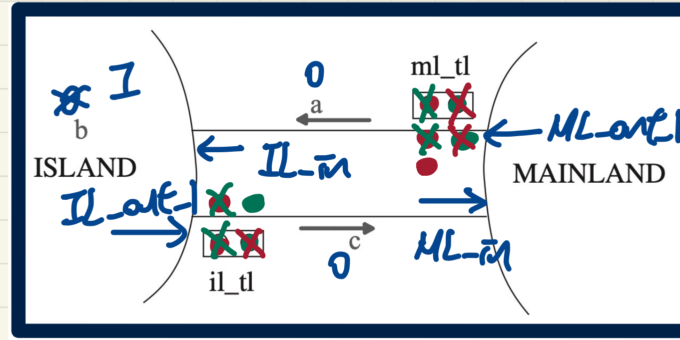
Lecture 2

Part R

Case Study on Reactive Systems -
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, finite trace

⟨init, $\underbrace{\text{ML\_tl\_green}}_{\text{a new event}}$, ML_out_1, IL_in, (old events) IL_tl_green, IL_out_1, ML_in⟩

also a valid trace of m2, but leading to livelock

Is ML_tl_g. enabled?

Is IL_tl_g. enabled?

⟨ 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 event 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

enable

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

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

init: 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
>		

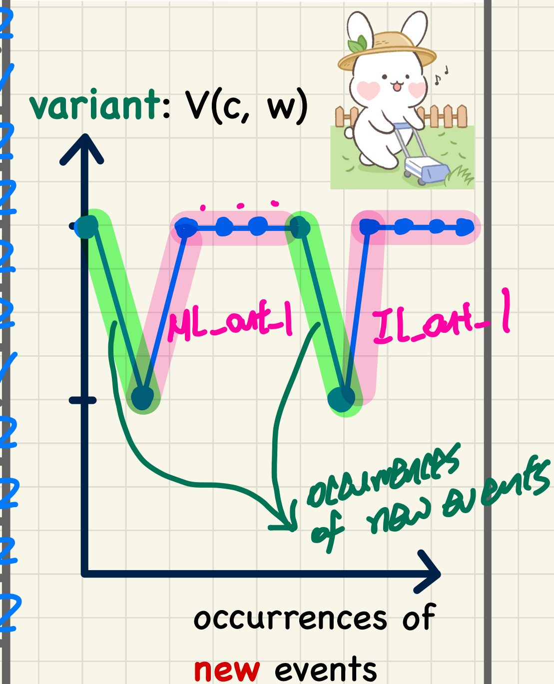
Fixing m2: Measuring Traffic Light Changes

```
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	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

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

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

```
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: $ml\_pass' = 0$
$il\_pass' = il\_pass$

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

Concrete guards of ML_tl_green

$\vdash$

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

Lecture 2

Part S

Case Study on Reactive Systems - Bridge Controller 2nd Refinement: Relative Deadlock Freedom

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

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 $ml\_tl = green$, $a + b + 1 \neq d$
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

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

Study

Ex.1

⋮

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

Ex.2

...

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

Ex3

...

$d > 0$, $b \in \mathbb{N}$ $\vdash$ $b < d \lor b > 0$ **ARI** $d > 0$, $b > 0 \lor b = 0$ $\vdash$ $b < d \lor b > 0$ **OR_L**

- $d > 0$, $b > 0$ $\vdash$ $b < d \lor b > 0$ **OR_R2** $d > 0$, $b > 0$ $\vdash$ $b > 0$ **HYP**
- $d > 0$, $b = 0$ $\vdash$ $b < d \lor b > 0$ **EQ_LR, MON** $d > 0$ $\vdash$ $0 < d \lor 0 > 0$ **OR_R1** $d > 0$ $\vdash$ $0 < d$ **HYP**

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

variants: $ml\_pass + il\_pass$

divergence freedom

```
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

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 ≠ 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
```