Lecture 23 - Nov 27

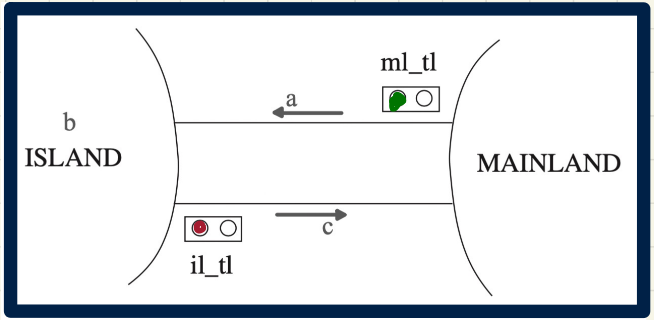
Bridge Controller

Adding Actions, Splitting Events
Preventing Livelock/Divergence
Proving Livelock/Divergence Freedom

Fixing m2: Adding Actions

Added inv2_5 : 1 * b
$ml\_tl = red \lor il\_tl = red$
new inv.

ML_out
ML_in
IL_out
IL_in
ML_tl_green
IL_tl_green.



ML_tl_green/inv2_5/INV

	axm0_1	$\{\ d \in \mathbb{N}$
	axm0_2	$\{\ d > 0$
	axm2_1	$\{\ COLOUR = \{green, red\}$
	axm2_2	$\{\ green \neq red$
m0	inv0_1	$\{\ n \in \mathbb{N}$
	inv0_2	$\{\ n \leq d$
	inv1_1	$\{\ a \in \mathbb{N}$
	inv1_2	$\{\ b \in \mathbb{N}$
m1	inv1_3	$\{\ c \in \mathbb{N}$
	inv1_4	$\{\ a + b + c = n$
	inv1_5	$\{\ a = 0 \lor c = 0$
	inv2_1	$\{\ ml\_tl \in COLOUR$
	inv2_2	$\{\ il\_tl \in COLOUR$
m2	inv2_3	$\{\ ml\_tl = green \Rightarrow a + b < d \land c = 0$
	inv2_4	$\{\ il\_tl = green \Rightarrow b > 0 \land a = 0$
	inv2_5	$\{\ ml\_tl = red \lor il\_tl = red$

ML_tl_green
when
$ml\_tl = red$
$a + b < d$
$c = 0$
then
$ml\_tl := green$
$il\_tl := red$
end

$ml\_tl' = g \land il\_tl' = r$

IL_tl_green
when
$il\_tl = red$
$b > 0$
$a = 0$
then
$il\_tl := green$
$ml\_tl := red$
end

Concrete grd. of ML_tl_gr.
$\left\{ \begin{array}{l} ml\_tl = red \\ a + b < d \\ c = 0 \end{array} \right.$

$\vdash$

$*$ $\boxed{green = red \lor red = red.}$

$\overset{green}{\cancel{ml\_tl'}} = red \lor \overset{red}{\cancel{il\_tl'}} = red$

Exercise: Specify IL_tl_green/inv2_5/INV

$inv2\_3: ml\_tl = g \Rightarrow a+b<d \wedge c=0$

$inv2\_4: il\_tl = g \Rightarrow b>0 \wedge a=0$

Discussed (Thursday)

$il\_tl = g \Rightarrow \boxed{a=0}$

ML_out / $\boxed{inv2\_4}$ / INV

IL_out / $\boxed{inv2\_3}$ / INV

$ml\_tl = g \Rightarrow \boxed{c=0}$

safety

To Discuss (Today)

$ml\_tl = g \Rightarrow \boxed{a+b<d}$

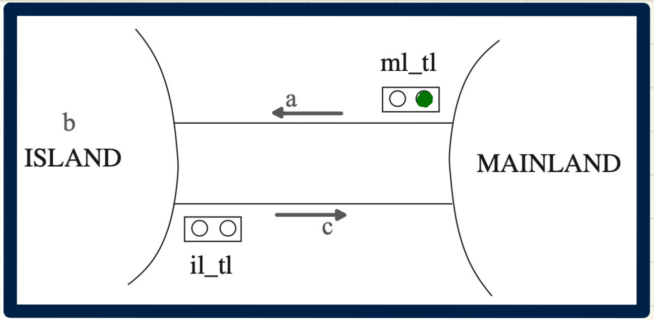
ML_out / $\boxed{inv2\_3}$ / INV

IL_out / $\boxed{inv2\_4}$ / INV

$il\_tl = g \Rightarrow \boxed{b>0}$

capacity

Invariant Preservation: ML_out/inv2_3/INV



variables:
a, b, c
ml_tl
il_tl

ML_out
when
$ml\_tl = green$
then
$\boxed{a := a + 1}$
end

$a' = a + 1$

IL_out
when
$il\_tl = green$ ✓
then
$\boxed{b := b - 1}$
$c := c + 1$
end

invariants:
inv2_1 : $ml\_tl \in COLOUR$
inv2_2 : $il\_tl \in COLOUR$
inv2_3 : $ml\_tl = green \Rightarrow a + b < d \land c = 0$
inv2_4 : $il\_tl = green \Rightarrow b > 0 \land a = 0$

ML_out/inv2_3/INV

axm0_1	$\{\ d \in \mathbb{N}$
axm0_2	$\{\ d > 0$
axm2_1	$\{\ COLOUR = \{green, red\}$
axm2_2	$\{\ green \neq red$
inv0_1	$\{\ n \in \mathbb{N}$
inv0_2	$\{\ n \leq d$
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	$\{\ a = 0 \lor c = 0$
inv2_1	$\{\ ml\_tl \in COLOUR$
inv2_2	$\{\ il\_tl \in COLOUR$
inv2_3	$\{\ ml\_tl = green \Rightarrow a + b < d \land c = 0$
inv2_4	$\{\ il\_tl = green \Rightarrow b > 0 \land a = 0$
inv2_5	$\{\ ml\_tl = red \lor il\_tl = red$
Concrete guards of *ML_out*	$\{\ ml\_tl = green$
	$\vdash$
Concrete invariant **inv2_3** with *ML_out*'s effect in the post-state	$\{\ ml\_tl = green \Rightarrow \boxed{(a + 1) + b < d} \land c = 0$

post-state of ML_out
$(a' = a + 1)$

$b' = b - 1$
$(b - 1) > 0$

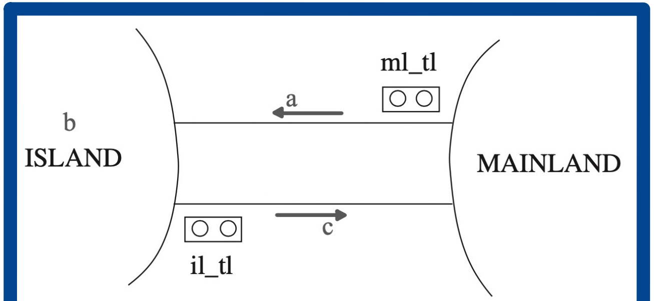
Exercise: Specify $\boxed{\text{IL\_out}}$/inv2_4/INV

Discharging POs of m2: Invariant Preservation

First Attempt

$d \in \mathbb{N}$
$d > 0$
$COLOUR = \{green, red\}$
$green \neq red$
$n \in \mathbb{N}$
$n \leq d$
$a \in \mathbb{N}$
$b \in \mathbb{N}$
$c \in \mathbb{N}$
$a + b + c = n$
$a = 0 \lor c = 0$
$ml\_tl \in COLOUR$
$il\_tl \in COLOUR$
$ml\_tl = green \Rightarrow a + b < d \land c = 0$
$il\_tl = green \Rightarrow b > 0 \land a = 0$
$ml\_tl = red \lor il\_tl = red$
$ml\_tl = green$
$\vdash$
$ml\_tl = green \Rightarrow (a + 1) + b < d \land c = 0$

ML_out/inv2_3/INV



$$\frac{H \vdash P \qquad H \vdash Q}{H \vdash P \land Q}\ \textbf{AND\_R}$$

$$\frac{H, P, Q \vdash R}{H, P \land Q \vdash R}\ \textbf{AND\_L}$$

$$\frac{H, P \vdash Q}{H \vdash P \Rightarrow Q}\ \textbf{IMP\_R}$$

Unprovable

$a + b < d$
$c = 0$
$ml\_tl = g.$
$\vdash$
$(a+1) + b < d$

MON

$ml\_tl = green \Rightarrow a + b < d \land c = 0$
$\vdash$
$ml\_tl = green \Rightarrow (a + 1) + b < d \land c = 0$

IMP_R

$ml\_tl = green \Rightarrow a + b < d \land c = 0$
$ml\_tl = green$
$\vdash$
$(a + 1) + b < d \land c = 0$

~~IMP_R~~ IMP_L.

$a + b < d \land c = 0$
$ml\_tl = green$
$\vdash$
$(a + 1) + b < d \land c = 0$

AND_L

$a + b < d$
$c = 0$
$ml\_tl = green$
$\vdash$
$(a + 1) + b < d \land c = 0$

AND_R

$a + b < d$
$c = 0$
$ml\_tl = green$
$\vdash$
$(a + 1) + b < d$

??

$a + b < d$
$c = 0$
$ml\_tl = green$
$\vdash$
$c = 0$

HYP

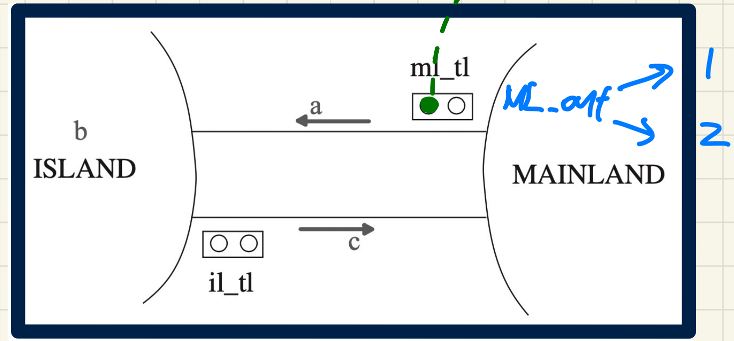
Understanding the Failed Proof on INV

variables:
a, b, c
ml_tl
il_tl

invariants:
inv2_1 : $ml\_tl \in COLOUR$
inv2_2 : $il\_tl \in COLOUR$
inv2_3 : $ml\_tl = green \Rightarrow a + b < d \wedge c = 0$
inv2_4 : $il\_tl = green \Rightarrow b > 0 \wedge a = 0$

ML_out
when
$\boxed{ml\_tl = green}$
then
$a := a + 1$
end

IL_out
when
$il\_tl = green$
then
$b := b - 1$
$c := c + 1$
end



Unprovable Sequent:

$$a + b < d$$
$$\wedge \quad c = 0$$
$$\wedge \quad ml\_tl = green$$
$$\vdash$$
$$(a + 1) + b < d$$

for $x+1 < y$, $\boxed{x < y}$ $\Rightarrow^{?}$ $x + 1 < y$ not true in general

e.g. $3 < 4$
$3 + 1 \cancel{<} 4$

x can't be equal to $\boxed{y-1}$

ML_out allowing one new car on to the bridge

$d = 3, b = 0, a = 0$	[$(a + 1) + b < d$ evaluates to ***true***]
$d = 3, b = 1, a = 0$	[$(a + 1) + b < d$ evaluates to ***true***]
$d = 3, b = 0, a = 1$	[$(a + 1) + b < d$ evaluates to ***true***]
$d = 3, b = 0, a = 2$	[$(a + 1) + b < d$ evaluates to ***false***]
$d = 3, b = 1, a = 1$	[$(a + 1) + b < d$ evaluates to ***false***]
$d = 3, b = 2, a = 0$	[$(a + 1) + b < d$ evaluates to ***false***]

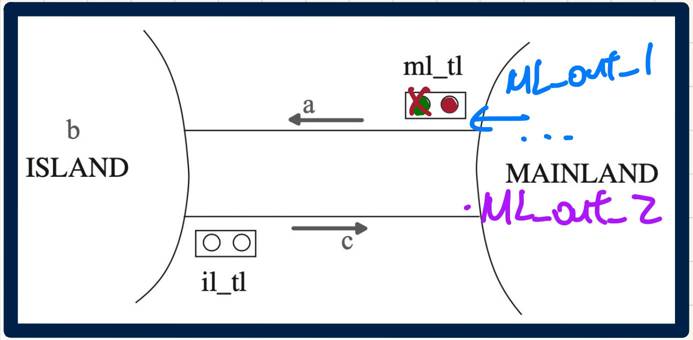
$(a+1)+b \neq d$
↳ no need to turn ml_tl to red

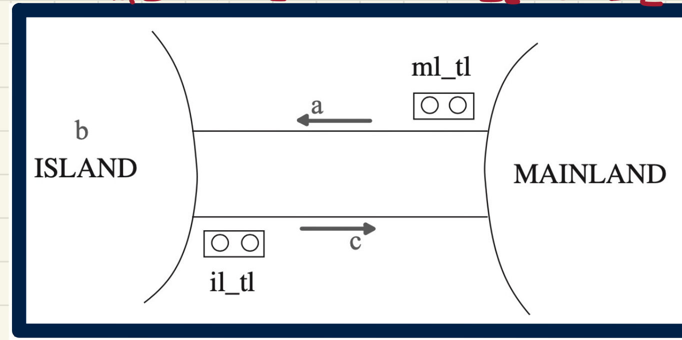
$(a+1)+b = d$ → need to turn ml_tl to red right away.

Fixing **m2**: Splitting **Events**

m1: ML_out → m2: ML_out_1, ML_out_2

IL_out → IL_out_1, IL_out_2





ML_out_1
when
$ml\_tl = green$
$a + b + 1 \neq d$
then
$a := a + 1$
end

ML_out_2
when
$ml\_tl = green$
$\boxed{a + b + 1 = d}$
then
$a := a + 1$
$\boxed{ml\_tl := red}$
end

disable ML_out_1

as soon as the capacity limit is reached, turn ml_tl to red

IL_out_1
when
$il\_tl = green$
$b \neq 1$
then
$b := b - 1$
$c := c + 1$
end

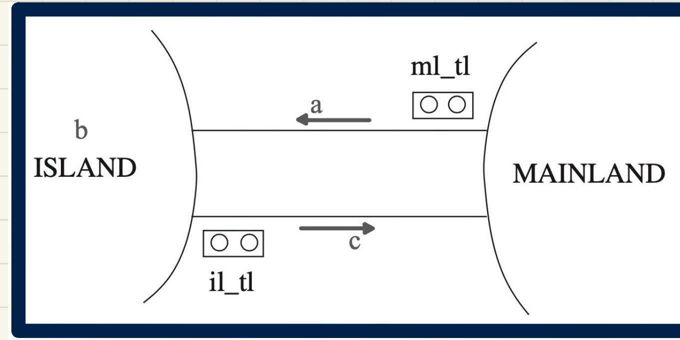
IL_out_2
when
$il\_tl = green$
$b = 1$
then
$b := b - 1$
$c := c + 1$
$il\_tl := red$
end

Current m2 May **Livelock**

infinite interleaving of new events

ML_tl_green
  when
    $ml\_tl = red$
    $\boxed{a + b < d \\ c = 0}$
  then
    $ml\_tl := green$
    $il\_tl := red$
  end

IL_tl_green
  when
    $il\_tl = red$
    $b > 0$
    $a = 0$
  then
    $il\_tl := green$
    $ml\_tl := red$
  end



The current m2 diverges ∵ there's one valid trace of infinite interleaving of new events

starting point of livelock

⟨ init , ML_tl_green , ML_out_1 , IL_in , IL_tl_green , ML_tl_green , IL_tl_green , . . . ⟩

init	ML_tl_green	ML_out_1	IL_in	IL_tl_green	ML_tl_green	IL_tl_green
$d = 2$	$d = 2$	$d = 2$	$d = 2$	$d = 2$	$d = 2$	$d = 2$
$a' = 0$	$a' = 0$	$a' = 1$	$a' = 0$	$a' = 0$	$a' = 0$	$a' = 0$
$b' = 0$	$b' = 0$	$b' = 0$	$b' = 1$	$b' = 1$	$b' = 1$	$b' = 1$
$c' = 0$	$c' = 0$	$c' = 0$	$c' = 0$	$c' = 0$	$c' = 0$	$c' = 0$
$ml\_tl = red$	$ml\_tl' = green$	$ml\_tl' = green$	$ml\_tl' = green$	$ml\_tl' = red$	$ml\_tl' = green$	$ml\_tl' = red$
$il\_tl = red$	$il\_tl' = red$	$il\_tl' = red$	$il\_tl' = red$	$il\_tl' = green$	$il\_tl' = red$	$il\_tl' = green$

Fixing m2: Regulating Traffic Light Changes

Divergence Trace: <init, ML_tl_green, ML_out_1, IL_in, IL_tl_green, ML_tl_green, IL_tl_green, ...>

```
ML_tl_green
  when
    ml_tl = red
    a + b < d
    c = 0
    il_pass = 1
  then
    ml_tl := green
    il_tl := red
    ml_pass := 0
  end
```

since ml_tl turned green, no car has passed

```
ML_out_1
  when
    ml_tl = green
    a + b + 1 ≠ d
  then
    a := a + 1
    ml_pass := 1
  end
```

```
IL_out_1
  when
    il_tl = green
    b ≠ 1
  then
    b := b − 1
    c := c + 1
    il_pass := 1
  end
```

disable

```
IL_tl_green
  when
    il_tl = red
    b > 0
    a = 0
    ml_pass = 1
  then
    il_tl := green
    ml_tl := red
    il_pass := 0
  end
```

```
ML_out_2
  when
    ml_tl = green
    a + b + 1 = d
  then
    a := a + 1
    ml_tl := red
    ml_pass := 1
  end
```

```
IL_out_2
  when
    il_tl = green
    b = 1
  then
    b := b − 1
    c := c + 1
    il_tl := red
    il_pass := 1
  end
```

since ml_tl turned green, ≥1 cars passed.

disabled IL_tl_green

both new events enabled.

d = 2	ml_pass	il_pass
< init,	1	1
ML_tl_green,	0	✓
ML_out_1,	✓	✓
ML_out_2,	✓	✓
IL_in,	✓	✓
IL_in,	✓	✓
IL_tl_green,	✓	0
IL_out_1,	✓	✓
IL_out_2,	✓	✓
ML_in,	✓	✓
ML_in	✓	✓
>		

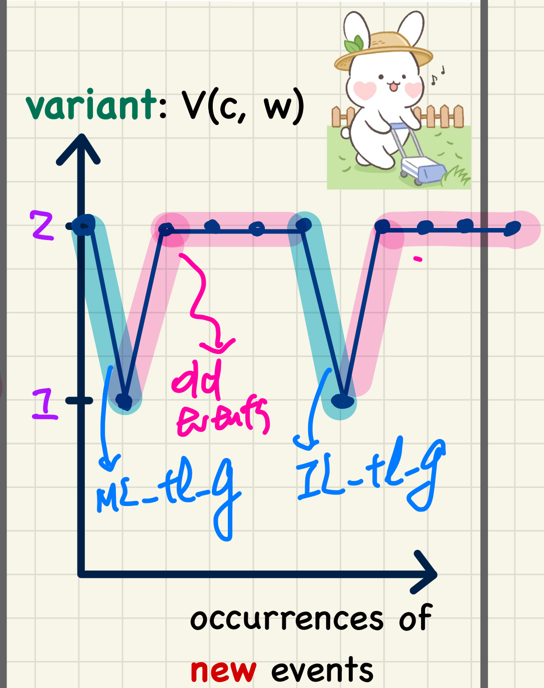
Fixing m2: Measuring Traffic Light Changes

ML_tl_green
when
ml_tl = red
a + b < d
c = 0
il_pass = 1
then
ml_tl := green
il_tl := red
ml_pass := 0
end

IL_tl_green
when
il_tl = red
b > 0
a = 0
ml_pass = 1
then
il_tl := green
ml_tl := red
il_pass := 0
end

d = 2	ml_pass	il_pass	
< init,	1	1	2
ML_tl_green,	0	1	1
ML_out_1,	1	1	2
ML_out_2,	1	1	2
IL_in,	1	1	2
IL_in,	1	1	2
IL_tl_green,	1	0	1
IL_out_1,	1	1	2
IL_out_2,	1	1	2
ML_in,	1	1	2
ML_in	1	1	2
>			

variants: *ml_pass + il_pass*



PO of Convergence/Non-Divergence/Livelock Freedom

A New Event Occurrence Decreases Variant

$$\frac{\begin{array}{l} A(c) \\ I(c,v) \\ J(c,v,w) \\ H(c,w) \\ \vdash \\ \boxed{V(c, F(c,w))} < \boxed{V(c,w)} \end{array}}{}\quad \text{VAR}$$

✓ post-state value of var.

pre-state value of var.

Variants: $\boxed{ml\_pass + il\_pass}$

ML_tl_green/VAR

ML_tl_green
when
- $ml\_tl = red$
- $a + b < d$
- $c = 0$
- $il\_pass = 1$

then
- $ml\_tl := green$
- $il\_tl := red$
- $ml\_pass := 0$

end

$ml\_pass' = 0$

$il\_pass' = il\_pass$

$d \in \mathbb{N}$	$d > 0$	
$COLOUR = \{green, red\}$	$green \neq red$	
$n \in \mathbb{N}$	$n \leq d$	
$a \in \mathbb{N}$	$b \in \mathbb{N}$	$c \in \mathbb{N}$
$a + b + c = n$	$a = 0 \lor c = 0$	
$ml\_tl \in COLOUR$	$il\_tl \in COLOUR$	
$ml\_tl = green \Rightarrow a + b < d \land c = 0$	$il\_tl = green \Rightarrow b > 0 \land a = 0$	
$ml\_tl = red \lor il\_tl = red$		
$ml\_pass \in \{0,1\}$	$il\_pass \in \{0,1\}$	
$ml\_tl = red \Rightarrow ml\_pass = 1$	$il\_tl = red \Rightarrow il\_pass = 1$	
$ml\_tl = red$	$a + b < d$	$c = 0$
$il\_pass = 1$		
$\vdash$		
* $\boxed{0 + il\_pass < ml\_pass + il\_pass}$		

$$* \ \overset{0}{\cancel{ml\_pass'}} + \overset{il\_pass}{\cancel{il\_pass'}} < ml\_pass + il\_pass$$

PO of Relative Deadlock Freedom

axm0_1	$d \in \mathbb{N}$
axm0_2	$d > 0$
axm2_1	$COLOUR = \{green, red\}$
axm2_2	$green \neq red$
inv0_1	$n \in \mathbb{N}$
inv0_2	$n \leq d$
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	$a = 0 \lor c = 0$
inv2_1	$ml\_tl \in COLOUR$
inv2_2	$il\_tl \in COLOUR$
inv2_3	$ml\_tl = green \Rightarrow a + b < d \land c = 0$
inv2_4	$il\_tl = green \Rightarrow b > 0 \land a = 0$
inv2_5	$ml\_tl = red \lor il\_tl = red$
inv2_6	$ml\_pass \in \{0, 1\}$
inv2_7	$il\_pass \in \{0, 1\}$
inv2_8	$ml\_tl = red \Rightarrow ml\_pass = 1$
inv2_9	$il\_tl = red \Rightarrow il\_pass = 1$

Disjunction of ***abstract*** guards

	$a + b < d \land c = 0$	**guards of** *ML_out* **in** m_1
$\lor$	$c > 0$	**guards of** *ML_in* **in** m_1
$\lor$	$a > 0$	**guards of** *IL_in* **in** m_1
$\lor$	$b > 0 \land a = 0$	**guards of** *IL_out* **in** m_1

$\vdash$

Disjunction of ***concrete*** guards

	$ml\_tl = red \land a + b < d \land c = 0 \land il\_pass = 1$	**guards of** *ML_tl_green* **in** m_2
$\lor$	$il\_tl = red \land b > 0 \land a = 0 \land ml\_pass = 1$	**guards of** *IL_tl_green* **in** m_2
$\lor$	$ml\_tl = green \land a + b + 1 \neq d$	**guards of** *ML_out_1* **in** m_2
$\lor$	$ml\_tl = green \land a + b + 1 = d$	**guards of** *ML_out_2* **in** m_2
$\lor$	$il\_tl = green \land b \neq 1$	**guards of** *IL_out_1* **in** m_2
$\lor$	$il\_tl = green \land b = 1$	**guards of** *IL_out_2* **in** m_2
$\lor$	$a > 0$	**guards of** *ML_in* **in** m_2
$\lor$	$c > 0$	**guards of** *IL_in* **in** m_2

Abstract m1

variables: a, b, c

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

Concrete m2

ML_tl_green
when
$ml\_tl = red$
$a + b < d$
$c = 0$
$il\_pass = 1$
then
$ml\_tl := green$
$il\_tl := red$
$ml\_pass := 0$
end

IL_tl_green
when
$il\_tl = red$
$b > 0$
$a = 0$
$ml\_pass = 1$
then
$il\_tl := green$
$ml\_tl := red$
$il\_pass := 0$
end

ML_out_1
when
$ml\_tl = green$
$a + b + 1 \neq d$
then
$a := a + 1$
$ml\_pass := 1$
end

IL_out_1
when
$il\_tl = green$
$b \neq 1$
then
$b := b - 1$
$c := c + 1$
$il\_pass := 1$
end

ML_out_2
when
$ml\_tl = green$
$a + b + 1 = d$
then
$a := a + 1$
$ml\_tl := red$
$ml\_pass := 1$
end

IL_out_2
when
$il\_tl = green$
$b = 1$
then
$b := b - 1$
$c := c + 1$
$il\_tl := red$
$il\_pass := 1$
end

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

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

Discharging POs of m2: Relative Deadlock Freedom

$$
\begin{array}{l}
d \in \mathbb{N} \\
d > 0 \\
COLOUR = \{green, red\} \\
green \neq red \\
n \in \mathbb{N} \\
n \leq d \\
a \in \mathbb{N} \\
b \in \mathbb{N} \\
c \in \mathbb{N} \\
a + b + c = n \\
a = 0 \lor c = 0 \\
ml\_tl \in COLOUR \\
il\_tl \in COLOUR \\
ml\_tl = green \Rightarrow a + b < d \land c = 0 \\
il\_tl = green \Rightarrow b > 0 \land a = 0 \\
ml\_tl = red \lor il\_tl = red \\
ml\_pass \in \{0, 1\} \\
il\_pass \in \{0, 1\} \\
ml\_tl = red \Rightarrow ml\_pass = 1 \\
il\_tl = red \Rightarrow il\_pass = 1 \\
\quad\;\; a + b < d \land c = 0 \\
\lor \;\; c > 0 \\
\lor \;\; a > 0 \\
\lor \;\; b > 0 \land a = 0 \\
\vdash \\
\quad\;\; ml\_tl = red \land a + b < d \land c = 0 \land il\_pass = 1 \\
\lor \;\; il\_tl = red \land b > 0 \land a = 0 \land ml\_pass = 1 \\
\lor \;\; ml\_tl = green \\
\lor \;\; il\_tl = green \\
\lor \;\; a > 0 \\
\lor \;\; c > 0
\end{array}
$$

⋮

IS#1

$$
\begin{array}{l}
d \in \mathbb{N} \\
d > 0 \\
b \in \mathbb{N} \\
ml\_tl = red \\
il\_tl = red \\
ml\_tl = red \Rightarrow ml\_pass = 1 \\
il\_tl = red \Rightarrow il\_pass = 1 \\
\vdash \\
\quad\;\; b < d \land ml\_pass = 1 \land il\_pass = 1 \\
\lor \;\; b > 0 \land ml\_pass = 1 \land il\_pass = 1
\end{array}
$$

...

IS#2

$$
\begin{array}{l}
d \in \mathbb{N} \\
d > 0 \\
b \in \mathbb{N} \\
ml\_tl = red \\
il\_tl = red \\
ml\_pass = 1 \\
il\_pass = 1 \\
\vdash \\
\quad\;\; b < d \land ml\_pass = 1 \land il\_pass = 1 \\
\lor \;\; b > 0 \land ml\_pass = 1 \land il\_pass = 1
\end{array}
$$

...

IS#3

$$
\begin{array}{l}
d > 0 \\
b \in \mathbb{N} \\
\vdash \\
b < d \lor b > 0
\end{array}
\quad \textbf{ARI} \quad
\begin{array}{l}
d > 0 \\
b > 0 \lor b = 0 \\
\vdash \\
b < d \lor b > 0
\end{array}
\quad \textbf{OR\_L}
\left\{
\begin{array}{l}
\begin{array}{l}
d > 0 \\
b > 0 \\
\vdash \\
b < d \lor b > 0
\end{array}
\quad \textbf{OR\_R2} \quad
\begin{array}{l}
d > 0 \\
b > 0 \\
\vdash \\
b > 0
\end{array}
\quad \textbf{HYP} \\[2em]
\begin{array}{l}
d > 0 \\
b = 0 \\
\vdash \\
b < d \lor b > 0
\end{array}
\quad \textbf{EQ\_LR, MON} \quad
\begin{array}{l}
d > 0 \\
\\
\vdash \\
0 < d \lor 0 > 0
\end{array}
\quad \textbf{OR\_R1} \quad
\begin{array}{l}
d > 0 \\
\vdash \\
0 < d
\end{array}
\quad \textbf{HYP}
\end{array}
\right.
$$

1st Refinement and 2nd Refinement: Provably Correct

Abstract m1

variables: a, b, c

constants: d

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

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** : $a = 0 \lor c = 0$

variants: $2 \cdot a + b$

init
begin
$a := 0$
$b := 0$
$c := 0$
end

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

Correctness Criteria:
- + Guard Strengthening
- + Invariant Establishment
- + Invariant Preservation
- + Convergence
- + Relative Deadlock Freedom

Concrete m2

variables:
a
b
c
ml_tl
il_tl
ml_pass
il_pass

constants: d

sets: $COLOR$

axioms:
- **axm0_1** : $d \in \mathbb{N}$
- **axm0_2** : $d > 0$
- **axm2_1** : $COLOR = \{green, red\}$
- **axm2_2** : $green \neq red$

invariants:
- **inv2_1** : $ml\_tl \in COLOUR$
- **inv2_2** : $il\_tl \in COLOUR$
- **inv2_3** : $ml\_tl = green \Rightarrow a + b < d \land c = 0$
- **inv2_4** : $il\_tl = green \Rightarrow b > 0 \land a = 0$
- **inv2_5** : $ml\_tl = red \lor il\_tl = red$
- **inv2_6** : $ml\_pass \in \{0, 1\}$
- **inv2_7** : $il\_pass \in \{0, 1\}$
- **inv2_8** : $ml\_tl = red \Rightarrow ml\_pass = 1$
- **inv2_9** : $il\_tl = red \Rightarrow il\_pass = 1$

variants: $ml\_pass + il\_pass$

ML_tl_green
when
$ml\_tl = red$
$a + b < d$
$c = 0$
$il\_pass = 1$
then
$ml\_tl := green$
$il\_tl := red$
$ml\_pass := 0$
end

IL_tl_green
when
$il\_tl = red$
$b > 0$
$a = 0$
$ml\_pass = 1$
then
$il\_tl := green$
$ml\_tl := red$
$il\_pass := 0$
end

ML_out_1
when
$ml\_tl = green$
$a + b + 1 \neq d$
then
$a := a + 1$
$ml\_pass := 1$
end

ML_out_2
when
$ml\_tl = green$
$a + b + 1 = d$
then
$a := a + 1$
$ml\_tl := red$
$ml\_pass := 1$
end

IL_out_1
when
$il\_tl = green$
$b \neq 1$
then
$b := b - 1$
$c := c + 1$
$il\_pass := 1$
end

IL_out_2
when
$il\_tl = green$
$b = 1$
then
$b := b - 1$
$c := c + 1$
$il\_tl := red$
$il\_pass := 1$
end

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

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