

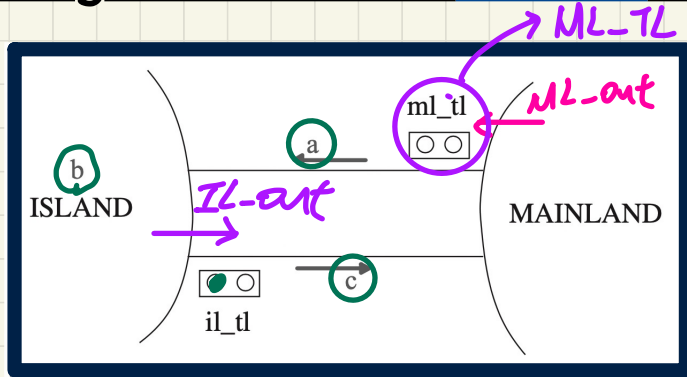
Lecture 20 - April 4

Reactive System: Bridge Controller

Announcements

- **ProgTest1**: Andy (eMail, Zoom); Jackie (Office Hour)
- **Lab4** released
- **ProgTest2**
- **Exam guide** to be released
- Final **makeup lecture** to be released

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



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

```

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

for driver to follow

abstract guard from ml:
 $C = 0 \wedge a + b < d$
 guard for new event ML-TL

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

```

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

abstract guard from ml:
 $a = 0 \wedge b > 0$

sets: COLOR

constants: red, green

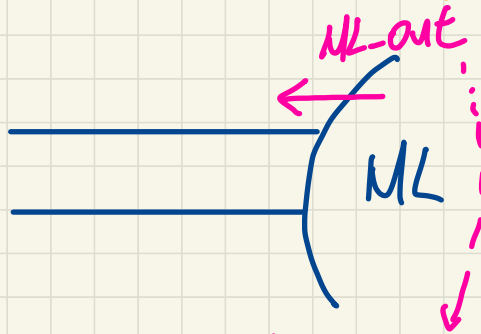
axioms:
 axm2.1 : COLOR = {green, red}
 axm2.2 : green ≠ red

variables:
 a, b, c
 ml_tl
 il_tl

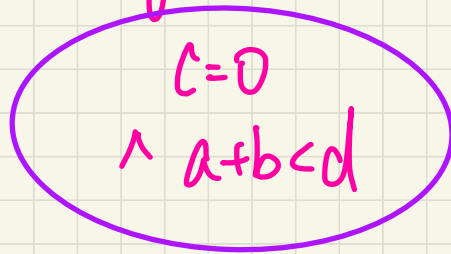
invariants:
 inv2.1 : ml_tl ∈ COLOUR
 inv2.2 : il_tl ∈ COLOUR
 inv2.3 : ml_tl = green ⇒ a + b < d ∧ c = 0
 inv2.4 : il_tl = green ⇒ b > 0 ∧ a = 0

M_1
(1st refinement)

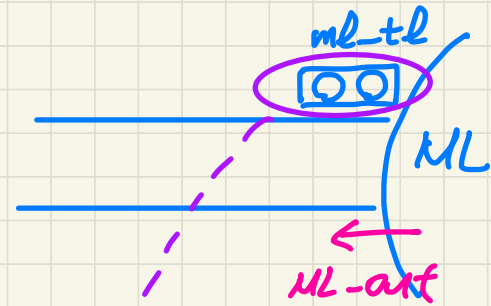
no notion
of traffic light



guard:



M_2
(2nd refinement)



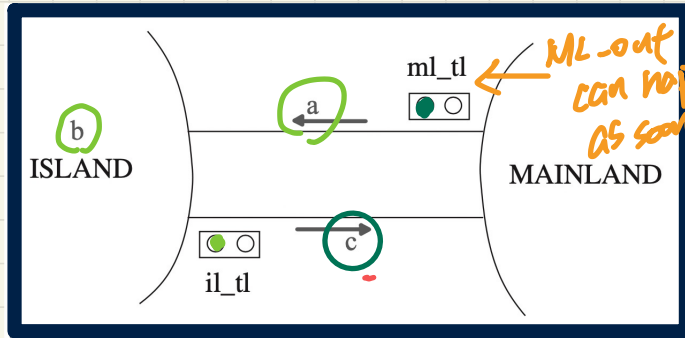
New Event:

$ml-tl-green$
 \Rightarrow guard

driver following
TL.

guard:
 $ml-tl = green$

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



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 M_1

IL_tl_green:

turn the traffic light `il_tl` to green

```

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

$il_tl = red$
 $b > 0$
 $a = 0$

abstract guard of IL-out in M_1

sets: `COLOR`

constants: `red, green`

axioms:

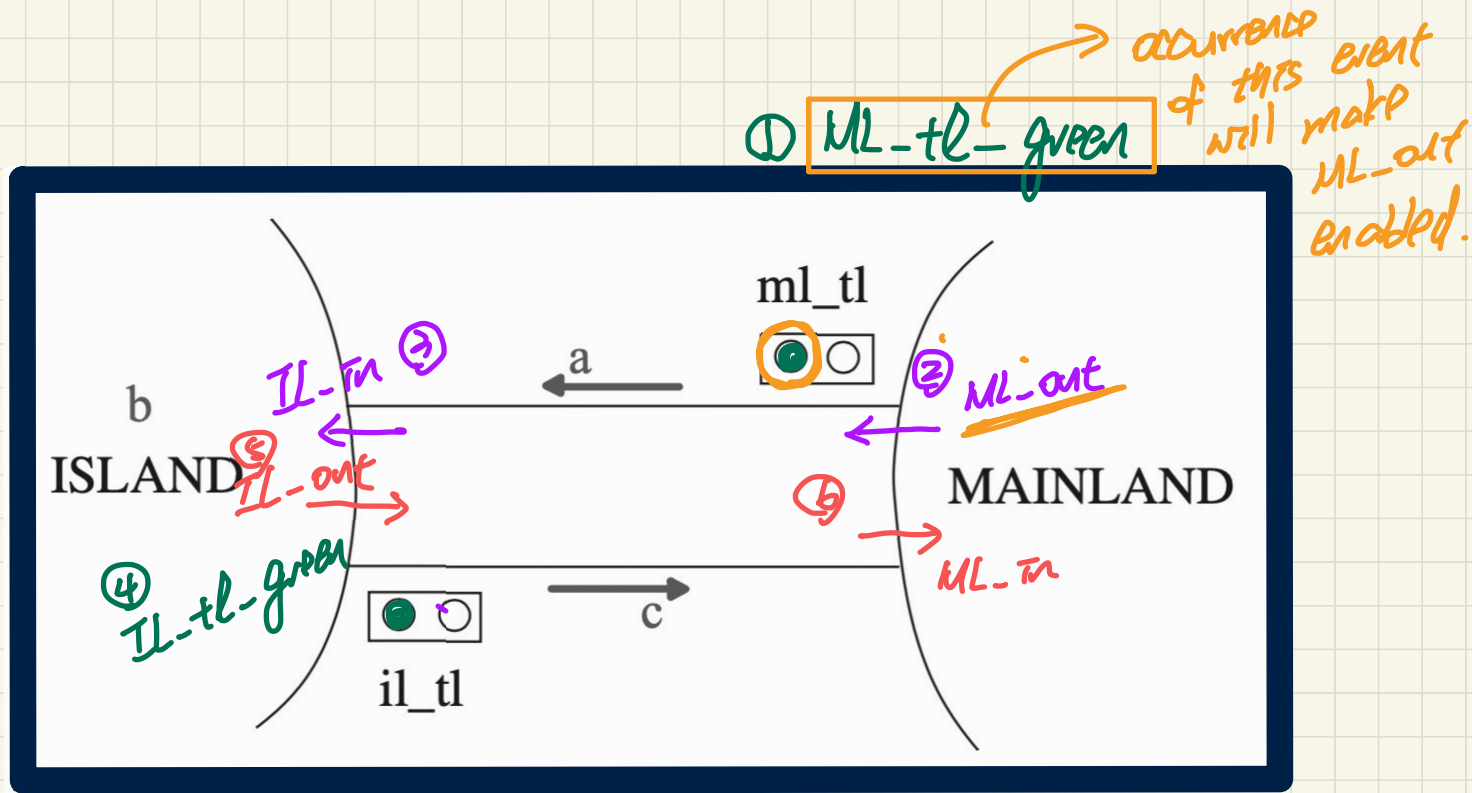
axm2.1 : `COLOR` = {`green, red`}
 axm2.2 : `green` ≠ `red`

variables:

`a, b, c`
`ml_tl`
`il_tl`

invariants:

inv2.1 : `ml_tl` ∈ `COLOUR`
 inv2.2 : `il_tl` ∈ `COLOUR`
 inv2.3 : `ml_tl` = `green` ⇒ `a` + `b` < `d` ∧ `c` = 0
 inv2.4 : `il_tl` = `green` ⇒ `b` > 0 ∧ `a` = 0



How can the order of events be enforced?

A. By the design of event guards.

Lecture

Reactive System: Bridge Controller

2nd Refinement: Invariant Preservation

PO/VC Rule of Invariant Preservation: Sequents

Abstract m1

variables: a, b, c	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
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: $a = 0 \vee c = 0$		

$A(c)$

$I(c, v)$

$J(c, v, w)$

$H(c, w)$

\vdash

$J_i(c, E(c, v), F(c, w))$

Concrete m2

variables: a, b, c ml_tl il_tl	ML_out when $ml_tl = green$ then $a := a + 1$ end <i>↳ BAP:</i>	IL_out when $il_tl = green$ then $b := b - 1$ $c := c + 1$ end
invariants: inv2.1: $ml_tl \in COLOUR$ inv2.2: $il_tl \in COLOUR$ * inv2.3: $ml_tl = green \Rightarrow a + b < d \wedge c = 0$ * inv2.4: $il_tl = green \Rightarrow b > 0 \wedge a = 0$		

** $\{il_tl = green\} = green \Rightarrow b' > 0 \wedge a' = 0$*
 il_tl
 b *$a+1$*

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	$il_tl = green \Rightarrow b > 0 \wedge a = 0$

abs. inv. from m1


con. inv. from m2

Concrete guards of ML_out

$ml_tl = green$

*Concrete invariant inv2.4**
with ML_out's effect in the post-state

$\{ il_tl = green \Rightarrow b > 0 \wedge (a + 1) = 0$



Exercise: Specify IL_out/inv2_3/INV

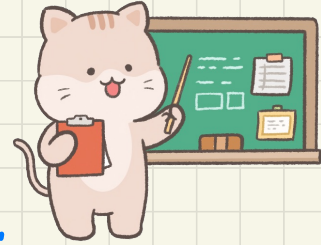
$a' = a + 1$
 $b' = b \wedge c' = c \wedge ml_tl' = ml_tl$
 $\wedge il_tl' = il_tl$

Example Inference Rules

$$\frac{H, P, Q \vdash R}{H, P, P \Rightarrow Q \vdash R} \text{IMP_L}$$

Modus Ponens

$$P \wedge (P \Rightarrow Q) \equiv Q.$$



$$\frac{H, P \Rightarrow Q}{H \Rightarrow (P \Rightarrow Q)} \text{IMP_R}$$

Shunting

$$P \wedge Q \Rightarrow V \equiv P \Rightarrow (Q \Rightarrow V)$$

$$\frac{H, \neg Q \vdash P}{H, \neg P \Rightarrow Q} \text{NOT_L}$$

Contra-positiv

$$P \Rightarrow Q \equiv \neg Q \Rightarrow \neg P$$

Discharging **POs** of m2: Invariant Preservation

First Attempt

ML_out/inv2_4/INV

Outstanding/Unprovable leg

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

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

MON

green ≠ 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 ≠ 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 ≠ red
 $b > 0 \wedge a = 0$
 $ml_tl = green$
 $il_tl = green$
 \vdash
 $b > 0 \wedge (a+1) = 0$

AND_L

green ≠ red
 $b > 0$
 $a = 0$
 $ml_tl = green$
 $il_tl = green$
 \vdash
 $b > 0 \wedge (a+1) = 0$

AND_R

green ≠ red
 $b > 0$
 $a = 0$
 $ml_tl = green$
 $il_tl = green$
 \vdash
 $b > 0$

HYP

green ≠ red
 $b > 0$
 $a = 0$
 $ml_tl = green$
 $il_tl = green$
 \vdash
 $(a+1) = 0$

EQ_LR,
MON

green ≠ red
 $ml_tl = green$
 $il_tl = green$
 \vdash
 $(0+1) = 0$

ARI

green ≠ 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

$$\frac{H \vdash P \quad H \vdash Q}{H \vdash P \wedge Q} \text{ AND_R}$$

$$\frac{H, P, Q \vdash R}{H, P \wedge Q \vdash R} \text{ AND_L}$$

$$\frac{H, P, Q \vdash R}{H, P, P \Rightarrow Q \vdash R} \text{ IMP_L}$$

$$\frac{H, P \vdash Q}{H \vdash P \Rightarrow Q} \text{ IMP_R}$$

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

EQ_LR,
MON

$green \neq red$
 $a + b < d$
 $c = 0$
 $il_tl = green$
 $ml_tl = green$
 \vdash
 $(c + 1) = 0$

$green \neq red$
 $il_tl = green$
 $ml_tl = green$
 \vdash
 $(0 + 1) = 0$

ARI

$green \neq red$
 $il_tl = green$
 $ml_tl = green$
 \vdash
 $1 = 0$

SHOCKED



??

Understanding the Failed Proof on INV

Exercise

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

* **IL_out/inv2_3/INV**

```

d ∈ ℕ
d > 0
COLOUR = {green, red}
green ≠ red
n ∈ ℕ
n ≤ d
a ∈ ℕ
b ∈ ℕ
c ∈ ℕ
a + b + c = n
a = 0 ∨ c = 0
ml_tl ∈ COLOUR
il_tl ∈ COLOUR
ml_tl = green ⇒ a + b < d ∧ c = 0
il_tl = green ⇒ b > 0 ∧ a = 0
il_tl = green ⇒ a + (b - 1) < d ∧ (c + 1) = 0
    
```

Contradiction

ML_out/inv2_4/INV

```

d ∈ ℕ
d > 0
COLOUR = {green, red}
green ≠ red
n ∈ ℕ
n ≤ d
a ∈ ℕ
b ∈ ℕ
c ∈ ℕ
a + b + c = n
a = 0 ∨ c = 0
ml_tl ∈ COLOUR
il_tl ∈ COLOUR
ml_tl = green ⇒ a + b < d ∧ c = 0
il_tl = green ⇒ b > 0 ∧ a = 0
il_tl = green ⇒ b > 0 ∧ (a + 1) = 0
    
```

Unprovable Sequent:

$green \neq red$
 $\wedge il_tl = green$
 $\wedge ml_tl = green$
 $\vdash 1 = 0$



init	ML_tl_green	ML_out	IL_in	IL_tl_green	IL_out	ML_out
$d = 2$	$d = 2$	$d = 2$	$d = 2$	$d = 2$	$d = 2$	$d = 2$
$a' = 0$	$a' = 0$	$a' = 1$	$a' = 0$	$a' = 0$	$a' = 0$	$a' = 1$
$b' = 0$	$b' = 0$	$b' = 0$	$b' = 1$	$b' = 1$	$b' = 0$	$b' = 0$
$c' = 0$	$c' = 0$	$c' = 0$	$c' = 0$	$c' = 0$	$c' = 1$	$c' = 1$
$ml_tl' = red$ $il_tl' = red$	$ml_tl' = green$ $il_tl' = red$	$ml_tl' = green$ $il_tl' = red$	$ml_tl' = green$ $il_tl' = red$	$ml_tl' = green$ $il_tl' = green$	$ml_tl' = green$ $il_tl' = green$	$ml_tl' = green$ $il_tl' = green$

Lecture

Reactive System: Bridge Controller

***2nd Refinement: Fixing the Model
Adding an Invariant***

Fixing **m2**: Adding an Invariant



Abstract **m1**

variables: a, b, c

invariants:

$\text{inv1.1} : a \in \mathbb{N}$
 $\text{inv1.2} : b \in \mathbb{N}$
 $\text{inv1.3} : c \in \mathbb{N}$
 $\text{inv1.4} : a + b + c = n$
 $\text{inv1.5} : a = 0 \vee c = 0$

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

REQ3

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

inv2.5: $ml_tl = red \vee il_tl = red$

Concrete **m2**

variables:

a, b, c
 ml_tl
 il_tl

invariants:

$\text{inv2.1} : ml_tl \in \text{COLOUR}$
 $\text{inv2.2} : il_tl \in \text{COLOUR}$
 $\text{inv2.3} : ml_tl = green \Rightarrow a + b < d \wedge c = 0$
 $\text{inv2.4} : il_tl = green \Rightarrow b > 0 \wedge a = 0$

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

ML_out/inv2_4/INV

$\text{axm0.1} \{ d \in \mathbb{N}$
 $\text{axm0.2} \{ d > 0$
 $\text{axm2.1} \{ \text{COLOUR} = \{green, red\}$
 $\text{axm2.2} \{ green \neq red$
 $\text{inv0.1} \{ n \in \mathbb{N}$
 $\text{inv0.2} \{ n \leq d$
 $\text{inv1.1} \{ a \in \mathbb{N}$
 $\text{inv1.2} \{ b \in \mathbb{N}$
 $\text{inv1.3} \{ c \in \mathbb{N}$
 $\text{inv1.4} \{ a + b + c = n$
 $\text{inv1.5} \{ a = 0 \vee c = 0$
 $\text{inv2.1} \{ ml_tl \in \text{COLOUR}$
 $\text{inv2.2} \{ il_tl \in \text{COLOUR}$
 $\text{inv2.3} \{ ml_tl = green \Rightarrow a + b < d \wedge c = 0$
 $\text{inv2.4} \{ il_tl = green \Rightarrow b > 0 \wedge a = 0$
 $\text{inv2.5} \{ ml_tl = red \vee il_tl = red$
 $\{ ml_tl = green$

Concrete guards of **ML_out**

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**

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
 $il_tl = green \Rightarrow b > 0 \wedge (a+1) = 0$

IMP L
 $green \neq red$
 $il_tl = green \Rightarrow b > 0 \wedge a = 0$
 $ml_tl = green$
 $ml_tl = red \vee il_tl = red$
 $il_tl = green$
 \vdash
 $b > 0 \wedge (a+1) = 0$

$green \neq red$
 $ml_tl = green$
 $ml_tl = red \vee il_tl = red$
 $il_tl = green$
 \vdash
 $1 = 0$

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
 $b > 0 \wedge (a+1) = 0$

$green \neq red$
 $ml_tl = green$
 $ml_tl = red$
 $il_tl = green$
 $1 = 0$

Exercise

HYP
 $green \neq red$
 $b > 0$
 $a = 0$
 $ml_tl = green$
 $ml_tl = red \vee il_tl = red$
 $il_tl = green$
 \vdash
 $b > 0$

EQ_LR, MON
 $green \neq red$
 $b > 0$
 $a = 0$
 $ml_tl = green$
 $ml_tl = red \vee il_tl = red$
 $il_tl = green$
 \vdash
 $(a+1) = 0$

EQ_LR, MON

Approach 1: NOT_L

$green \neq red$
 $green = red$
 $il_tl = green$
 $1 = 0$

Approach 2: ARI

used to be unprovable before EN2-5 was written.

☆ Good job ☆

ARI

$green \neq red$
 $ml_tl = green$
 $ml_tl = red \vee il_tl = red$
 $il_tl = green$
 \vdash
 $1 = 0$

↓
EN2-5

$$\frac{H, \neg Q \vdash P}{H, \neg P \vdash Q} \text{ NOT_L}$$

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

$$\frac{H, P \vdash R \quad H, Q \vdash R}{H, P \vee Q \vdash R} \text{ OR_L}$$

Discharging POs of m2: Invariant Preservation

Second Attempt

IL_out/inv2_3/INV

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

$green \neq red$
 $il_tl = green$
 $ml_tl = red \vee il_tl = red$
 $ml_tl = green$
 \vdash
 $1 = 0$



Assignment

MON
 $green \neq red$
 $ml_tl = green \Rightarrow a + b < d \wedge c = 0$
 $ml_tl = red \vee il_tl = red$
 $il_tl = green$
 \vdash
 $ml_tl = green \Rightarrow a + (b - 1) < d \wedge (c + 1) = 0$

IMP R

$green \neq red$
 $ml_tl = green \Rightarrow a + b < d \wedge c = 0$
 $il_tl = green$
 $ml_tl = red \vee il_tl = red$
 $ml_tl = green$
 \vdash
 $a + (b - 1) < d \wedge (c + 1) = 0$

IMP L

$green \neq red$
 $a + b < d \wedge c = 0$
 $il_tl = green$
 $ml_tl = red \vee il_tl = red$
 $ml_tl = green$
 \vdash
 $a + (b - 1) < d \wedge (c + 1) = 0$

AND L

$green \neq red$
 $a + b < d$
 $c = 0$
 $il_tl = green$
 $ml_tl = red \vee il_tl = red$
 $ml_tl = green$
 \vdash
 $a + (b - 1) < d \wedge (c + 1) = 0$

AND R

$green \neq red$
 $a + b < d$
 $c = 0$
 $il_tl = green$
 $ml_tl = red \vee il_tl = red$
 $ml_tl = green$
 \vdash
 $a + (b - 1) < d$

MON

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

ARI

$green \neq red$
 $a + b < d$
 $c = 0$
 $il_tl = green$
 $ml_tl = red \vee il_tl = red$
 $ml_tl = green$
 \vdash
 $(c + 1) = 0$

EQ LR, MON

$green \neq red$
 $il_tl = green$
 $ml_tl = red \vee il_tl = red$
 $ml_tl = green$
 \vdash
 $(0 + 1) = 0$

ARI

$green \neq red$
 $il_tl = green$
 $ml_tl = red \vee il_tl = red$
 $ml_tl = green$
 \vdash
 $1 = 0$

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

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

$$\frac{H, P \vdash R \quad H, Q \vdash R}{H, P \vee Q \vdash R} \text{ OR.L}$$