Lecture 2

Part M

Case Study on Reactive Systems - Bridge Controller 2nd Refinement: State and Events

Bridge Controller: Abstraction in the 2nd Refinement

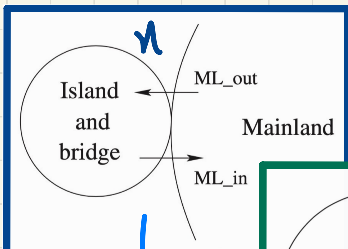
ENV1	The system is equipped with two traffic lights with two colors: green and red.
ENV2	The traffic lights control the entrance to the bridge at both ends of it.
ENV3	Cars are not supposed to pass on a red traffic light, only on a green one.

E-descriptions (environmental constraints)

important to assume, otherwise m2 would be much more complicated

m0:

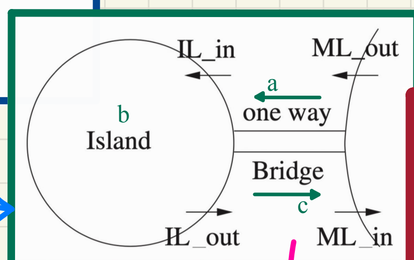
more abstract than m1



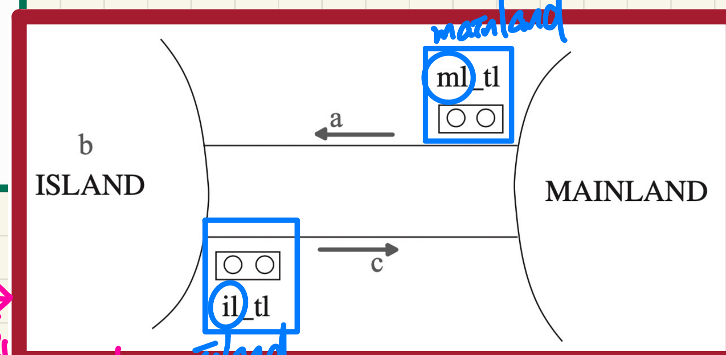
replaced n var. by a, b, c (bridge)

m1:

more concrete than m0, more abstract than m2



superposition
① inherits a, b, c from m1
② introduces ml_tl, il_tl



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.

* $il\_tl = green \Rightarrow b > 0 \land a = 0$

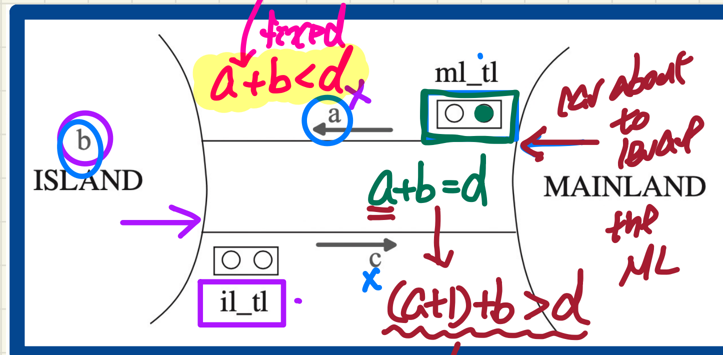
** $ml\_tl = green \Rightarrow a + b \leq d \land c = 0$

fixed: $a + b < d$

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 : ?? *



violation of capacity req.

Static Part of Model

sets: $COLOR$

constants: $red, green$

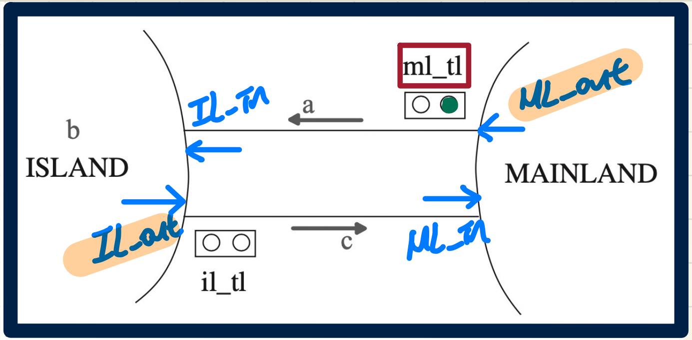
axioms:
axm2_1 : $COLOR = \{green, red\}$
axm2_2 : $green \neq red$

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

Bridge Controller: Guards of "old" Events 2nd Refinement



sets: $COLOR$

constants: $red, green$

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

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

from driver's perspective

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

ml_tl = green

abstract guards from m1 : $c=0 \land (a+b<d)$

IL_out: A car exits **island** (getting onto the **bridge**).

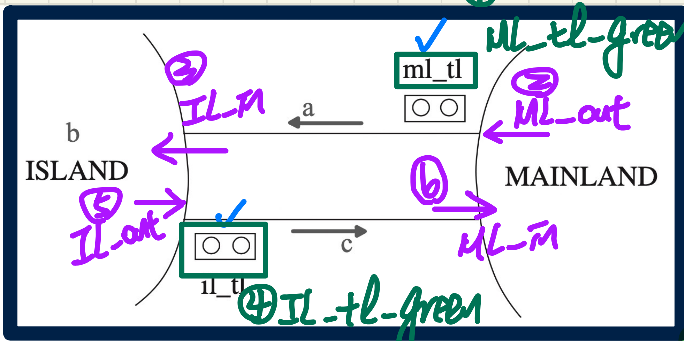
```
IL_out
  when
    ??
  then
    b := b − 1
    c := c + 1
  end
```

il_tl = green

abstract guards from m1: $a=0 \land b>0$

all these values should not be a driver's concern

Bridge Controller: Guards of "new" Events 2nd Refinement



⟨ init, ..., ML_tl_green, ML_out, ..., ... ⟩

sets: *COLOR*

constants: *red*, *green*

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

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 : $il\_tl = green \Rightarrow b > 0 \land a = 0$

turns ml_tl to green, before a car can exit the ML (ML_out)

turns IL_tl to green, before a car can exit the IL (IL_out)

ML_tl_green:

turn the traffic light **ml_tl** to green

ML_tl_green
when
??
then
ml_tl := *green*
end

ml_tl = red

$c = 0$
$a + b < d$

abstract guards of ML_out in m1

IL_tl_green:

turn the traffic light **il_tl** to green

IL_tl_green
when
??
then
il_tl := *green*
end

il_tl = red

$a = 0$
$b > 0$

abstract guards of IL_out in m1

Lecture 2

Part N

Case Study on Reactive Systems -
Bridge Controller
2nd Refinement: Invariant Preservation

PO/VC Rule of Invariant Preservation: Sequents

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
```

```
IL_out
  when
    b > 0
    a = 0
  then
    b := b − 1
    c := c + 1
  end
```

$$A(c)$$
$$I(c, v)$$
$$J(c, v, w)$$
$$H(c, w)$$
$$\vdash$$
$$J_i(c, E(c, v), F(c, w))$$

post-state version of inv.

Concrete m2

$* \ \underbrace{il\_tl'}_{il\_tl} = green \Rightarrow \underbrace{b'}_{b} > 0 \land \underbrace{a'}_{a+1} = 0$

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** : $\boxed{il\_tl = green \Rightarrow b > 0 \land a = 0}$

```
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
```

BAP: $a' = a + 1 \land b' = b \land c' = c \land ml\_tl' = ml\_tl \land il\_tl' = il\_tl$

ML_out/inv2_4/INV

$$\begin{array}{ll}
\textbf{axm0_1} & d \in \mathbb{N} \\
\textbf{axm0_2} & d > 0 \\
\textbf{axm2_1} & COLOUR = \{green, red\} \\
\textbf{axm2_2} & green \neq red \\
\textbf{inv0_1} & n \in \mathbb{N} \\
\textbf{inv0_2} & n \leq d \\
\textbf{inv1_1} & a \in \mathbb{N} \\
\textbf{inv1_2} & b \in \mathbb{N} \\
\textbf{inv1_3} & c \in \mathbb{N} \\
\textbf{inv1_4} & a + b + c = n \\
\textbf{inv1_5} & a = 0 \lor c = 0 \\
\textbf{inv2_1} & ml_tl \in COLOUR \\
\textbf{inv2_2} & il_tl \in COLOUR \\
\textbf{inv2_3} & ml_tl = green \Rightarrow a + b < d \land c = 0 \\
\textbf{inv2_4} & il_tl = green \Rightarrow b > 0 \land a = 0 \\
\textit{Concrete} \text{ guards of } \textit{ML_out} & ml_tl = green \\
 & \vdash \\
\textit{Concrete} \text{ invariant } \textbf{inv2_4} \text{ with } \textit{ML_out}\text{'s effect in the post-state} & il_tl = green \Rightarrow b > 0 \land (a + 1) = 0
\end{array}$$

abs. inv.

con. inv.

con. guard of ML_out

Exercise: Specify IL_out/inv2_3/INV

Example Inference Rules

$$\frac{H, P, Q \vdash R}{H, P, \boxed{P \Rightarrow Q} \vdash R} \quad \textbf{IMP\_L}$$

implicative hypothesis

Modus ponens

$$(p \Rightarrow q) \wedge p \equiv q$$

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

$\wedge$

implicative goal

Shunting

$$p \wedge q \Rightarrow r \equiv p \Rightarrow (q \Rightarrow r)$$

$$\frac{H, \neg Q \vdash P}{H, \neg P \vdash Q} \quad \textbf{NOT\_L}$$

$\neg P \Rightarrow Q$

$\equiv \neg Q \Rightarrow P$

Contrapositive:

$$p \Rightarrow q \equiv \neg q \Rightarrow \neg p$$

Discharging POs of m2: Invariant Preservation

First Attempt

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

ML_out/inv2_4/INV

Outstanding Sequent

$$
\begin{array}{l}
green \neq red \\
ml\_tl = green \\
il\_tl = green \\
\vdash \\
1 = 0
\end{array}
$$

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

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

MON

$$
\begin{array}{l}
green \neq red \\
il\_tl = green \Rightarrow b > 0 \land a = 0 \\
ml\_tl = green \\
\vdash \\
\boxed{il\_tl = green} \Rightarrow \boxed{b > 0 \land (a + 1) = 0}
\end{array}
\ \textbf{IMP\_R}\
\begin{array}{l}
green \neq red \\
\boxed{il\_tl = green} \Rightarrow b > 0 \land a = 0 \\
ml\_tl = green \\
\boxed{il\_tl = green} \\
\vdash \\
\boxed{b > 0 \land (a + 1) = 0}
\end{array}
\ \textbf{IMP\_L}\
\begin{array}{l}
green \neq red \\
b > 0 \land a = 0 \\
ml\_tl = green \\
il\_tl = green \\
\vdash \\
b > 0 \land (a + 1) = 0
\end{array}
\ \textbf{AND\_L}\
\begin{array}{l}
green \neq red \\
b > 0 \\
a = 0 \\
ml\_tl = green \\
il\_tl = green \\
\vdash \\
b > 0 \land (a + 1) = 0
\end{array}
\ \textbf{AND\_R}
$$

$$
\begin{array}{l}
green \neq red \\
b > 0 \\
a = 0 \\
ml\_tl = green \\
il\_tl = green \\
\vdash \\
b > 0
\end{array}
\ \textbf{HYP}
$$

$$
\begin{array}{l}
green \neq red \\
b > 0 \\
a = 0 \\
ml\_tl = green \\
il\_tl = green \\
\vdash \\
(a + 1) = 0
\end{array}
\ \textbf{EQ\_LR, MON}\
\begin{array}{l}
green \neq red \\
ml\_tl = green \\
il\_tl = green \\
\vdash \\
(0 + 1) = 0
\end{array}
\ \textbf{ARI}\
\begin{array}{l}
green \neq red \\
ml\_tl = green \\
il\_tl = green \\
\vdash \\
1 = 0
\end{array}
\ ??
$$

Discharging POs of m2: Invariant Preservation

First Attempt

IL_out/inv2_3/INV

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

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

$$\begin{array}{l}
d \in \mathbb{N} \\
d > 0 \\
COLOUR = \{green, red\} \\
green \neq red \\
n \in \mathbb{N} \\
n \leq d \\
a \in \mathbb{N} \\
b \in \mathbb{N} \\
c \in \mathbb{N} \\
a + b + c = n \\
a = 0 \lor c = 0 \\
ml_tl \in COLOUR \\
il_tl \in COLOUR \\
ml_tl = green \Rightarrow a + b < d \land c = 0 \\
il_tl = green \Rightarrow b > 0 \land a = 0 \\
il_tl = green \\
\vdash \\
ml_tl = green \Rightarrow a + (b-1) < d \land (c+1) = 0
\end{array}$$

MON

$$\begin{array}{l}
green \neq red \\
ml_tl = green \Rightarrow a + b < d \land c = 0 \\
il_tl = green \\
\vdash \\
ml_tl = green \Rightarrow a + (b-1) < d \land (c+1) = 0
\end{array}$$

IMP_R

$$\begin{array}{l}
green \neq red \\
ml_tl = green \Rightarrow a + b < d \land c = 0 \\
il_tl = green \\
ml_tl = green \\
\vdash \\
a + (b-1) < d \land (c+1) = 0
\end{array}$$

IMP_L

$$\begin{array}{l}
green \neq red \\
a + b < d \land c = 0 \\
il_tl = green \\
ml_tl = green \\
\vdash \\
a + (b-1) < d \land (c+1) = 0
\end{array}$$

AND_L

$$\begin{array}{l}
green \neq red \\
a + b < d \\
c = 0 \\
il_tl = green \\
ml_tl = green \\
\vdash \\
a + (b-1) < d \land (c+1) = 0
\end{array}$$

AND_R

$$\begin{array}{l}
green \neq red \\
a + b < d \\
c = 0 \\
il_tl = green \\
ml_tl = green \\
\vdash \\
a + (b-1) < d
\end{array}$$

MON

$$\begin{array}{l}
a + b < d \\
\vdash \\
a + (b-1) < d
\end{array}$$

ARI

$$\begin{array}{l}
green \neq red \\
a + b < d \\
c = 0 \\
il_tl = green \\
ml_tl = green \\
\vdash \\
(c+1) = 0
\end{array}$$

EQ_LR, MON

$$\begin{array}{l}
green \neq red \\
il_tl = green \\
ml_tl = green \\
\vdash \\
(0 + 1) = 0
\end{array}$$

ARI

$$\begin{array}{l}
green \neq red \\
il_tl = green \\
ml_tl = green \\
\vdash \\
1 = 0
\end{array}$$

??

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 : $ml\_tl = green \Rightarrow a + b < d \land c = 0$
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

ML_out/inv2_4/INV

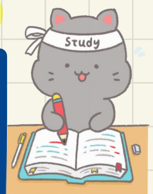
$d \in \mathbb{N}$
$d > 0$
$COLOUR = \{green, red\}$
$green \neq red$
$n \in \mathbb{N}$
$n \leq d$
$a \in \mathbb{N}$
$b \in \mathbb{N}$
$c \in \mathbb{N}$
$a + b + c = n$
$a = 0 \lor c = 0$
$ml\_tl \in COLOUR$
$il\_tl \in COLOUR$
$ml\_tl = green \Rightarrow a + b < d \land c = 0$
$il\_tl = green \Rightarrow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

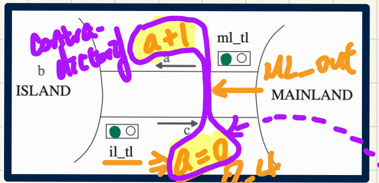
IL_out/inv2_3/INV

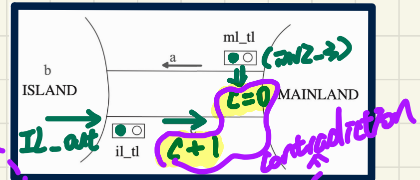
$d \in \mathbb{N}$
$d > 0$
$COLOUR = \{green, red\}$
$green \neq red$
$n \in \mathbb{N}$
$n \leq d$
$a \in \mathbb{N}$
$b \in \mathbb{N}$
$c \in \mathbb{N}$
$a + b + c = n$
$a = 0 \lor c = 0$
$ml\_tl \in COLOUR$
$il\_tl \in COLOUR$
$ml\_tl = green \Rightarrow a + b < d \land c = 0$
$il\_tl = green \Rightarrow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

Unprovable Sequent:

$$
\begin{array}{ll}
 & green \neq red \\
\land & il\_tl = green \\
\land & ml\_tl = green \\
\vdash & \\
 & 1 = 0
\end{array}
$$







init	ML_tl_green	ML_out	IL_in	IL_tl_green	IL_out	ML_out
$d = 2$	$d = 2$	$d = 2$	$d = 2$	$d = 2$	$d = 2$	$d = 2$
$a' = 0$	$a' = 0$	$\mathbf{a' = 1}$	$\mathbf{a' = 0}$	$a' = 0$	$a' = 0$	$\mathbf{a' = 1}$
$b' = 0$	$b' = 0$	$b' = 0$	$\mathbf{b' = 1}$	$b' = 1$	$\mathbf{b' = 0}$	$b' = 0$
$c' = 0$	$c' = 0$	$c' = 0$	$c' = 0$	$c' = 0$	$\mathbf{c' = 1}$	$c' = 1$
$ml\_tl' = red$	$\mathbf{ml\_tl' = green}$	$ml\_tl' = green$	$ml\_tl' = green$	$ml\_tl' = green$	$ml\_tl' = green$	$ml\_tl' = green$
$il\_tl' = red$	$il\_tl' = red$	$il\_tl' = red$	$il\_tl' = red$	$\mathbf{il\_tl' = green}$	$il\_tl' = green$	$il\_tl' = green$

Lecture 2

Part O

Case Study on Reactive Systems -
Bridge Controller
2nd Refinement: Fixing the Model
Adding an Invariant

Fixing m2: Adding an Invariant

REQ3	The bridge is one-way or the other, not both at the same time.

inv2_5 : $ml\_tl = red \lor il\_tl = red$

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

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

Concrete m2

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

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

ML_out/inv2_4/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_4** with *ML_out*'s effect in the post-state	$\{ il\_tl = green \Rightarrow b > 0 \land (a + 1) = 0$

Exercise: Specify IL_out/inv2_3/INV

Discharging POs of m2: Invariant Preservation

Second Attempt

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

MON

$green \neq red$
$il\_tl = green \Rightarrow b > 0 \land a = 0$
$ml\_tl = red \lor il\_tl = red$
$ml\_tl = green$
$\vdash$
$il\_tl = green \Rightarrow b > 0 \land (a + 1) = 0$

IMP_R

$green \neq red$
$il\_tl = green \Rightarrow b > 0 \land a = 0$
$ml\_tl = green$
$ml\_tl = red \lor il\_tl = red$
$il\_tl = green$
$\vdash$
$b > 0 \land (a + 1) = 0$

IMP_L

$green \neq red$
$b > 0 \land a = 0$
$ml\_tl = green$
$ml\_tl = red \lor il\_tl = red$
$il\_tl = green$
$\vdash$
$b > 0 \land (a + 1) = 0$

AND_L

$green \neq red$
$b > 0$
$a = 0$
$ml\_tl = green$
$ml\_tl = red \lor il\_tl = red$
$il\_tl = green$
$\vdash$
$b > 0 \land (a + 1) = 0$

AND_R

$green \neq red$
$b > 0$
$a = 0$
$ml\_tl = green$
$ml\_tl = red \lor il\_tl = red$
$il\_tl = green$
$\vdash$
$b > 0$

HYP

$green \neq red$
$b > 0$
$a = 0$
$ml\_tl = green$
$ml\_tl = red \lor il\_tl = red$
$il\_tl = green$
$\vdash$
$(a + 1) = 0$

EQ_LR, MON

$green \neq red$
$ml\_tl = green$
$ml\_tl = red \lor il\_tl = red$
$il\_tl = green$
$\vdash$
$(0 + 1) = 0$

ARI

$green \neq red$
$ml\_tl = green$
$ml\_tl = red \lor il\_tl = red$
$il\_tl = green$
$\vdash$
$1 = 0$

ML_out/inv2_4/INV

green ≠ red
ml_tl = green
ml_tl = red ∨ il_tl = red
il_tl = green
⊢
1 = 0

OR_L

green ≠ red
ml_tl = green
ml_tl = red
il_tl = green
⊢ 1 = 0

EQ_LR, MON

green ≠ red
green = red
il_tl = green
⊢ 1 = 0

NOT_L

green = red
il_tl = green
1 ≠ 0
⊢ green ≠ red

HYP

green ≠ red
ml_tl = green
il_tl = red
il_tl = green
⊢ 1 = 0

EQ_LR, MON

green ≠ red
ml_tl = green
red = green
⊢ 1 = 0

NOT_L

ml_tl = green
red = green
1 ≠ 0
⊢ green ≠ red

HYP

$$\frac{H, \neg Q \vdash P}{H, \neg P \vdash Q} \quad \textbf{NOT\_L}$$

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

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

Discharging POs of m2: Invariant Preservation

Second Attempt

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

IL_out/inv2_3/INV

MON

$green \neq red$
$ml\_tl = green \Rightarrow a + b < d \land c = 0$
$ml\_tl = red \lor il\_tl = red$
$il\_tl = green$
$\vdash$
$ml\_tl = green \Rightarrow a + (b - 1) < d \land (c + 1) = 0$

IMP_R

$green \neq red$
$il\_tl = green$
$ml\_tl = red \lor il\_tl = red$
$ml\_tl = green$
$\vdash$
$1 = 0$

Assignment

$green \neq red$
$ml\_tl = green \Rightarrow a + b < d \land c = 0$
$il\_tl = green$
$ml\_tl = red \lor il\_tl = red$
$ml\_tl = green$
$\vdash$
$a + (b - 1) < d \land (c + 1) = 0$

IMP_L

$green \neq red$
$a + b < d \land c = 0$
$il\_tl = green$
$ml\_tl = red \lor il\_tl = red$
$ml\_tl = green$
$\vdash$
$a + (b - 1) < d \land (c + 1) = 0$

AND_L

$green \neq red$
$a + b < d$
$c = 0$
$il\_tl = green$
$ml\_tl = red \lor il\_tl = red$
$ml\_tl = green$
$\vdash$
$a + (b - 1) < d \land (c + 1) = 0$

AND_R

$green \neq red$
$a + b < d$
$c = 0$
$il\_tl = green$
$ml\_tl = red \lor il\_tl = red$
$ml\_tl = green$
$\vdash$
$a + (b - 1) < d$

MON

$a + b < d$
$\vdash$
$a + (b - 1) < d$

ARI

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

EQ_LR, MON

$green \neq red$
$il\_tl = green$
$ml\_tl = red \lor il\_tl = red$
$ml\_tl = green$
$\vdash$
$(0 + 1) = 0$

ARI

$green \neq red$
$il\_tl = green$
$ml\_tl = red \lor il\_tl = red$
$ml\_tl = green$
$\vdash$
$1 = 0$

$$\frac{H, \neg Q \vdash P}{H, \neg P \vdash Q} \quad \textbf{NOT\_L}$$

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

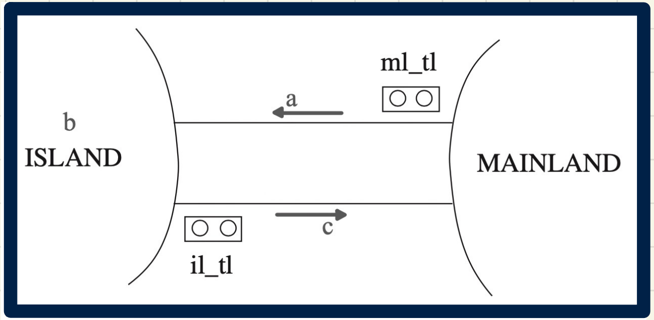
$$\frac{H, P \vdash R \qquad H, Q \vdash R}{H, P \lor Q \vdash R} \quad \textbf{OR\_L}$$

Lecture 2

Part P

Case Study on Reactive Systems - Bridge Controller
2nd Refinement: Fixing the Model
Adding Actions

Fixing m2: Adding Actions



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

$\vdash$

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

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

Exercise: Proof

Exercise: Specify IL_tl_green/inv2_5/INV

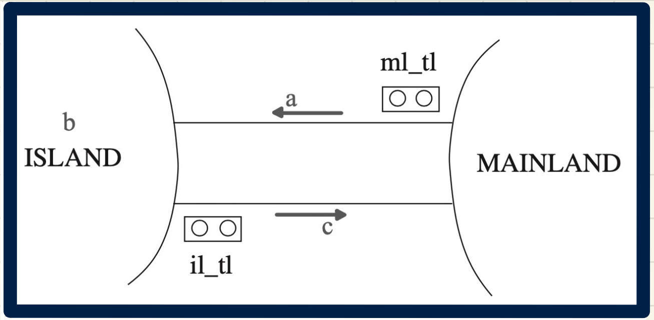
Lecture 2

Part Q

***Case Study on Reactive Systems -
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 : $ml\_tl = green \Rightarrow a + b < d \wedge c = 0$
inv2_4 : $il\_tl = green \Rightarrow b > 0 \wedge a = 0$

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	$a = 0 \vee c = 0$
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 of *ML_out*	$ml\_tl = green$
	$\vdash$
Concrete invariant **inv2_3** with *ML_out*'s effect in the post-state	$ml\_tl = green \Rightarrow (a + 1) + b < d \wedge c = 0$

IL_out/inv2_3 discussed earlier

Exercise: Specify IL_out/inv2_4/INV

Discharging POs of m2: Invariant Preservation

First Attempt

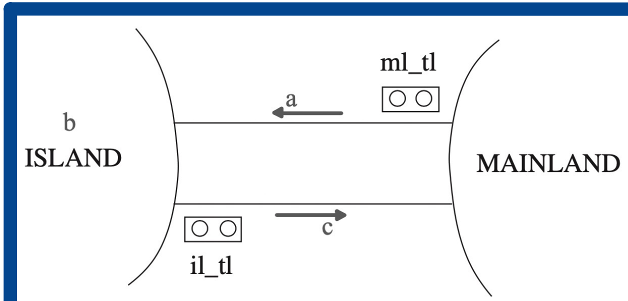
$d \in \mathbb{N}$
$d > 0$
$COLOUR = \{green, red\}$
$green \neq red$
$n \in \mathbb{N}$
$n \leq d$
$a \in \mathbb{N}$
$b \in \mathbb{N}$
$c \in \mathbb{N}$
$a + b + c = n$
$a = 0 \lor c = 0$
$ml\_tl \in COLOUR$
$il\_tl \in COLOUR$
$ml\_tl = green \Rightarrow a + b < d \land c = 0$
$il\_tl = green \Rightarrow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

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

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

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**

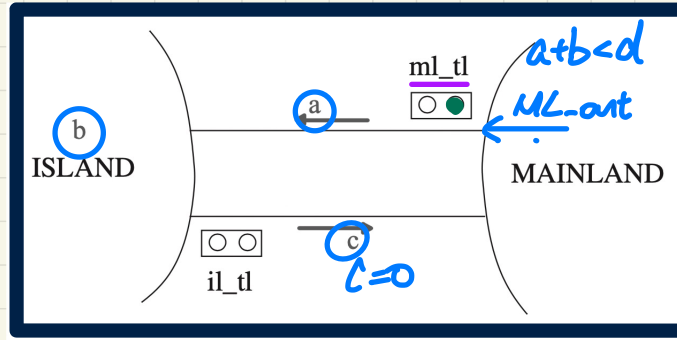
Understanding the Failed Proof on INV

variables:
a, b, c
ml_tl
il_tl

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

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



$$\boxed{\begin{array}{l} x < y \\ \Rightarrow x + 1 < y \end{array}}$$

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

Unprovable Sequent from ML_out/inv2_3/INV

$$\begin{array}{ll} & a + b < d \\ \wedge & c = 0 \\ \wedge ✓ & ml\_tl = green \\ \vdash & \\ & (a + 1) + b < d \end{array}$$

another ML_out allowed

ML_out

inv2_3 is preserved

∴ false ⇒ _ ✓

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

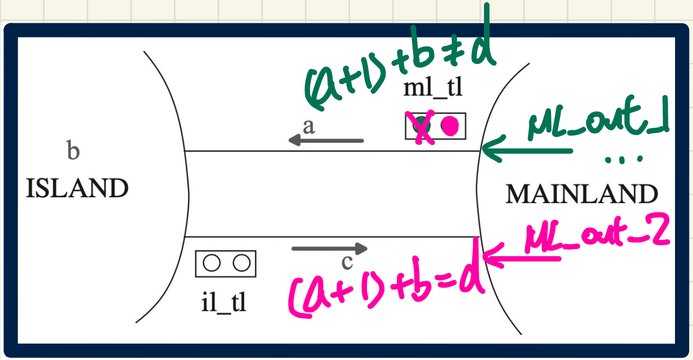
no more ML_out allowed ⇒ $\boxed{ml\_tl := red}$

Fixing m2: Splitting Events

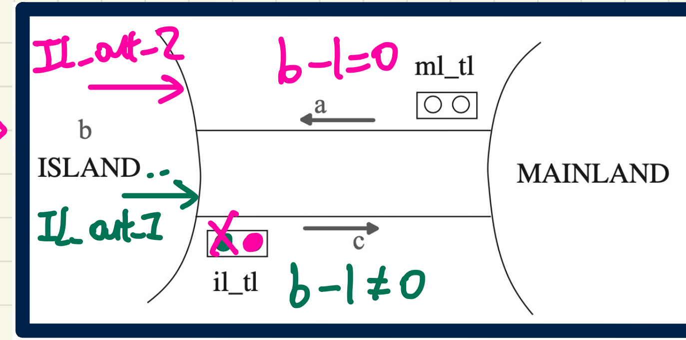
ml: ML_out IL_out

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:
$8 \times 5 = 40$