PO/VC Rule of Invariant Preservation: Sequents

Abstract m0

IL_in/INV1_4/INV

constants: d

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

variables: n

invariants:
inv0_1 : $n \in \mathbb{N}$
inv0_2 : $n \leq d$

$A(c)$
$I(c, v)$
$J(c, v, w)$
$H(c, w)$
$\vdash$
$J_i(c, E(c, v), F(c, w))$

Concrete m1

IL_in/INV1_5/INV

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 : $a = 0 \vee c = 0$

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

Q. How many PO/VC rules for model m1?

Discharging POs of m1: Invariant Preservation in Refinement

IL_in/inv1_4/INV

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

$$\frac{H1 \vdash G}{H1, H2 \vdash G}\ \textbf{MON} \qquad \frac{}{H, P \vdash P}\ \textbf{HYP}$$

Discharging POs of m1: Invariant Preservation in Refinement

ML_in/inv1_5/INV

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

$$\frac{}{\bot \vdash P}\ \textbf{FALSE\_L} \qquad \frac{H1 \vdash G}{H1, H2 \vdash G}\ \textbf{MON} \qquad \frac{H \vdash Q}{H \vdash P \lor Q}\ \textbf{OR\_R2}$$

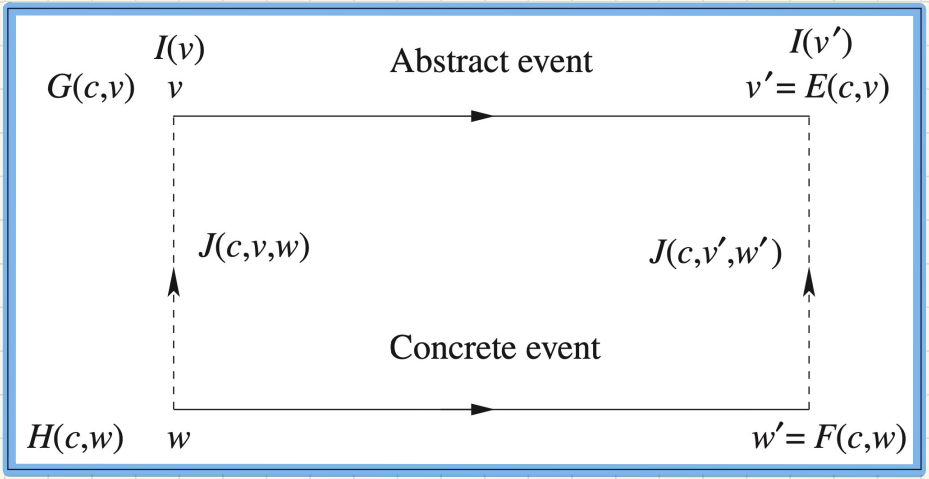
$$\frac{}{H, P \vdash P}\ \textbf{HYP} \qquad \frac{H(F), E = F \vdash P(F)}{H(E), E = F \vdash P(E)}\ \textbf{EQ\_LR} \qquad \frac{H, P \vdash R \quad H, Q \vdash R}{H, P \lor Q \vdash R}\ \textbf{OR\_L}$$

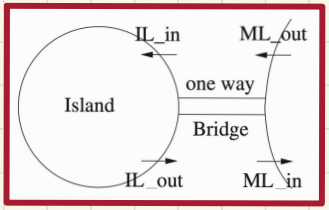
Visualizing Invariant Preservation in Refinement

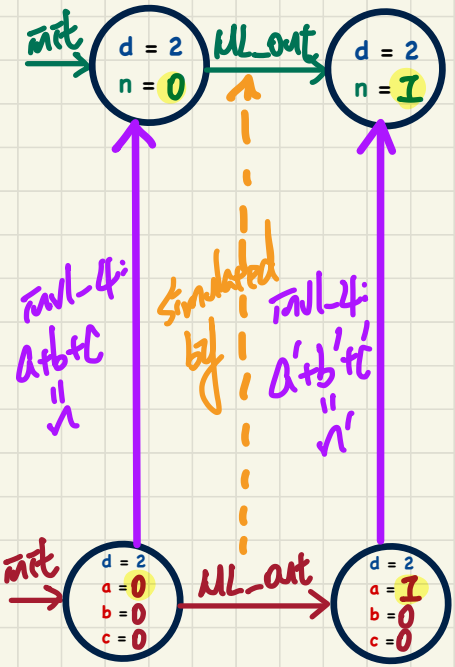
Each new state transition (from w to w′)
should be simulated by
an abstract dummy state transition (from v to v′)

skip
begin

end







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 : $c \in \mathbb{Z}$

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

Use of a Variant to Measure New Events Converging

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

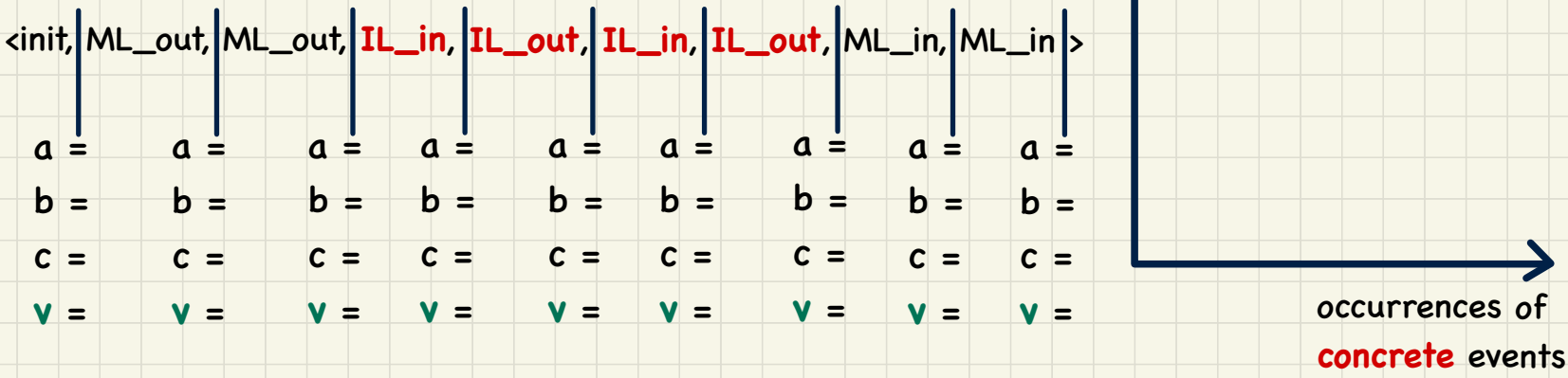
ML_in
when
$c > 0$
then
$c := c - 1$
end

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

Variants for New Events: 2 · a + b

variant: 2 · a + b



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

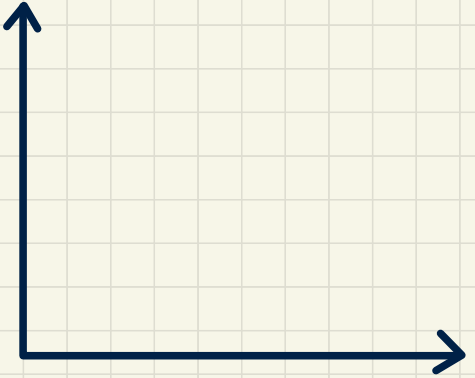
IL_out
when
$b > 0$
$a = 0$
then
$b := b - 1$
$c := c + 1$
end

Variants for New Events: 2 · a + b

variant: 2 · a + b

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

a =	a =	a =	a =	a =	a =	a =	a =	a =
b =	b =	b =	b =	b =	b =	b =	b =	b =
c =	c =	c =	c =	c =	c =	c =	c =	c =
v =	v =	v =	v =	v =	v =	v =	v =	v =



PO of Convergence/Non-Divergence/Livelock Freedom

Variants for New Events: 2 · a + b

Variant Stays Non-Negative

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

IL_in/NAT

A New Event Occurrence Decreases Variant

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

IL_in/VAR