Lecture 18 - March 28

Reactive System: Bridge Controller

Announcements

- Bonus Opportunity - **Course Evaluation**
- **ProgTest1**: Andy (eMail, Zoom); Jackie (Office Hour)
- **Lab3 Part 2** released
- **ProgTest2** → format identical to Labs

  60%
  Part 1: complete context

  Part 2: complete manual proofs
- **Final Exam**: Review Q&A Sessions

Tue: 1pm Maria

Thur: 2:30pm Andy

Exam

- ↳ 3 hours] Sunday, April 16 2pm (tennis centre)
- ↳ papper (no Rodin, but you may be asked to read or write in Rodin syntax)
- ↳ a piece of data sheet allowed
  - ↳ 1. one side
  - 2. computer-typed (font ≥ 10pt)

Livelock Caused by New Events Diverging

An alternative m1 (for demonstration)

constants: d

axioms:
- **axm0_1** : $d \in \mathbb{N}$
- **axm0_2** : $d > 0$

variables: a, b, c

invariants:
- **inv1_1** : $a \in \mathbb{Z}$
- **inv1_2** : $b \in \mathbb{Z}$
- **inv1_3** : $c \in \mathbb{Z}$

old events

new events.

guardless
↳ always enabled

```
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
  begin
    a := a − 1
    b := b + 1
  end
```

```
IL_out
  begin
    b := b − 1
    c := c + 1
  end
```

as if:
while(1){
;
}

Abstract Transitions: < init , skip , skip , skip , skip , ... >

2. none of the old events is allowed to occur

Concrete Transitions: < init , IL_in , IL_out , IL_in , IL_out , ... >

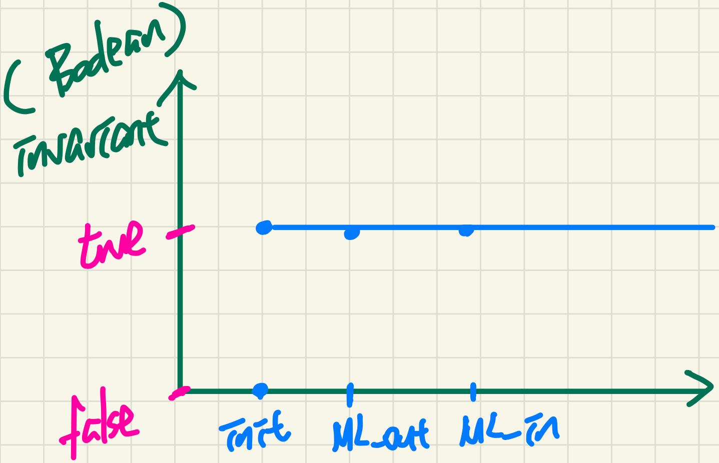
divergence : livelock

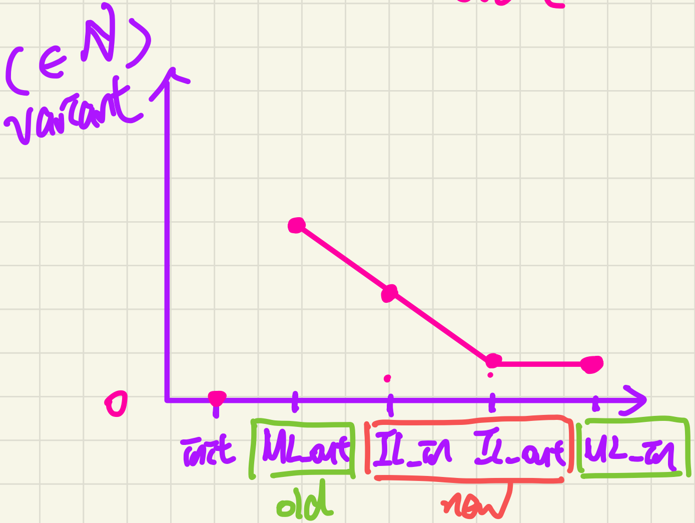
↳ a set of events keep interleaving.

↳ 1. new events interleave indefinitely

Invariant : Boolean exp. that should always hold true after each event occurrence.

Variant : Integer exp. that may change after event occurrence.





Q. Is an infinite interleaving of old events bad?

$$\begin{tikzcd}
\text{concrete} & \langle\, \text{init}, & \text{ML\_out} \arrow[d] & , \text{ML\_out}, \ldots \,\rangle \\
\text{abstract} & \langle\, \text{init}, & \text{ML\_out} & , \text{ML\_out}, \ldots \,\rangle
\end{tikzcd}$$

Use of a Variant to Measure New Events Converging

fixed

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 : $a = 0 \lor c = 0$

old

```
ML_out
  when
    a + b < d
    c = 0
  then
    a := a + 1
  end
```

```
ML_in
  when
    c > 0
  then
    c := c − 1
  end
```

new

```
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
```

IL ML

Exercise: VAR: $a+b$.

Variants for New Events: $2 \cdot a + b$

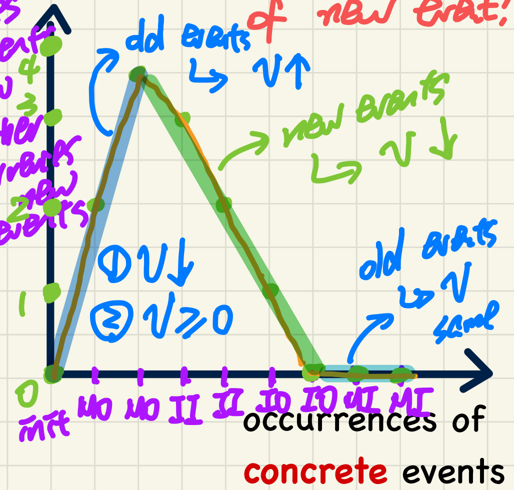
Is it still possible to have an occurrence of new event?

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

	init	ML_out	ML_out	IL_in	IL_in	IL_out	IL_out	ML_in	ML_in
a =	0	1	2	1	0	0	0	0	0
b =	0	0	0	1	2	1	0	0	0
c =	0	0	0	0	0	1	2	1	0
v =	0	2	4	3	2	1	0	0	0

occurrences of old events allow further occurrences of new events

variant: $2 \cdot a + b$



PO of Convergence/Non-Divergence/Livelock Freedom

Variant Stays Non-Negative

$A(c)$ axioms

$I(c, v)$ abs. inv.

$J(c, v, w)$ con. inv.

$H(c, w)$ con. grd

$\vdash$

$V(c, w) \in \mathbb{N}$

NAT

IL_in/NAT

$d \in \mathbb{N}$

$d > 0$

$n \in \mathbb{N}$

$n \leq d$

$a \in \mathbb{N}$ $c \in \mathbb{N}$ $a = 0 \lor c = 0$

$b \in \mathbb{N}$ $a + b + c = n$ $a > 0$

A New Event Occurrence Decreases Variant

$A(c)$

$I(c, v)$

$J(c, v, w)$

$H(c, w)$

$\vdash$

post-state ✓ pre-state ✓

$V(c, F(c, w)) < V(c, w)$

VAR

IL_in/VAR

$d \in \mathbb{N}$

$d > 0$

$n \in \mathbb{N}$

$n \leq d$

$a \in \mathbb{N}$ $c \in \mathbb{N}$ $a = 0 \lor c = 0$

$b \in \mathbb{N}$ $a + b + c - n$ $a > 0$

Variants for New Events: 2 · a + b

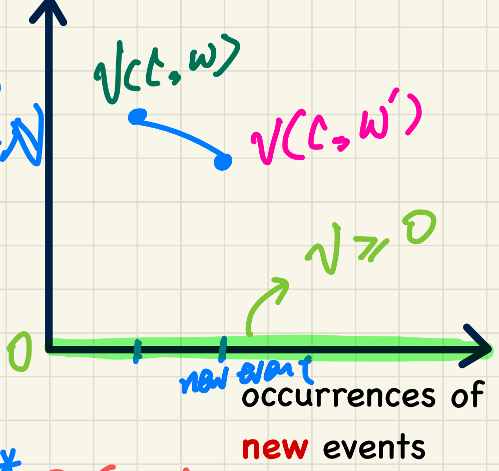
How many NAT POs to generate?

concrete (old + new) events

variant: V(c, w)

$\vdash 2 \cdot a + b$

$\in \mathbb{N}$



$\vdash \boxed{2 \cdot (a-1) + (b+1) <} \; 2 \cdot a + b$

$2 \cdot \overset{a-1}{\cancel{a}} + \overset{b+1}{\cancel{b}} < 2 \cdot a + b$

Example Inference Rules

$$\frac{H, \neg P \vdash Q}{H \vdash P \vee Q} \quad \text{OR\_R}$$

Justify:

$$H \Rightarrow P \vee Q \overset{\Leftrightarrow}{\equiv} H \wedge \neg P \Rightarrow Q$$

$$\frac{H \vdash P}{H \vdash P \vee Q} \quad \text{OR\_R1}$$

$$\boxed{H \vdash P \vee Q} \quad \text{ARI} \quad \boxed{H \vdash Q \vee P} \quad \text{OR\_R} \quad \boxed{H \; \neg Q \vdash P}$$

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

$$\frac{H \vdash P \qquad H \vdash Q}{H \vdash P \wedge Q} \quad \text{AND\_R}$$