Lecture 21 - Nov. 21

Bridge Controller

Proof Obligations of System Variant

Announcements/Reminders

- **Lab5** released (due on Tuesday, December 3)
- **WrittenTest2** results to be released on Wednesday
- **Exam** review sessions polling
- **Bonus** Opportunity coming: Formal Course Evaluation

LiveLock / Divergence

→ Caused by an infinite interleaving of

new events / Concrete model, busy looping in the abstract model

→ Variant ($\in \mathbb{N}$) is

~ not the cause of livelock of a model

~ just a measure on if livelock is present in your model

→ 2 POs → provable means the model livelocks & needs to be fixed

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 : $a = 0 \vee c = 0$

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

ML_in
when
$c > 0$
then
$c := c - 1$
end

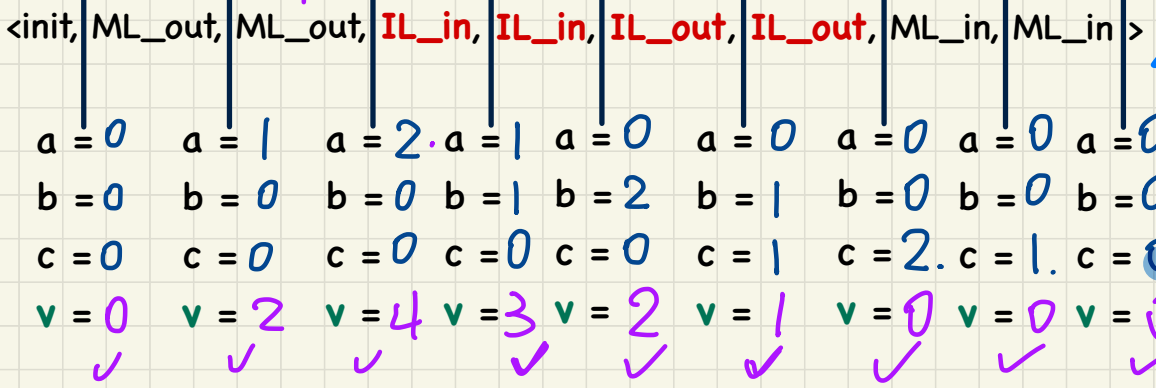
IL_in
when
$a > 0$
then
$a := a - 1$
$b := b + 1$
end

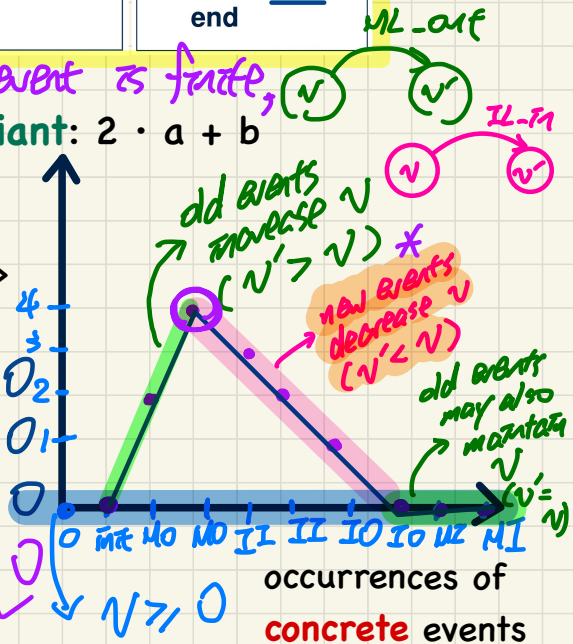
IL_out
when
$b > 0$
$a = 0$
then
$b := b - 1$
$c := c + 1$
end

* Given that the starting value of v of the first new event is finite,

Variants for New Events: 2 · a + b

the # of interleaved new events is also finite.





PO of Convergence/Non-Divergence/Livelock Freedom

Variants for New Events: 2 · a + b

Variant Stays Non-Negative

$A(c)$
$I(c, v)$
$J(c, v, w)$
$H(c, w)$
$\vdash$ $V(c, w) \in \mathbb{N}$

guard of new event

NAT

IL_in/NAT

new event

$v \geq 0$

$d \in \mathbb{N}$
$d > 0$
$n \in \mathbb{N}$ $n \leq d$

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

$\vdash 2 \cdot a + b \in \mathbb{N}$

* $v' < v$ $(b+1)$

$2 \cdot a' + b' < 2 \cdot a + b$

$(a-1)$

variant: V(c, w)

v

$V(c, w)$

v

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

IL_in/NAT

new event

occurrences of **new** events

A New Event Occurrence Decreases Variant

$A(c)$
$I(c, v)$
$J(c, v, w)$
$H(c, w)$
$\vdash$ $V(c, F(c, w)) < V(c, w)$

$a' = a - 1$ $\wedge$ $b' = b + 1$

effect of new event

v v

VAR

IL_in/VAR

new event

v's value strictly decreased.

$d \in \mathbb{N}$
$d > 0$
$n \in \mathbb{N}$ $n \leq d$

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

* $\vdash 2 \cdot (a-1) + (b+1) < 2 \cdot a + b$

Exercise Given variant: $a + b$

(1) Re-trace the value of v using the same trace (and plot the diagram). Can the same patterns be observed?

(2) Formulate the VAR and VAT POs. ($2 * 2 = 4$ sequents)

VAT, VAR — IL-in, IL-out

(3) Are they provable?

Example Inference Rules

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

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

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

$H \Rightarrow P \vee Q$

$\equiv \{ P \equiv \neg\neg P \}$

$H \Rightarrow \neg(\neg P) \vee Q$

$\equiv \{ P \Rightarrow Q \equiv \neg P \vee Q \}$

$H \Rightarrow (\neg P \Rightarrow Q)$

$\equiv \{$ shunting $\}$

$H \wedge \neg P \Rightarrow Q$

Question

$R \vee S \vdash P \wedge Q$

# of maximum sequents to prove instead?