Lecture 20 - Nov 18

Bridge Controller

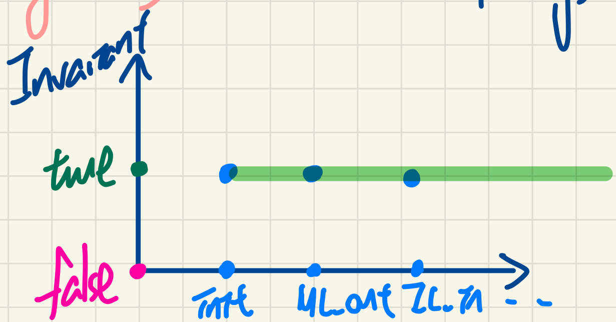
Invariant vs. Variant
Observing Patterns of Variant Values
POs of Variants: NAT vs. VAR

Announcements/Reminders

- Today's class: notes template posted
- Lab4 released
- A reference paper for the tabular method (Lab4)
- Online course evaluation

Invariant vs. Variant

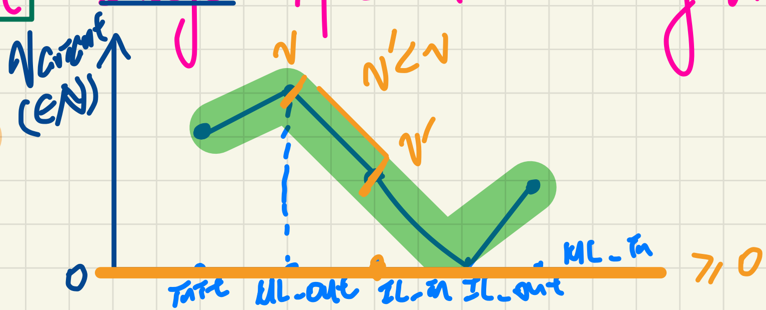
Invariant (system) : Boolean expression that should always hold (after init and all event occurrences)



$\in \mathbb{N} \geq 0$

Variant : Integer expression that may change after event occurrences.

meant to measure # of interleavings of new events



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 : $a = 0 \lor c = 0$

ML_out
when
$a + b < d$
$c = 0$
then
$a := \underline{a + 1}$
end

ML_in
when
$c > 0$
then
$c := \underline{c - 1}$
end

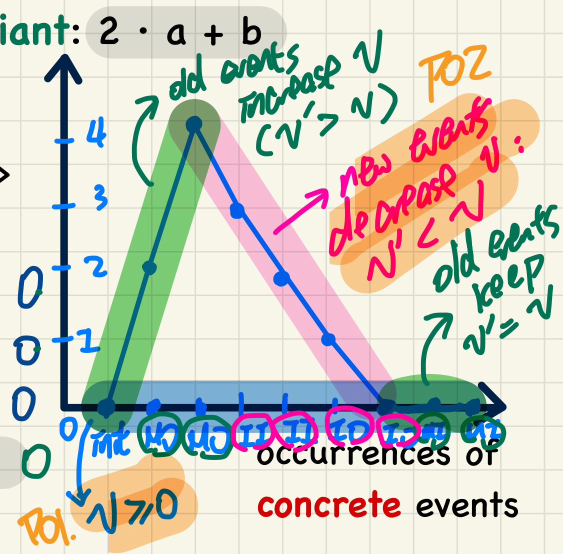
IL_in
when
$\boxed{a > 0}$
then
$a := \underline{a - 1}$
$b := \underline{b + 1}$
end

IL_out
when
$b > 0$
$a = 0$
then
$b := \underline{b - 1}$
$c := \underline{c + 1}$
end

Variants for New Events: 2 · a + b

<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



PO of Convergence/Non-Divergence/Livelock Freedom

Variant Stays Non-Negative

$$\frac{\begin{array}{l} A(c) \\ I(c,v) \\ J(c,v,w) \\ H(c,w) \\ \vdash \\ V(c,w) \in \mathbb{N} \end{array}}{}\ \text{NAT}$$

$A(c)$ actions
$I(c,v)$ abs. Inv.
$J(c,v,w)$ con. Inv.
$H(c,w)$ guard of new event.
const.
variant
con. var.

IL_in/NAT

new event $v \geq 0$

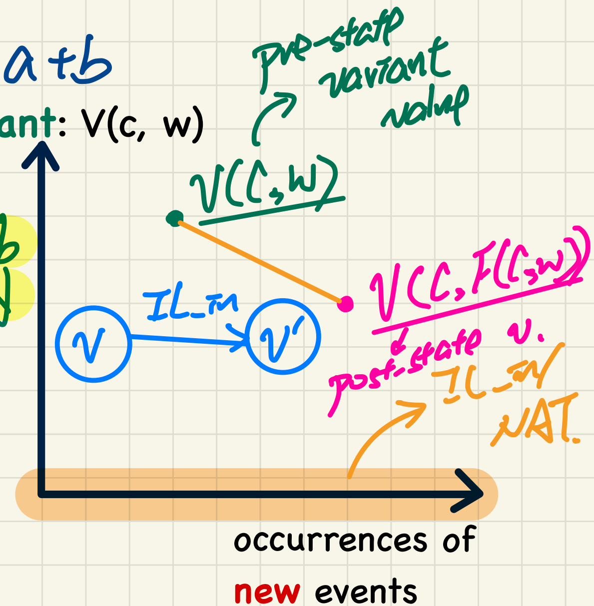
$d \in \mathbb{N}$
$d > 0$
$n \in \mathbb{N}$ $a \in \mathbb{N}$ $b \in \mathbb{N}$ $c \in \mathbb{N}$ $a > 0$
$n \leq d$ $a = 0 \lor c = 0$ $a + b + c = n$
$\vdash 2 \cdot a + b \in \mathbb{N}$

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

* $v' < v$

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

$a-1$ $b+1$



A New Event Occurrence Decreases Variant

$$\frac{\begin{array}{l} A(c) \\ I(c,v) \\ J(c,v,w) \\ H(c,w) \\ \vdash \\ V(c, F(c,w)) < V(c,w) \end{array}}{}\ \text{VAR}$$

effect of new event.
v'
v

IL_in/VAR

new event
v's value strictly dec.

$d \in \mathbb{N}$
$d > 0$
$n \in \mathbb{N}$ $a \in \mathbb{N}$ $b \in \mathbb{N}$ $c \in \mathbb{N}$ $a > 0$
$n \leq d$ $a = 0 \lor c = 0$ $a + b + c = n$
$\vdash$ * $\boxed{2 \cdot (a-1) + (b+1) < 2 \cdot a + b}$

<u>Exercise</u> Given variant: $a + b$

(1) Trace the value of v using the same trace.

Can the same patterns be observed?

(2) Formulate the VAR and NAT POs.

($\underbrace{2}_{\text{IL\_in, IL\_out}}$ * $\underbrace{2}_{\text{NAT, VAR}}$ sequents to prove)

(3) Are they provable?

Example Inference Rules

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

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

disjunction

right of $\vdash$

splitting a single hypothesis to two.

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

left of $\vdash$

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

right of $\vdash$

(compare: OR_L)

$H \Rightarrow P \vee Q$

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

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

$\equiv \{ p \Rightarrow q \equiv \neg p \vee q \}$

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

$\equiv \{ \text{shunting} : x \Rightarrow (y \Rightarrow z) \equiv x \wedge y \Rightarrow z \}$

$H \wedge \neg P \Rightarrow Q$

$$H \vdash P \wedge Q \quad \xrightarrow{\text{AND\_R}} \quad \left\{ \begin{array}{l} H \vdash P \\ H \vdash Q \end{array} \right.$$

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

$$H \vdash \underbrace{(x \lor y)}_{P} \lor \underbrace{z}_{Q} \qquad \text{OR\_R} \qquad H, \neg(x \lor y) \vdash z$$