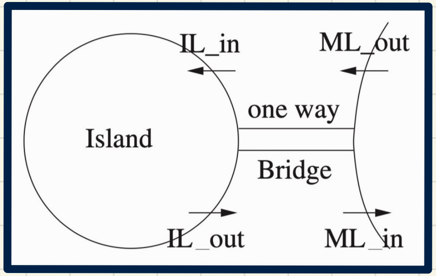
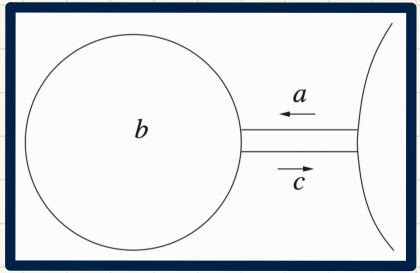
Bridge Controller: Guards of "old" Events 1st Refinement





constants: d

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

variables: a, b, c

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

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

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

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

Bridge Controller: Abstract vs. Concrete State Transitions

Abstract m0

variables: n

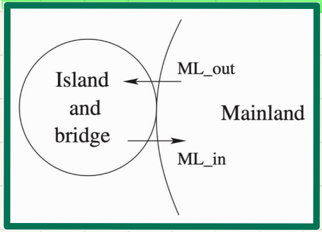
invariants:
- **inv0_1** : $n \in \mathbb{N}$
- **inv0_2** : $n \leq d$

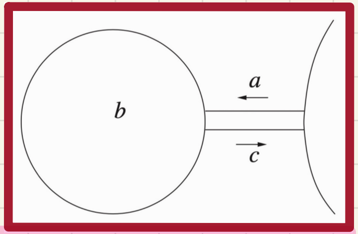
ML_out
  when
    $n < d$
  then
    $n := n + 1$
  end

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

d = 2
n =

d = 2
n initialized to 0





Scenario
- car leaving ML
- car entering ML

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

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

d = 2
a, b, c initialized to 0

d = 2
a =
b =
c =

Before-After Predicates of Event Actions: 1st Refinement

	ML_in	ML_out
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	$a' = a \ \wedge \ b' = b \ \wedge$ $c' = c - 1$	$a' = a + 1 \ \wedge \ b' = b \ \wedge$ $c' = c$

- Pre-State
- Post-State
- Sate Transition

States, Invariants, Events: Abstract vs. Concrete

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

constants: d

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

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

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

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

PO Rule of Invariant Preservation in Refinement: Components

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

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

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

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

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

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

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

$$A(c)$$
$$I(c, v)$$
$$J(c, v, w)$$
$$H(c, w)$$
$$\vdash$$
$$G_i(c, v)$$

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 : $a = 0 \lor c = 0$

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

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

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

Discharging POs of m1: Guard Strengthening in Refinement

ML_out/GRD

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

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

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

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

Discharging POs of m1: Guard Strengthening in Refinement

ML_in/GRD

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

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

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

$$\frac{}{\perp \vdash P} \quad \textbf{FALSE\_L}$$

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

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