbb{N}$
$n \leq d$
$a \in \mathbb{N}$
$b \in \mathbb{N}$
$c \in \mathbb{N}$
$a + b + c = n$
$a = 0 \vee c = 0$
$n < d \vee n > 0$
$\vdash$
$\quad a + b < d \wedge c = 0$
$\vee \quad c > 0$
$\vee \quad a > 0$
$\vee \quad b > 0 \wedge a = 0$

Discharging POs of m1: Relative Deadlock Freedom

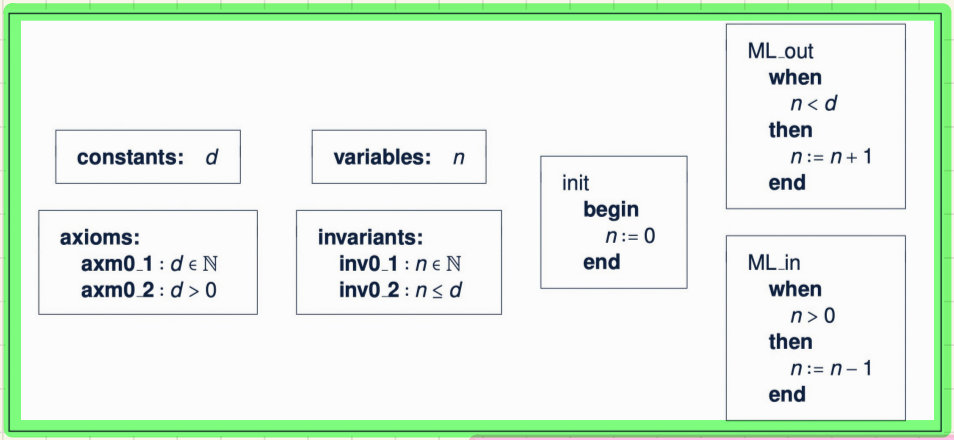
Part 2

$$\frac{H, P \vdash R \qquad H, Q \vdash R}{H, P \vee Q \vdash R}\ \text{OR\_L} \qquad \frac{H \vdash P}{H \vdash P \vee Q}\ \text{OR\_R1} \qquad \frac{}{P \vdash E = E}\ \text{EQ}$$

$$\frac{H \vdash P \qquad H \vdash Q}{H \vdash P \wedge Q}\ \text{AND\_R} \qquad \frac{H \vdash Q}{H \vdash P \vee Q}\ \text{OR\_R2} \qquad \frac{}{H, P \vdash P}\ \text{HYP}$$

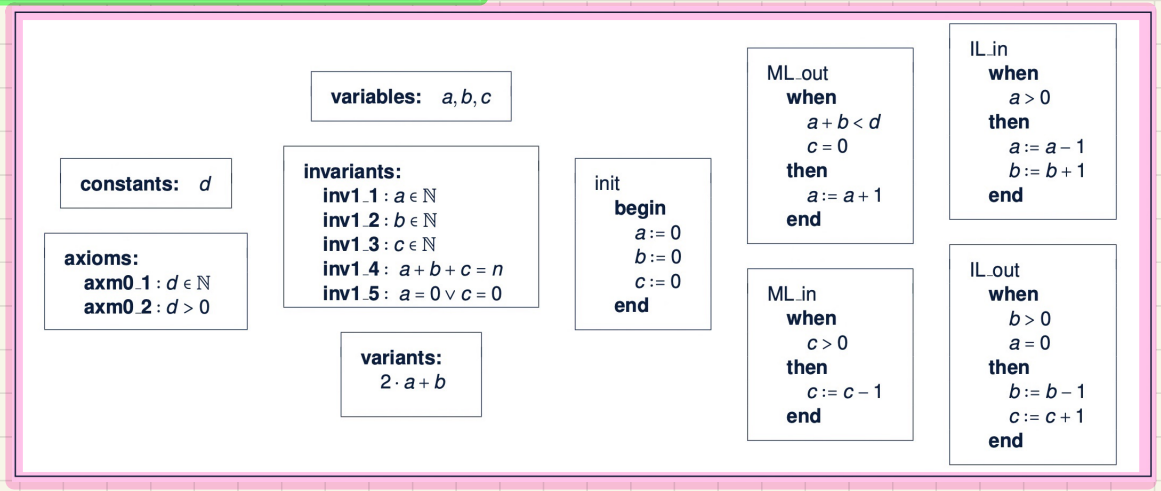
$$d > 0$$
$$b = 0 \vee b > 0$$
$$\vdash$$
$$b < d \wedge 0 = 0$$
$$\vee \quad b > 0 \wedge 0 = 0$$

Initial Model and 1st Refinement: Provably Correct



Abstract m0

Concrete m1



Correctness Criteria:

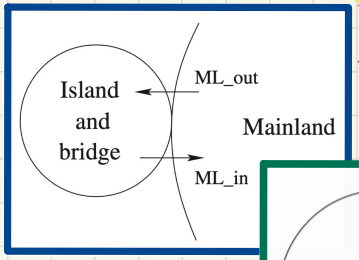
+ Guard Strengthening
+ Invariant Establishment
+ Invariant Preservation
+ Convergence
+ Relative Deadlock Freedom

Bridge Controller: Abstraction in the 2nd Refinement

ENV1	The system is equipped with two traffic lights with two colors: green and red.
ENV2	The traffic lights control the entrance to the bridge at both ends of it.
ENV3	Cars are not supposed to pass on a red traffic light, only on a green one.

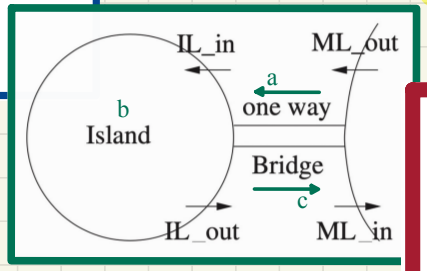
m0:

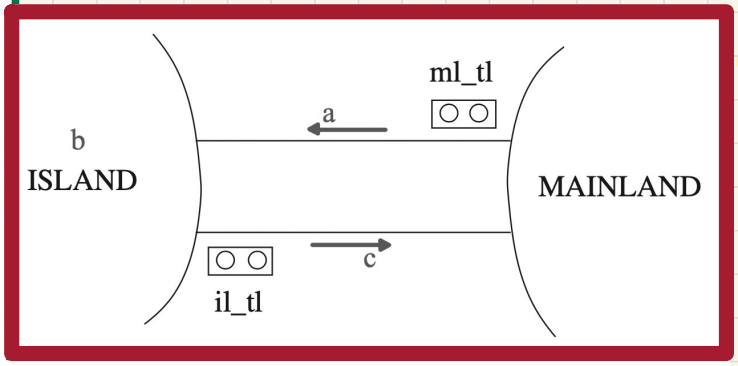
more abstract than m1



m1:

more concrete than m0, more abstract than m2





m2:

more concrete than m1

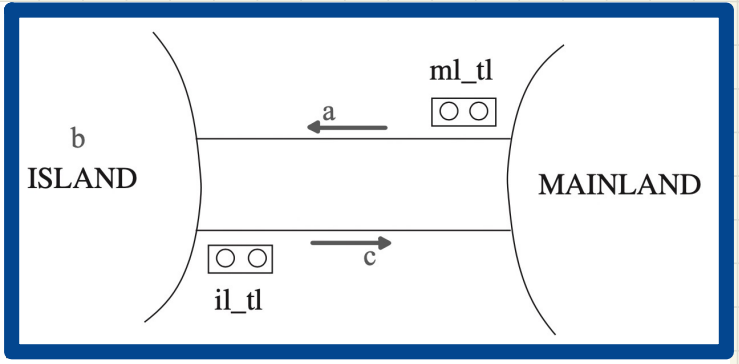
Bridge Controller: State Space of the 2nd Refinement

ENV1	The system is equipped with two traffic lights with two colors: green and red.
ENV2	The traffic lights control the entrance to the bridge at both ends of it.
ENV3	Cars are not supposed to pass on a red traffic light, only on a green one.

Dynamic Part of Model

variables:
a, *b*, *c*
ml_tl
il_tl

invariants:
inv2_1 : $ml\_tl \in COLOUR$
inv2_2 : $il\_tl \in COLOUR$
inv2_3 : ??
inv2_4 : ??



Static Part of Model

sets: *COLOR*

constants: *red*, *green*

axioms:
axm2_1 : $COLOR = \{green, red\}$
axm2_2 : $green \neq red$

Exercises

inv2_3: being allowed to exit ML means limited cars & no crash
inv2_4: being allowed to exit IL means some car in IL & no crash