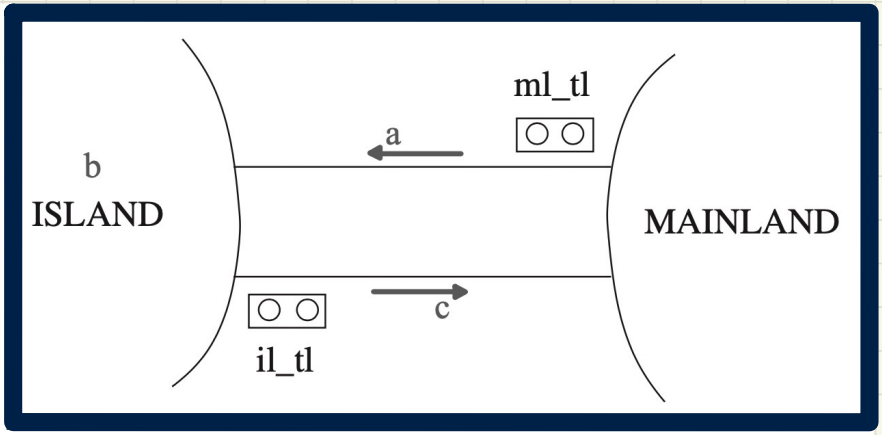
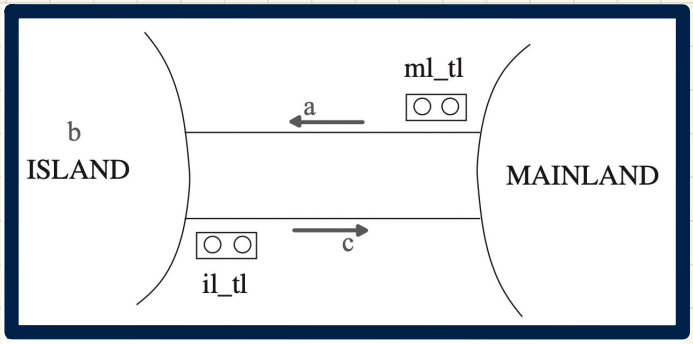
Bridge Controller: "Old" and "New" Events



Single Car Travel:

<init,
ml_tl_green, ML_out,
IL_in,
il_tl_green, IL_out, ML_in>

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 : $ml\_tl = green \Rightarrow a + b < d \wedge c = 0$
inv2_4 : $il\_tl = green \Rightarrow b > 0 \wedge a = 0$

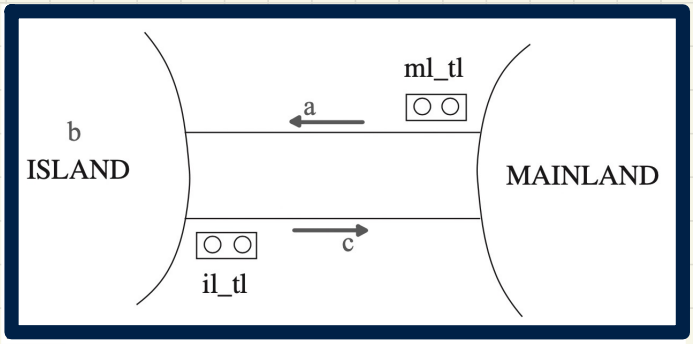
ML_out: A car exits **mainland** (getting onto the **bridge**).

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

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

IL_out
when
??
then
$b := b - 1$
$c := c + 1$
end

Bridge Controller: Guards of "new" 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 : $ml\_tl = green \Rightarrow a + b < d \wedge c = 0$
inv2_4 : $il\_tl = green \Rightarrow b > 0 \wedge a = 0$

ML_tl_green:

turn the traffic light ml_tl to green

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

IL_tl_green:

turn the traffic light il_tl to green

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

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

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** : $ml\_tl = green \Rightarrow a + b < d \wedge c = 0$
- **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

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

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	$a = 0 \vee c = 0$
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	$il\_tl = green \Rightarrow b > 0 \wedge a = 0$
Concrete guards of *ML_out*	$ml\_tl = green$
	$\vdash$
Concrete invariant **inv2_4** with *ML_out*'s effect in the post-state	$il\_tl = green \Rightarrow b > 0 \wedge (a + 1) = 0$

Exercise: Specify IL_out/inv2_3/INV

Example Inference Rules

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

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

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

Discharging POs of m2: Invariant Preservation

First Attempt

ML_out/inv2_4/INV

$$\frac{H \vdash P \qquad H \vdash Q}{H \vdash P \wedge Q}\ \text{AND\_R} \qquad \frac{H, P, Q \vdash R}{H, P \wedge Q \vdash R}\ \text{AND\_L}$$

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

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

MON

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

IMP_R

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

IMP_L

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

AND_L

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

AND_R

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

HYP

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

EQ_LR, MON

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

ARI

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

??

Discharging POs of m2: Invariant Preservation

First Attempt

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

IL_out/inv2_3/INV

$$\frac{H \vdash P \qquad H \vdash Q}{H \vdash P \wedge Q}\ \text{AND\_R} \qquad \frac{H, P, Q \vdash R}{H, P \wedge Q \vdash R}\ \text{AND\_L}$$

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

MON

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

IMP_R

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

IMP_L

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

AND_L

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

AND_R

- $green \neq red$, $a + b < d$, $c = 0$, $il\_tl = green$, $ml\_tl = green$, $\vdash$ $a + (b-1) < d$ — **MON** → $a + b < d \vdash a + (b-1) < d$ — **ARI**
- $green \neq red$, $a + b < d$, $c = 0$, $il\_tl = green$, $ml\_tl = green$, $\vdash$ $(c+1) = 0$ — **EQ_LR, MON** → $green \neq red$, $il\_tl = green$, $ml\_tl = green \vdash (0+1) = 0$ — **ARI** → $green \neq red$, $il\_tl = green$, $ml\_tl = green \vdash 1 = 0$??

Understanding the Failed Proof on INV

Fixed

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

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

Unprovable Sequent:

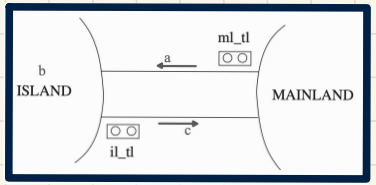
$$\begin{array}{ll} & green \neq red \\ \wedge & il\_tl = green \\ \wedge & ml\_tl = green \\ \vdash & \\ & 1 = 0 \end{array}$$

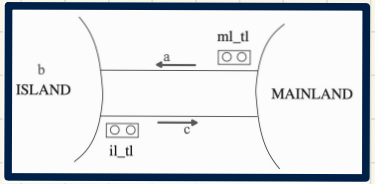
IL_out/inv2_3/INV

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

ML_out/inv2_4/INV

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





⟨ *init*	, *ML_tl_green*	, *ML_out*	, *IL_in*	, *IL_tl_green*	, *IL_out*	, *ML_out* ⟩
$d = 2$ $a' = 0$ $b' = 0$ $c' = 0$ $ml\_tl' = red$ $il\_tl' = red$	$d = 2$ $a' = 0$ $b' = 0$ $c' = 0$ **$ml\_tl' = green$** $il\_tl' = red$	$d = 2$ **$a' = 1$** $b' = 0$ $c' = 0$ $ml\_tl' = green$ $il\_tl' = red$	$d = 2$ **$a' = 0$** **$b' = 1$** $c' = 0$ $ml\_tl' = green$ $il\_tl' = red$	$d = 2$ $a' = 0$ $b' = 1$ $c' = 0$ $ml\_tl' = green$ **$il\_tl' = green$**	$d = 2$ $a' = 0$ **$b' = 0$** **$c' = 1$** $ml\_tl' = green$ $il\_tl' = green$	$d = 2$ **$a' = 1$** $b' = 0$ $c' = 1$ $ml\_tl' = green$ $il\_tl' = green$

Fixing m2: Adding an Invariant

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

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

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

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*	$ml\_tl = green$
⊢	
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

ML_out/inv2_4/INV

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

MON

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

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

IMP_R

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

IMP_L

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

AND_L

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

AND_R

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

HYP

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

EQ_LR, MON

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

ARI

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

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

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

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