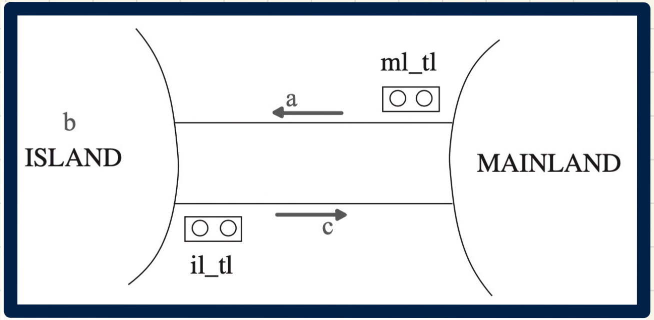
Lecture

Reactive System: Bridge Controller

2nd Refinement: Fixing the Model
Adding Actions

Fixing m2: Adding Actions



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

$ml\_tl' = g$
$il\_tl' = r \wedge a' = a \wedge b' = b \wedge c' = c$

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

ML_tl_green/inv2_5/INV

axm0_1	$d \in \mathbb{N}$
axm0_2	$d > 0$
axm2_1	$COLOUR = \{green, red\}$
axm2_2	$green \neq red$
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	$a = 0 \vee c = 0$
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	$il\_tl = green \Rightarrow b > 0 \wedge a = 0$
inv2_5	$ml\_tl = red \vee il\_tl = red$

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

$\vdash$

* $\boxed{green = red \vee red = red}$

* $ml\_tl' = red \vee il\_tl' = red$

Exercise: Proof

Exercise: Specify IL_tl_green/inv2_5/INV

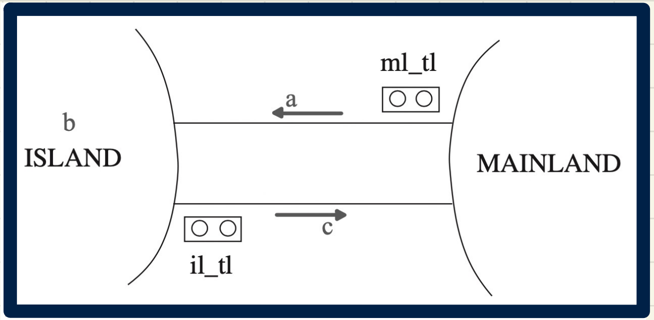
Lecture

Reactive System: Bridge Controller

2nd Refinement: Fixing the Model
Splitting Events

Invariant Preservation: ML_out/inv2_3/INV

ML_out/inv2_4 discussed earlier



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

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

variables:
a, b, c
ml_tl
il_tl

invariants:
inv2_1 : $ml\_tl \in COLOUR$
inv2_2 : $il\_tl \in COLOUR$
inv2_3 : $ml\_tl = green \Rightarrow a + b < d \land c = 0$
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	$ml\_tl = green \Rightarrow (a + 1) + b < d \land c = 0$

IL_out/inv2_3 discussed earlier

Exercise: Specify IL_out/inv2_4/INV

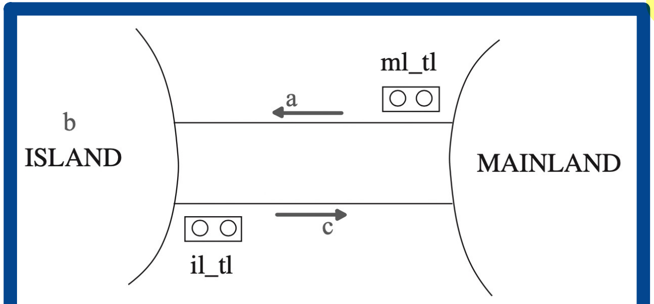
Discharging POs of m2: Invariant Preservation

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 → Exercise: IL_out/inv2_4/INV

expected to see: a similar unprovable sequent



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

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

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

MON

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

IMP_R

$ml\_tl = green \Rightarrow a + b < d \land c = 0,\; \boxed{ml\_tl = green} \;\vdash\; (a + 1) + b < d \land c = 0$

IMP_R

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

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**

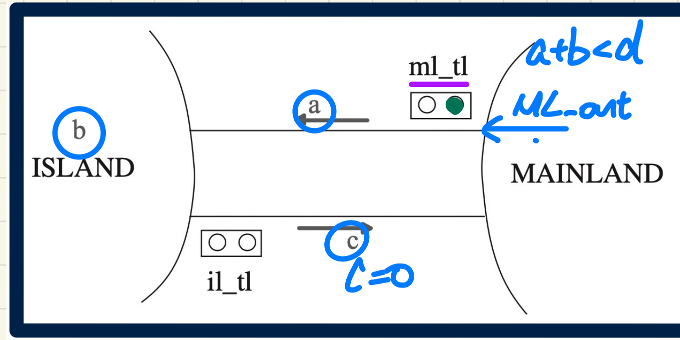
Understanding the Failed Proof on INV

variables:
a, b, c
ml_tl
il_tl

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

```
ML_out
  when
    ml_tl = green
  then
    a := a + 1
  end
```

```
IL_out
  when
    il_tl = green
  then
    b := b - 1
    c := c + 1
  end
```



$$x < y \Rightarrow x + 1 < y$$

e.g. $x = 3$
$y = 4$

Unprovable Sequent from ML_out/inv2_3/INV

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

another ML_out allowed

ML_out

inv2_3 is preserved

false $\Rightarrow$ _ $\checkmark$

$d = 3$,	$b = 0, a = 0$	$(a+1)+b \neq d$	[$(a + 1) + b < d$ 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***]
$d = 3$,	$b = 0, a = 2$	$(a+1)+b = d$	[$(a + 1) + b < d$ 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***]

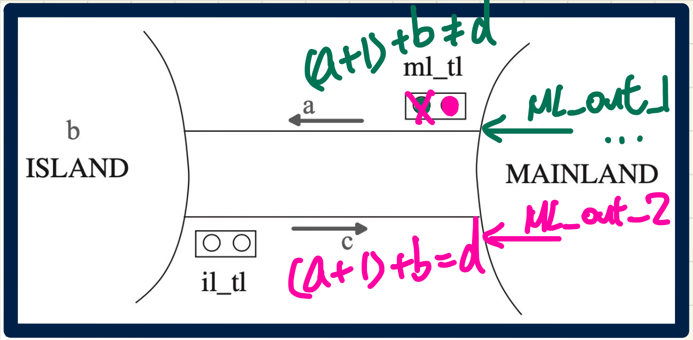
no more ML_out allowed $\Rightarrow$ $\boxed{ml\_tl := red}$

Fixing m2: Splitting Events

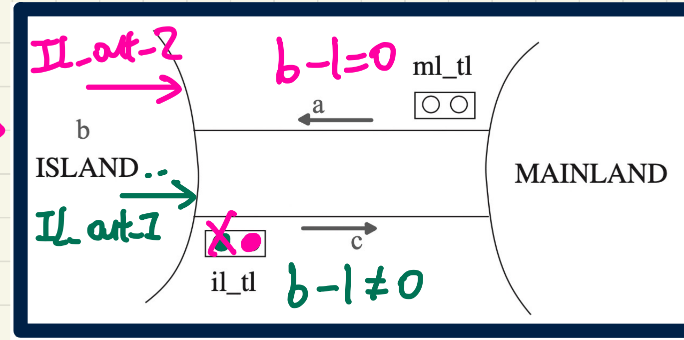
m1: ML_out IL_out

refines

m2: ML_out_1 ML_out_2 IL_out_1 IL_out_2

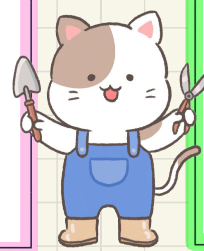


old, concrete events



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

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



IL_out_1
when
$il\_tl = green$
$\boxed{b \neq 1} \equiv b - 1 \neq 0$
then
$b := b - 1$
$c := c + 1$
end

IL_out_2
when
$il\_tl = green$
$b = 1 \equiv b - 1 = 0$
then
$b := b - 1$
$c := c + 1$
$il\_tl := red$
end

6 ↑ 8 : ML_out split
IL_out split

# of sequents for INV:
$8 \times 5 = 40$

Lecture

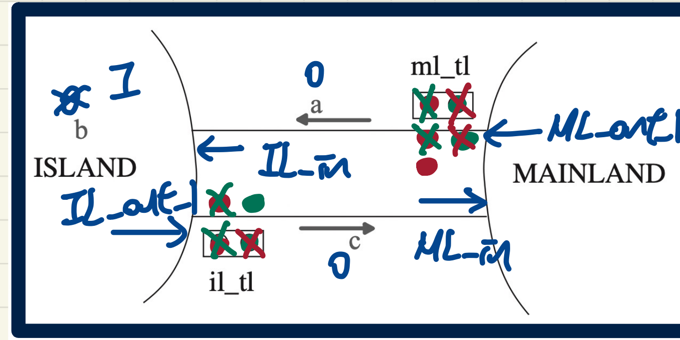
Reactive System: Bridge Controller

2nd Refinement: Livelock/Divergence

Current m2 May Livelock

ML_tl_green
when
✓ $ml\_tl = red$
✓ $a + b < d$
✓ $c = 0$
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



d=2

Expected trace: no divergence found this trace

$\langle$ init, ML_tl_green, ML_out_1, IL_in, IL_tl_green, IL_out_1, ML_in $\rangle$

a new event

old events

also a valid trace of m2, but leading to livelock

Is ML_tl_g. enabled?

Is IL_tl_g. enabled?

$\langle$ init, ML_tl_green, ML_out_1, IL_in, IL_tl_green, ML_tl_green, IL_tl_green, $\ldots$ $\rangle$

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

pattern of divergence

Fixing m2: Regulating Traffic Light Changes

To break the divergence pattern, after each new exit occurring, some old events occur.

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 exited ML.

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

since il_tl turned green, no car exited IL

disable

disable

enables

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

since ml_tl turned green, some car exited ML

enable

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

since il_tl turned green, some car exited IL

: ml_tl, il_tl both red

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

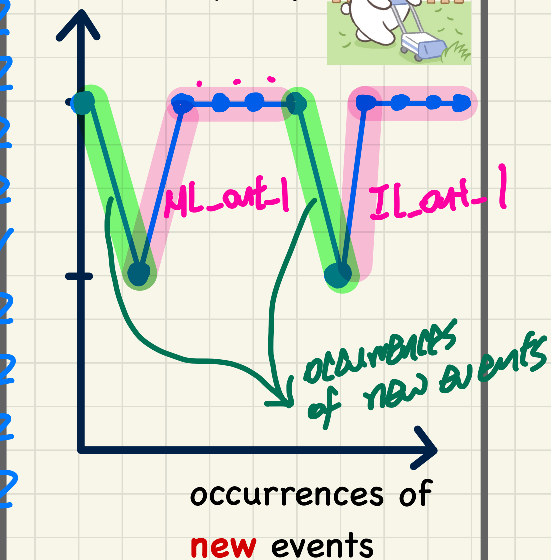
Fixing m2: Measuring Traffic Light Changes

```
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 dd	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 dd	2
ML_in,	1	1	2
ML_in	1	1	2
>			

variants : $ml\_pass + il\_pass$



PO of Convergence/Non-Divergence/Livelock Freedom

$* \ \cancel{ml\_pass'}^{\,0} + \cancel{il\_pass'}^{\,il\_pass}$

$< ml\_pass + il\_pass$

A New Event Occurrence Decreases Variant

$A(c)$

$I(c, v)$

$J(c, v, w)$

$H(c, w)$

$\vdash$

$\boxed{V(c, F(c, w))} < \boxed{V(c, w)}$

post-state evaluation

pre-state evaluation

VAR

applicable to new events

Variants: ml_pass + il_pass

ML_tl_green/VAR

$d \in \mathbb{N}$	$d > 0$	
$COLOUR = \{green, red\}$	$green \neq red$	
$n \in \mathbb{N}$	$n \leq d$] m0	
$a \in \mathbb{N}$	$b \in \mathbb{N}$	$c \in \mathbb{N}$] m1
$a + b + c = n$	$a = 0 \lor c = 0$	
$ml\_tl \in COLOUR$	$il\_tl \in COLOUR$	m2
$ml\_tl = green \Rightarrow a + b < d \land c = 0$	$il\_tl = green \Rightarrow b > 0 \land a = 0$	
$ml\_tl = red \lor il\_tl = red$		
$ml\_pass \in \{0, 1\}$	$il\_pass \in \{0, 1\}$	
$ml\_tl = red \Rightarrow ml\_pass = 1$	$il\_tl = red \Rightarrow il\_pass = 1$	
$ml\_tl = red$	$a + b < d$	$c = 0$]
$il\_pass = 1$		

$\vdash$

$* \ \boxed{0 + il\_pass < ml\_pass + il\_pass}$

Concrete guards of ML_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
```

BAP: $\underline{ml\_pass'} := 0$

$\cancel{il\_pass'} = il\_pass$

Lecture

Reactive System: Bridge Controller

2nd Refinement:
Relative Deadlock Freedom

PO of Relative Deadlock Freedom

$$
\begin{array}{ll}
\textbf{axm0\_1} & d \in \mathbb{N} \\
\textbf{axm0\_2} & d > 0 \\
\textbf{axm2\_1} & COLOUR = \{green, red\} \\
\textbf{axm2\_2} & green \neq red \\
\textbf{inv0\_1} & n \in \mathbb{N} \\
\textbf{inv0\_2} & n \leq d \\
\textbf{inv1\_1} & a \in \mathbb{N} \\
\textbf{inv1\_2} & b \in \mathbb{N} \\
\textbf{inv1\_3} & c \in \mathbb{N} \\
\textbf{inv1\_4} & a + b + c = n \\
\textbf{inv1\_5} & a = 0 \lor c = 0 \\
\textbf{inv2\_1} & ml\_tl \in COLOUR \\
\textbf{inv2\_2} & il\_tl \in COLOUR \\
\textbf{inv2\_3} & ml\_tl = green \Rightarrow a + b < d \land c = 0 \\
\textbf{inv2\_4} & il\_tl = green \Rightarrow b > 0 \land a = 0 \\
\textbf{inv2\_5} & ml\_tl = red \lor il\_tl = red \\
\textbf{inv2\_6} & ml\_pass \in \{0, 1\} \\
\textbf{inv2\_7} & il\_pass \in \{0, 1\} \\
\textbf{inv2\_8} & ml\_tl = red \Rightarrow ml\_pass = 1 \\
\textbf{inv2\_9} & il\_tl = red \Rightarrow il\_pass = 1
\end{array}
$$

Disjunction of *abstract* guards

$$
\begin{array}{rll}
 & a + b < d \land c = 0 & \textbf{guards of } ML\_out \textbf{ in } m_1 \\
\lor & c > 0 & \textbf{guards of } ML\_in \textbf{ in } m_1 \\
\lor & a > 0 & \textbf{guards of } IL\_in \textbf{ in } m_1 \\
\lor & b > 0 \land a = 0 & \textbf{guards of } IL\_out \textbf{ in } m_1
\end{array}
$$

$\vdash$

Disjunction of *concrete* guards

$$
\begin{array}{rll}
 & ml\_tl = red \land a + b < d \land c = 0 \land il\_pass = 1 & \textbf{guards of } ML\_tl\_green \textbf{ in } m_2 \\
\lor & il\_tl = red \land b > 0 \land a = 0 \land ml\_pass = 1 & \textbf{guards of } IL\_tl\_green \textbf{ in } m_2 \\
\lor & ml\_tl = green \land a + b + 1 \neq d & \textbf{guards of } ML\_out\_1 \textbf{ in } m_2 \\
\lor & ml\_tl = green \land a + b + 1 = d & \textbf{guards of } ML\_out\_2 \textbf{ in } m_2 \\
\lor & il\_tl = green \land b \neq 1 & \textbf{guards of } IL\_out\_1 \textbf{ in } m_2 \\
\lor & il\_tl = green \land b = 1 & \textbf{guards of } IL\_out\_2 \textbf{ in } m_2 \\
\lor & a > 0 & \textbf{guards of } ML\_in \textbf{ in } m_2 \\
\lor & c > 0 & \textbf{guards of } IL\_in \textbf{ in } m_2
\end{array}
$$

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

```
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
```

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 ≠ 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
```

```
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

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

Study

Ex. 1

$\vdots$

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

Ex. 2

$\cdots$

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

Ex3

$\cdots$

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

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

Superposition

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** : $il\_tl = red \Rightarrow il\_pass = 1$

divergence freedom

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