Lecture 2

Part F

Case Study on Reactive Systems - Bridge Controller
First Refinement: State and Events (continued)

Bridge Controller: State Space of the 1st Refinement

REQ1	The system is controlling cars on a bridge connecting the mainland to an island.
REQ3	The bridge is one-way or the other, not both at the same time.

Dynamic Part of Model

Counter example to violate this safety inv.

unsafe

$a = 2$
$c = 1$
$b = ?$

crash

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 : ?? $n = a + b + c$
- inv1_5 : ??

abstract state

concrete state

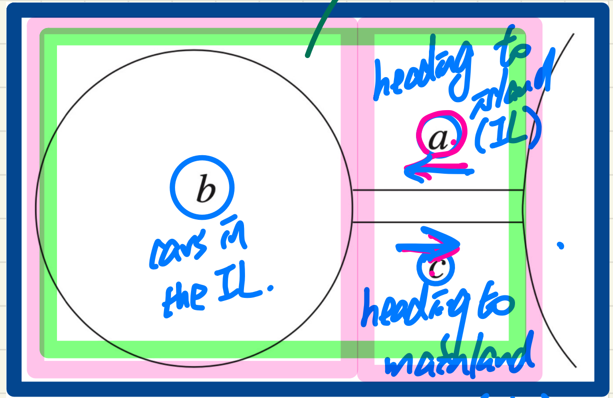
need inv1_5 to disallow.

1st refinement m1

$c = 0 \lor a = 0$

flow to IL   flow to ML

n : IB compound



Static Part of Model

constants: d

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

Exercises

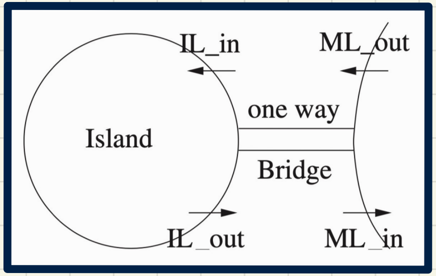
n a, b, c

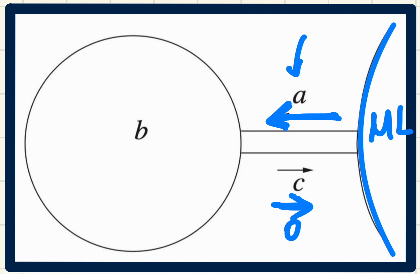
inv1_4: linking abstract & concrete states

inv1_5: bridge is one-way

safety invariant

Bridge Controller: Guards of "old" Events 1st Refinement





constants: d

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

variables: a, b, c

invariants: ② $n \leq d$
- inv1_1 : $a \in \mathbb{N}$
- inv1_2 : $b \in \mathbb{N}$
- inv1_3 : $c \in \mathbb{N}$ ①
- inv1_4 : $a + b + c = n$
- inv1_5 : $a = 0 \lor c = 0$

ML_out: A car exits **mainland** (getting on the **bridge**).

```
ML_out
  when
    ??
  then
    a := a + 1
  end
```

abstract: BAP: $n' = n + 1$

BAP: $a' = a + 1$, $b' = b$, $c' = c$

$a + b = n < d$

G1 : $c = 0$

G2 : $a + b < d$

Post-state:
- $n' \leq d$
- $a' + b' + c' = n'$
- $c = 0$

$n + 1 \leq d$

$(a+1) + b + 0 = n + 1$

$n < d$

ML_in: A car enters **mainland** (getting off the **bridge**).

```
ML_in
  when
    ??
  then
    c := c - 1
  end
```

G1 : $c > 0$

$n \leq d$ not relevant

unnecessary: $a = 0$

$\Rightarrow a = 0$

inv1_5 : $a = 0 \lor c = 0$
G1 : $c > 0$

Bridge Controller: Abstract vs. Concrete State Transitions

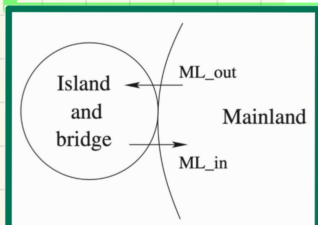
Abstract m0

variables: n

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

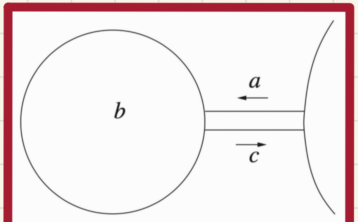
ML_out
when
$n < d$
then
$n := n + 1$
end

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



Concrete m1

invariants involving both abs. & con. variables

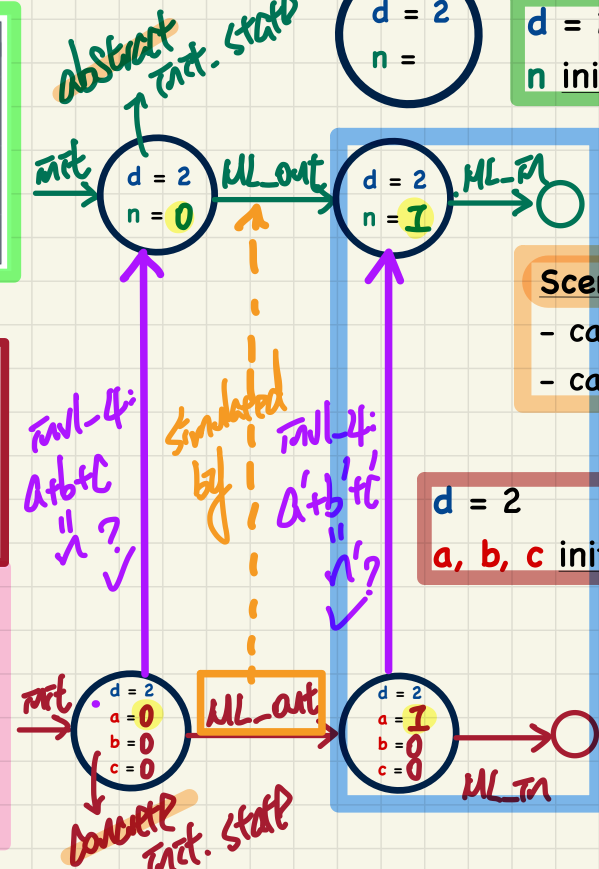


variables: a, b, c

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
$a := a + 1$
end

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



d = 2
n =

d = 2
n initialized to 0

Exercise.

Scenario
- car leaving ML
- car entering ML

d = 2
a, b, c initialized to 0

d = 2
a =
b =
c =

Before-After Predicates of Event Actions: 1st Refinement

Events	ML_in **when** $0 < c$ **then** $c := c - 1$ **end**	ML_out **when** $a + b < d$ $c = 0$ **then** $a := a + 1$ **end**
Before–after predicates	$a' = a \;\wedge\; b' = b \;\wedge$ $c' = c - 1$	$a' = a + 1 \;\wedge\; b' = b \;\wedge$ $c' = c$

actions

post-state value

becomes

evaluation of pre-state value

as if: $a := a$ $b := b$

- Pre-State
- Post-State
- Sate Transition

States, Invariants, Events: Abstract vs. Concrete

abs. variables (abstract state)

abstract version

Abstract m0

variables: n

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

abs. invariants (involving abs. state only)

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

abs. state

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

constants: d

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

Concrete m1

concrete version

variables: a, b, c

concrete variables (concrete state)

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** : $a = 0 \lor c = 0$

special kind of con. inv. involving both state spaces

concrete invariants (involving at least con. vars.)

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

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

con. state

PO Rule of Invariant Preservation in Refinement: Components

Abstract m0

abs. guards

variables: n

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

$\to v$

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

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

Concrete m1

concrete guards

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 : $a = 0 \lor c = 0$

$\to w$

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

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

v and v′: **abstract** variables in pre-/post-states

w and w′: **concrete** variables in pre-/post-states

G(c, v): an **abstract** event's guards

H(c, w): a **concrete** event's guards

I(c, v): list of **abstract invariants**

J(c, v, w): list of **concrete invariants**

abs. variables

concrete vars.

E(c, v): an **abstract** event's effect

F(c, w): a **concrete** event's effect

E(c, v) of ML_out: <n+1>

F(c, w) of ML_out: <a+1, b, c>

Lecture 2

Part G

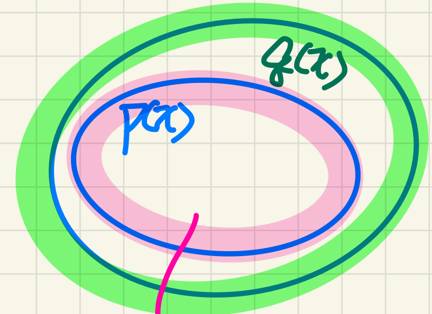
Case Study on Reactive Systems -
Bridge Controller
First Refinement: Guard Strengthening

satisfying values

$$P \Rightarrow q \qquad \{x \mid P(x)\} \subseteq \{x \mid q(x)\}$$

"P is stronger than q"

"q is weaker than P"



satisfying values of a stronger predicate

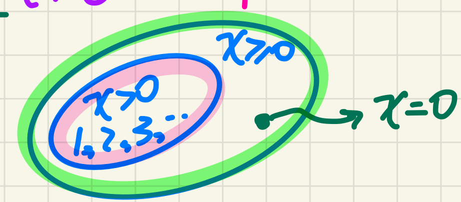
$x > 0$

$x \geq 0$

$x > 0$ is stronger than $x \geq 0$

$x \geq 0$ is weaker than $x > 0$

$$\boxed{x > 0 \Rightarrow x \geq 0}$$



PO/VC Rule of Guard Strengthening: Sequents

Abstract m0

variables: n

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

ML_out ✓
when
$\boxed{n < d}$ ✓
then
$n := n + 1$
end

ML_in
when
$\boxed{n > 0}$
then
$n := n - 1$
end

$$
\begin{array}{l}
A(c) \\
I(c, v) \\
J(c, v, w) \\
H(c, w) \\
\vdash \\
G_i(c, v)
\end{array}
$$

event-independent

abs. inv.

con. inv.

con. guard

single cond.

abs. guard

depends on event under consideration

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

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

2

abstract guard conditions

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

$d \in \mathbb{N}$	axm0_1
$d > 0$	axm0_2
$n \in \mathbb{N}$	inv0_1
$n \leq d$	inv0_2
$a \in \mathbb{N}$	inv1_1
$b \in \mathbb{N}$	inv1_2
$c \in \mathbb{N}$	inv1_3
$a+b+c=n$	inv1_4
$a=0 \vee c=0$	inv1_5

$\left.\begin{array}{l} a+b<d \\ c=0 \end{array}\right\}$ concrete grds of ML_out

ML_out/GRD

$\vdash \boxed{n<d}$ abstract guard of ML_out

Exercise
Formulate ML_in/GRD

Discharging POs of m1: Guard Strengthening in Refinement

ML_out/GRD

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

when applying MON IR, guide yourself by the goal to see which hypotheses to drop.

$$\frac{H1 \;\vdash\; G}{H1, H2 \;\vdash\; G}\ \textbf{MON}$$

$$\frac{}{H, P \;\vdash\; P}\ \textbf{HYP}$$

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

$\xrightarrow{\text{MON}}$

$a+b+c=n$
$a+b<d$
$c=0$
$\vdash$
$n<d$

$\xrightarrow{\text{EQ\_LR}}$

$a+b+0=n$
$a+b<d$
$c=0$
$\vdash$
$n<d$

$\xrightarrow{\text{MON}}$

$a+b+0=n$
$a+b<d$
$\vdash$
$n<d$

$\xrightarrow{\text{ARI}}$

ARI: arithmetic (basic)

$a+b=n$
$a+b<d$
$\vdash$
$n<d$

$\xrightarrow{\text{EQ\_LR, MON}}$

$n<d$
$\vdash$
$n<d$

HYP ✓

Discharging POs of m1: Guard Strengthening in Refinement

ML_in/GRD

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

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

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

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

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

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

col. inv.

con. guard

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

$n = b + c$

0 1

0 1 1

$c > 0$

MON

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

OR_L

$b \in \mathbb{N}$, $a+b+c = n$, $a = 0$, $c > 0 \vdash n > 0$ — EQ_LR, MON — $b \in \mathbb{N}$, $0+b+c = n$, $c > 0 \vdash n > 0$ — ARI — $b \in \mathbb{N}$, $b+c = n$, $c > 0 \vdash n > 0$ — ARI — $n > 0 \vdash n > 0$ ✓ HYP

$b \in \mathbb{N}$, $a+b+c = n$, $c = 0$, $c > 0 \vdash n > 0$ — EQ_LR, MON — $0 > 0 \vdash n > 0$ — ARI — $\bot \vdash n > 0$ ✓ FALSE_L

Lecture 2

Part H

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

PO/VC Rule of Invariant Preservation: Sequents

Abstract m0

variables: n

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

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

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

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

a single concrete inv. cond.

Effect of abs. vars.

Effect of con. vars.

Concrete m1

* $\cancel{a'} + \cancel{b'} + \cancel{c'} = n'$
$(a+1) + b + c = n+1$

** $\cancel{a'} = 0 \lor \cancel{c'} = 0$
a $(c-1)$

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
$\boxed{a + b < d \quad c = 0}$
then
$a := a + 1$
end
BAP: $a' = a+1 \land b' = b. \land c' = c.$

ML_in
when
$\boxed{c > 0}$
then
$c := c - 1$
end
BAP: $c' = c-1 \land a' = a \land b' = b$

$2 * 5 = 10$

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

ML_out/inv1_4/INV

$d \in \mathbb{N}$	axm0_1
$d > 0$	axm0_2
$n \in \mathbb{N}$	inv0_1
$n \leq d$	inv0_2
$a \in \mathbb{N}$	inv1_1
$b \in \mathbb{N}$	inv1_2
$c \in \mathbb{N}$	inv1_3
$a+b+c=n$	inv1_4
$a=0 \lor c=0$	inv1_5
$a+b<d$	
$c=0$	

$\vdash$ ✓ *
$\boxed{(a+1)+b+c=n+1}$

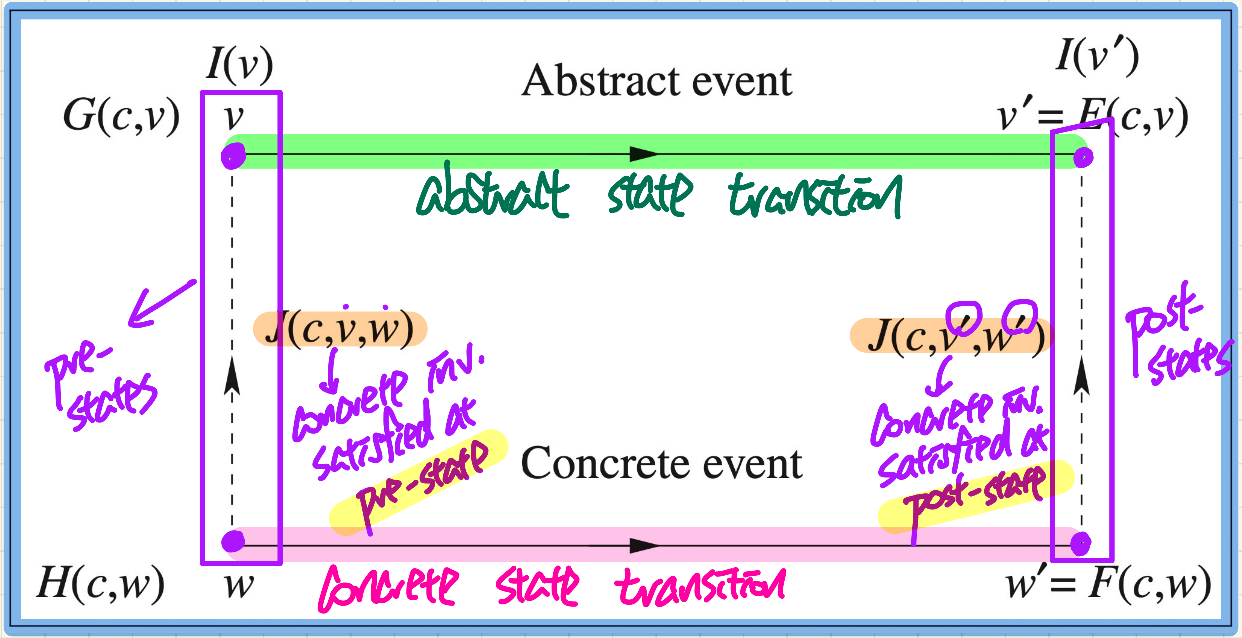
ML_in/inv1_5/INV

$d \in \mathbb{N}$	axm0_1
$d > 0$	axm0_2
$n \in \mathbb{N}$	inv0_1
$n \leq d$	inv0_2
$a \in \mathbb{N}$	inv1_1
$b \in \mathbb{N}$	inv1_2
$c \in \mathbb{N}$	inv1_3
$a+b+c=n$	inv1_4
$a=0 \lor c=0$	inv1_5
$c>0$	

$\vdash$ **
$\boxed{a=0 \lor (c-1)=0}$

Visualizing Invariant Preservation in Refinement

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



Discharging POs of m1: Invariant Preservation in Refinement

ML_out/inv1_4/INV

Exercise

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

$$\frac{}{P \vdash E = E}\ \textbf{EQ}$$

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

$$
\begin{array}{l}
d \in \mathbb{N} \\
d > 0 \\
n \in \mathbb{N} \\
n \leq d \\
a \in \mathbb{N} \\
b \in \mathbb{N} \\
c \in \mathbb{N} \\
a + b + c = n \\
a = 0 \lor c = 0 \\
a + b < d \\
c = 0 \\
\vdash \\
(a + 1) + b + c = (n + 1)
\end{array}
$$

Discharging POs of m1: Invariant Preservation in Refinement

ML_in/inv1_5/INV

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

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

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

$$\frac{H \vdash P}{H \vdash P \lor Q}\ \textbf{OR\_R1}$$

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

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

$$\frac{H, P \vdash R \qquad H, Q \vdash R}{H, P \lor Q \vdash R}\ \textbf{OR\_L}$$

Exercise

Lecture 2

Part I

Case Study on Reactive Systems - Bridge Controller First Refinement: Inv. Establishment

PO of Invariant Establishment in Refinement

constants: d

axioms:
- $\boxed{\textbf{axm0\_1}: d \in \mathbb{N}}$
- $\boxed{\textbf{axm0\_2}: d > 0}$

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** : $a = 0 \lor c = 0$

init
  begin
    $a := 0$
    $b := 0$
    $c := 0$
  end

BAP: $a' = 0$, $b' = 0$, $c' = 0$

Components

K(c): effect of abstract init

L(c): effect of concrete init

$* \; \cancel{a'}_{0} + \cancel{b'}_{0} + \cancel{c'}_{0} = \cancel{n'} \, 0$

$** \; \cancel{a'}_{0} = 0 \lor \cancel{c'}_{0} = 0$

Rule of Invariant Establishment

$$\frac{A(c)}{\vdash} \quad \text{Post-state con. inv.}$$

$$J_i(c, K(c), L(c))$$

con. inv. cond. 5

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

Exercise:

Generate Sequents from the INV rule.

init/inv1_4/INV

$d \in \mathbb{N}$
$d > 0$
$\vdash *$
$\boxed{0 + 0 + 0 = 0}$

init/inv1_5/INV

$d \in \mathbb{N}$
$d > 0$
$\vdash **$
$\boxed{0 = 0 \lor 0 = 0}$

Discharging PO of Invariant Establishment in Refinement

Exercises

$$\begin{array}{l} d \in \mathbb{N} \\ d > 0 \\ \vdash \\ 0 + 0 + 0 = 0 \end{array}$$

init/**inv1_4**/INV

$$\begin{array}{l} d \in \mathbb{N} \\ d > 0 \\ \vdash \\ 0 = 0 \lor 0 = 0 \end{array}$$

init/**inv1_5**/INV

$$\frac{H1 \;\vdash\; G}{H1, H2 \;\vdash\; G} \quad \textbf{MON}$$

$$\frac{}{P \;\vdash\; \top} \quad \textbf{TRUE\_R}$$