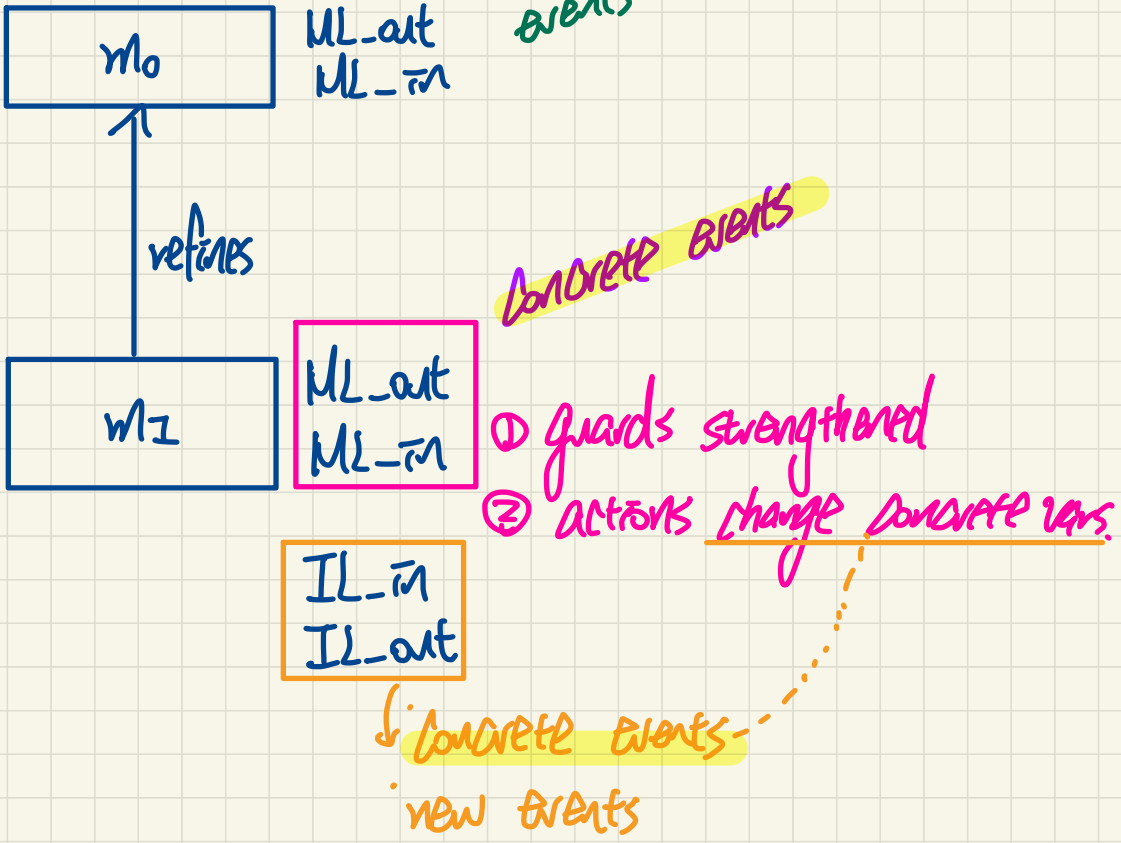
Lecture 2

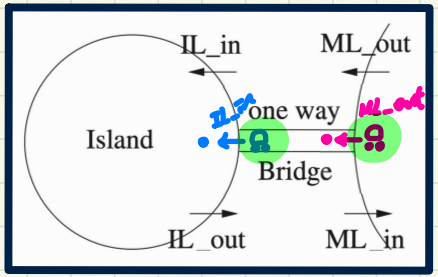
Part J

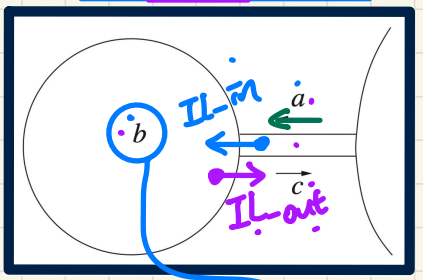
Case Study on Reactive Systems - Bridge Controller
First Refinement: Invariant Preservation
New Events

Events

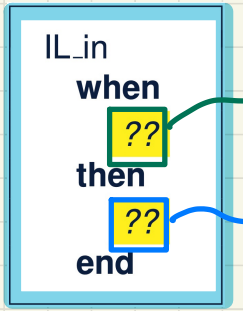

m0
ML_out
ML_in
abstract events
refines
m1
ML_out
ML_in
concrete events
① guards strengthened
② actions change concrete vars.
IL_in
IL_out
concrete events
new events

Bridge Controller: Guarded Actions of "new" Events in 1st Refinement





IL_in: A car enters **island** (getting off the **bridge**).



$c = 0$

$a + b < d$? unnecess.

$a := a - 1$

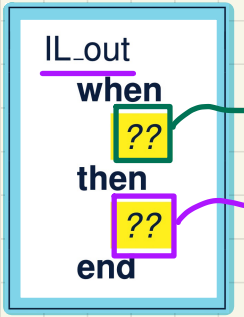
$b := b + 1$

① $a' + b'$ = $(a-1) + (b+1)$ = $a + b$

② ML_out earlier for the same car already checked it

IL_in but $b = d$ which will violate: $n \le d$

IL_out: A car exits **island** (getting on the **bridge**).



$b > 0$

$a = 0$

$b := b - 1$

$c := c + 1$

constants: d

axioms:

axm0_1 : $d \in \mathbb{N}$

axm0_2 : $d > 0$

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 : $a = 0 \vee c = 0$

Before-After Predicates of Event Actions: 1st Refinement

IL_in

when

$a > 0$

then

$a := a - 1$

$b := b + 1$

end

$a' = a - 1$

$\wedge$

$b' = b + 1$

$\wedge$

$c' = c$

IL_out

when

$b > 0$

$a = 0$

then

$b := b - 1$

$c := c + 1$

end

$b' = b - 1$

$\wedge$

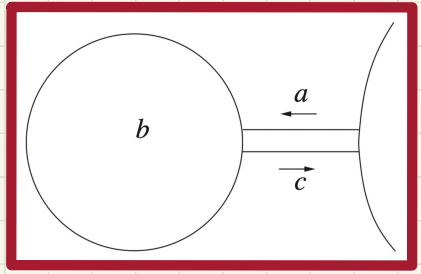
$c' = c + 1$

$\wedge$

$a' = a$

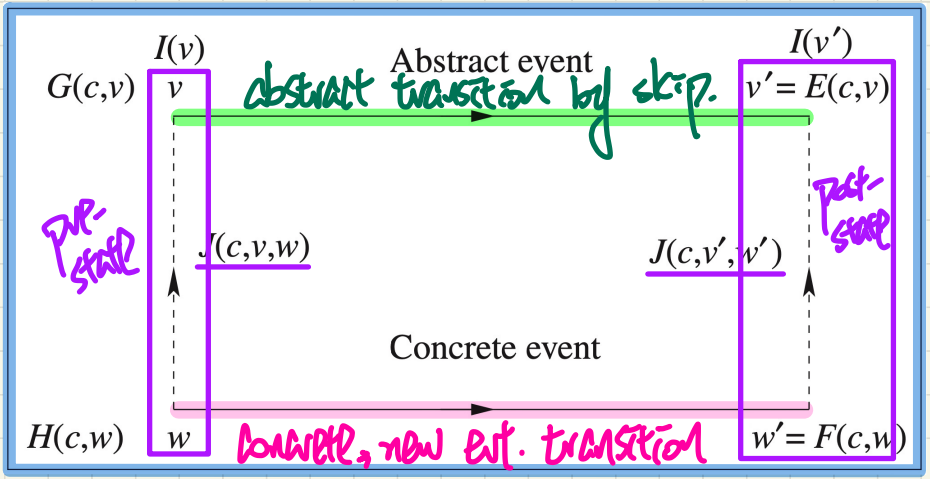
- Pre-State
- Post-State
- Sate Transition

Concrete State Space

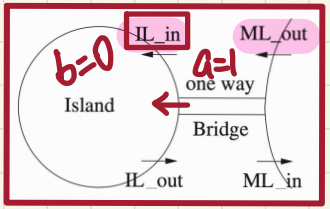


Visualizing Invariant Preservation in Refinement

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

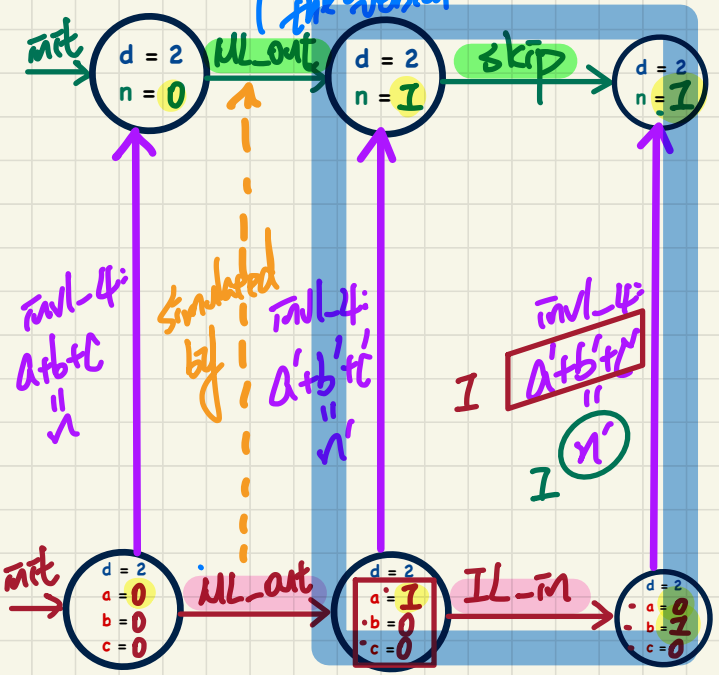


(IL_in & IL_out)



skip
begin
n′=n
end

abs. version simulating the con. version



PO/VC Rule of Invariant Preservation: Sequents

Abstract m0

skip (n'=n)

constants: d

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

variables: n

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

$A(c)$
$I(c, v)$ abs. ew.
$J(c, v, w)$ con. ew
$H(c, w)$ con. guard
$\vdash$
$J_i(c, E(c, v), F(c, w))$ effect of new est.

effect of skip

Concrete 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 : $a = 0 \vee c = 0$

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

BAP: $a' = a-1 \wedge b = b+1 \wedge c' = c$

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

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

IL_in/INV1_4/INV

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

$a' + b' + c' = n'$
$(a-1)(b+1)c$ n

IL_in/INV1_5/INV

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

$a' = 0 \vee c' = 0$
$a-1$ c

Discharging POs of m1: Invariant Preservation in Refinement

IL_in/inv1_4/INV

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

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

MON $\quad a+b+c=n \vdash (a-1)+(b+1)+c=n$ $\quad$ ARI $\quad a+b+c=n \vdash a+b+c=n$ $\quad$ HYP

Discharging POs of m1: Invariant Preservation in Refinement

ML_in/inv1_5/INV

$$\frac{}{\bot \vdash P}\ \text{FALSE\_L}$$

$$\frac{H1 \vdash G}{H1, H2 \vdash G}\ \text{MON}$$

$$\frac{H \vdash Q}{H \vdash P \vee Q}\ \text{OR\_R2}$$

$$\frac{}{H, P \vdash P}\ \text{HYP}$$

$$\frac{H(F), E = F \vdash P(F)}{H(E), E = F \vdash P(E)}\ \text{EQ\_LR}$$

$$\frac{H, P \vdash R \qquad H, Q \vdash R}{H, P \vee Q \vdash R}\ \text{OR\_L}$$

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

pre-state satisfaction of INV_5

post-state satisfaction of INV_5

MON

$a=0 \vee c=0$
$a>0.$
$\vdash$
$(a-1)=0 \vee c=0$

OR_L

$a=0$
$a>0$
$\vdash.$
$(a-1)=0 \vee c=0$

EQ_LR, MON

$0>0$
$\vdash.$
$(0-1)=0 \vee c=0$

ARI

$\bot$
$\vdash$
$-1=0 \vee c=0$

✓ FALSE_L

$c=0$
$a>0$
$\vdash$
$(a-1)=0 \vee c=0$

OR_R2

$c=0$
$a>0$
$\vdash$
$c=0$

✓ HYP

Lecture 2

Part K

Case Study on Reactive Systems - Bridge Controller
First Refinement: Convergence
New Events

Livelock Caused by New Events Diverging

An alternative m1 (for demonstration)

incomplete : lacking (1) connection to abs. state (2) safety constraints.

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

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

while(true);

Shockingly, this model can be proved correct w.r.t. inv preservation.

relative to

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

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

① not deadlock

② livelock : nothing useful ever done

new events diverge

indefinitely, presenting other "old" events.

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 : $a = 0 \vee c = 0$

old events

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

new events

preventing divergence

Exercise
Cont. trace with occ. of IL_out

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

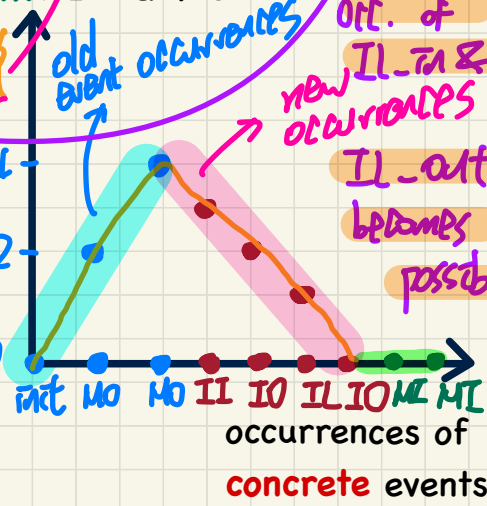
global exp evaluated after each evt occurrence

variant: $2 \cdot a + b$

no further occ. of new evts allowed

s.t. new occ. of IL_in & new occurrences IL_out becomes possible.

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



PO of Convergence/Non-Divergence/Livelock Freedom

↳ applicable to new events

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

Variant Stays Non-Negative

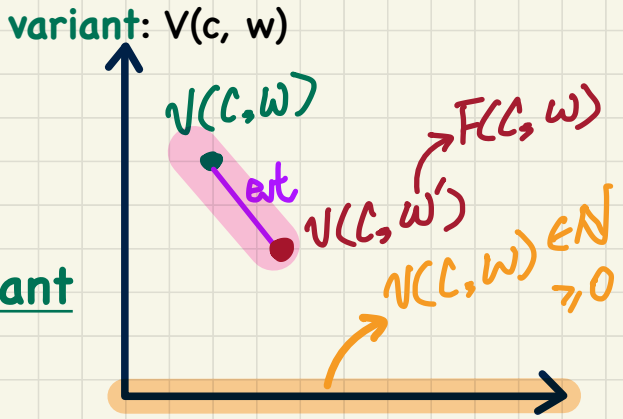
$A(c)$
$I(c, v)$
$J(c, v, w)$
$H(c, w)$
$\vdash$
$V(c, w) \in \mathbb{N}$

NAT

IL_in/NAT

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

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



A New Event Occurrence Decreases Variant

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

evt
effect of evt
pre-state
post-state

VAR

IL_in/VAR

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

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

$V(c, w) = 2 \cdot a + b$

$V(c, w') = 2 \cdot a' + b' = 2 \cdot (a-1) + (b+1) <$

Lecture 2

Part L

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

Idea of Relative Deadlock Freedom

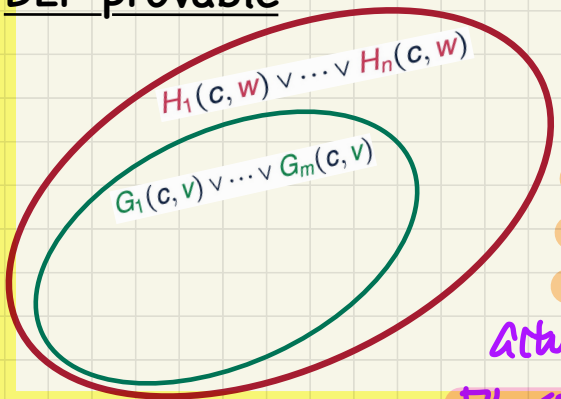
$\{x \mid P(x)\}$

$A(c)$
$I(c, v)$
$J(c, v, w)$ — stronger
$G_1(c, v) \vee \cdots \vee G_m(c, v)$
$\vdash \Rightarrow$ — weaker
$H_1(c, w) \vee \cdots \vee H_n(c, w)$

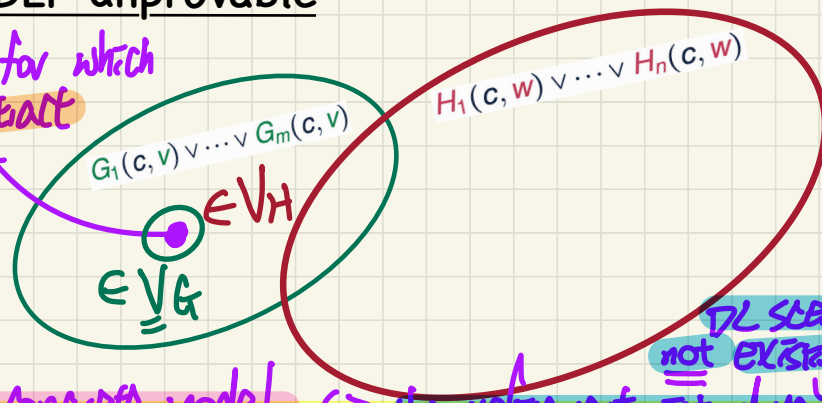
DLF

If an abstract state doesn't deadlock, then the corresponding concrete state doesn't DL.

DLF provable



DLF unprovable



a state for which the abstract model doesn't DL is actually a DL state for concrete model. (⇒ the refinement introduce a DL scenario ≡ not existing in AM.

PO of Relative Deadlock Freedom

✓Abstract m0

variables: n

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

ML_out
when $n < d$
then $n := n + 1$
end

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

Concrete 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 : $a = 0 \vee c = 0$

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

ML_in
when ② $c > 0$
then $c := c - 1$
end

IL_in
when ③ $a > 0$
then $a := a - 1$, $b := b + 1$
end

IL_out
when ④ $b > 0$, $a = 0$
then $b := b - 1$, $c := c + 1$
end

$A(c)$
$I(c, v)$
$J(c, v, w)$
$G_1(c, v) \vee \cdots \vee G_m(c, v)$
$\vdash$
$H_1(c, w) \vee \cdots \vee H_n(c, w)$

DLF

$d \in \mathbb{N}$
$d > 0$
$n \in \mathbb{N}$
$n \le d$
$a \in \mathbb{N}$
$b \in \mathbb{N}$
$c \in \mathbb{N}$
$a + b + c = n$
$a = 0 \vee c = 0$
$(n < d) \vee (n > 0)$

$\vdash$
① $(a+b) < d \wedge c = 0$
$\vee$ $c > 0$ ②
$\vee$ $a > 0$ ③
$\vee$ $(b > 0) \wedge (a = 0)$ ④

Example Inference Rules

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

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

Look up: OR_L

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

$H \Rightarrow P \vee Q$

$\equiv$ { def. of $\Rightarrow$: $x \Rightarrow y \equiv \neg x \vee y$ }

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

$\equiv$ { commutativity: $x \vee (y \vee z) \equiv (x \vee y) \vee z$ }

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

$\equiv$ { double negation: $P \equiv \neg\neg P$ }

$\neg\neg(\neg H \vee P) \vee Q$, d.n.

$\equiv$ { de morgan: $\neg(x \vee y) \equiv \neg x \wedge \neg y$ }

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

$\equiv$ { def. of $\Rightarrow$ }

$H \wedge \neg P \Rightarrow Q$

Discharging POs of m1: Relative Deadlock Freedom

Part 1

Exercise.

$$\frac{H1 \vdash G}{H1, H2 \vdash G}\ \text{MON} \qquad \frac{H(F), E = F \vdash P(F)}{H(E), E = F \vdash P(E)}\ \text{EQ\_LR} \qquad \frac{H, \neg P \vdash Q}{H \vdash P \vee Q}\ \text{OR\_R}$$

$$\begin{array}{l} d \in \mathbb{N} \\ d > 0 \\ n \in \mathbb{N} \\ n \leq d \\ a \in \mathbb{N} \\ b \in \mathbb{N} \\ c \in \mathbb{N} \\ a + b + c = n \\ a = 0 \vee c = 0 \\ n < d \vee n > 0 \\ \vdash \\ \quad a + b < d \wedge c = 0 \\ \vee \quad c > 0 \\ \vee \quad a > 0 \\ \vee \quad b > 0 \wedge a = 0 \end{array}$$

$$\begin{array}{l} d > 0 \\ b = 0 \vee b > 0 \\ \vdash \\ \quad b < d \wedge 0 = 0 \\ \vee \quad b > 0 \wedge 0 = 0 \end{array}$$

Discharging POs of m1: Relative Deadlock Freedom

Part 2

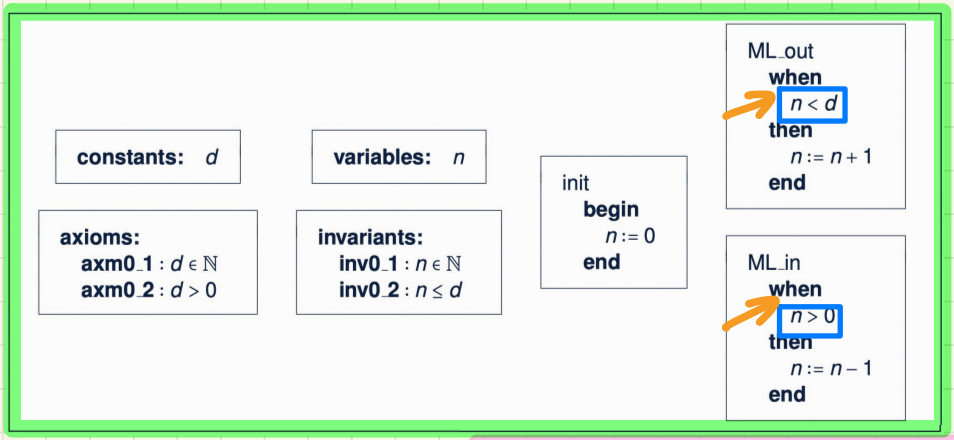
Exercise .

$$\frac{H, P \vdash R \qquad H, Q \vdash R}{H, P \lor Q \vdash R}\ \text{OR\_L} \qquad \frac{H \vdash P}{H \vdash P \lor Q}\ \text{OR\_R1} \qquad \frac{}{P \vdash E = E}\ \text{EQ}$$

$$\frac{H \vdash P \qquad H \vdash Q}{H \vdash P \land Q}\ \text{AND\_R} \qquad \frac{H \vdash Q}{H \vdash P \lor Q}\ \text{OR\_R2} \qquad \frac{}{H, P \vdash P}\ \text{HYP}$$

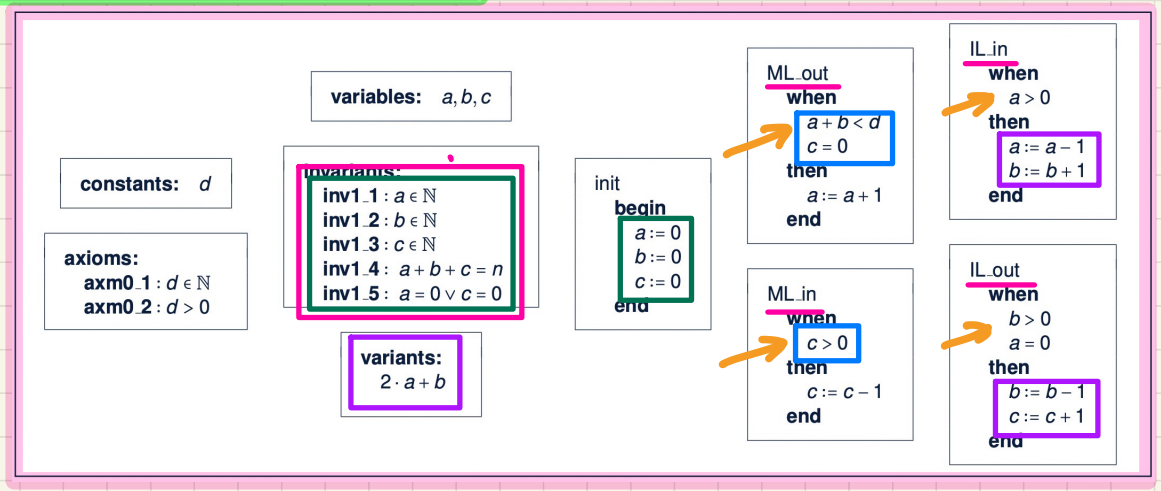
$$\begin{array}{l} d > 0 \\ b = 0 \lor b > 0 \\ \vdash \\ \qquad b < d \land 0 = 0 \\ \lor \quad b > 0 \land 0 = 0 \end{array}$$

Initial Model and 1st Refinement: Provably Correct



Abstract m0

Concrete m1



Correctness Criteria:

+ Guard Strengthening
+ Invariant Establishment
+ Invariant Preservation
+ Convergence
+ Relative Deadlock Freedom