Lecture 15 - March 14

Reactive System: Bridge Controller

Announcements

- ProgTest1 result to be released by Friday
- Lab~~2~~3 to be released by the end of Thursday
- ✓ To be completed by the final exam:

  Makeup lectures for WT1, WT2, ProgTest1, ProgTest2

Before-After Predicates of Event Actions: 1st Refinement

Concrete events

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

Concrete guards

Concrete Actions

b, c absent

↳ stay unchanged

- Pre-State
- Post-State
- Sate Transition

Consider an exec: < init, ML_out, ML_in >

Bridge Controller: Abstract vs. Concrete State Transitions

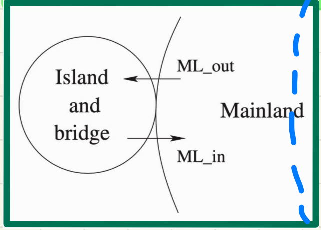
Abstract m0

variables: n

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

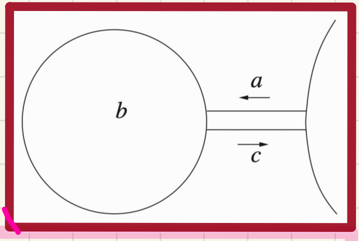
```
ML_out
  when
    $n < d$
  then
    $n := n + 1$
  end
```

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



?

?



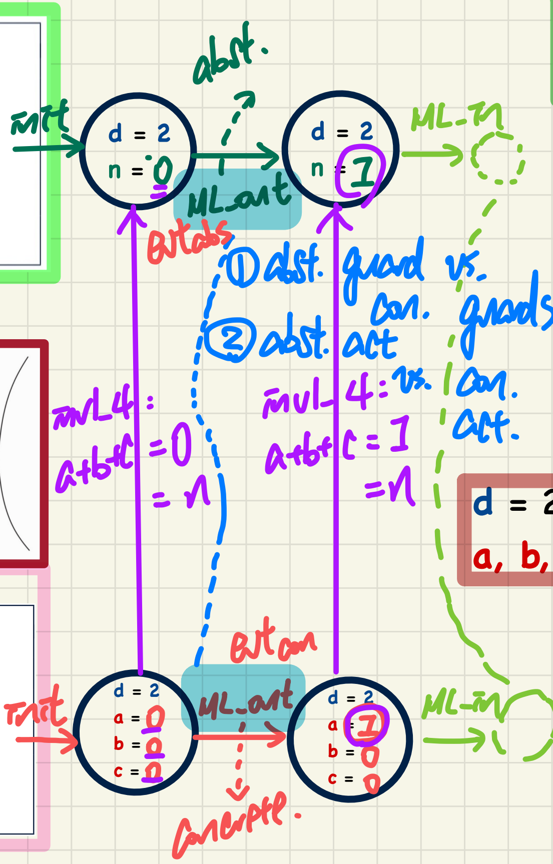
Concrete m1

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
```



① abst. guard vs. con. guards

② abst. act vs. con. act.

d = 2
n initialized to 0

Scenario
- car leaving ML
- car entering ML

d = 2
a, b, c initialized to 0

evt_con is simulated by evt_abs

PO Rule of Invariant Preservation in Refinement: Components

Abstract m0

v
v' → n'

```
variables: n
```

```
invariants:
  inv0_1 : n ∈ ℕ
  inv0_2 : n ≤ d
```

abs. inv.

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

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

abs. effect

G(<d>, <n>) of ML_out: $n<d$

Concrete m1

w: <a, b, c>
w': <a', b', c'>

```
variables: a, b, c
```

```
invariants:
  inv1_1 : a ∈ ℕ
  inv1_2 : b ∈ ℕ
  inv1_3 : c ∈ ℕ
  inv1_4 : a + b + c = n
  inv1_5 : a = 0 ∨ c = 0
```

con. inv.

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

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

con. effect

H(<d>, <a, b, c>): $a+b<d \land c=0$

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

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

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

Lecture

Reactive System: Bridge Controller

First Refinement: Guard Strengthening

$P \Rightarrow q$

↳ "p is stronger than q"

↳ "q is weaker than p"

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

$q(x) = \{x \mid q(x)\}$

sets of satisfying values

① → $q(x) \subseteq P(x)$?

② $p(x) = q(x)$

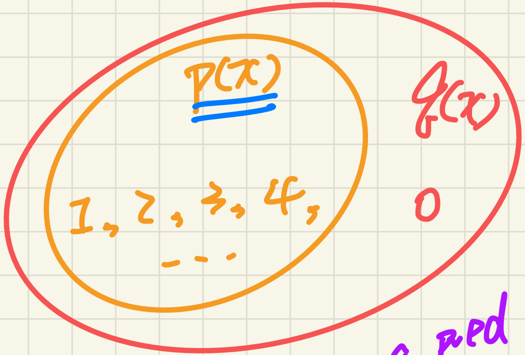
③ $\boxed{p(x) \subseteq q(x)}$? *

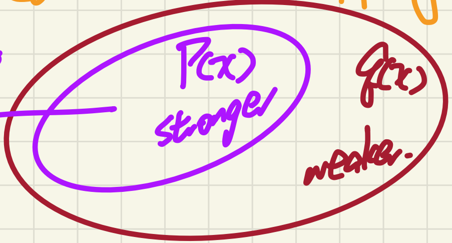
④ non-overlapping.

$P(x) = x > 0$

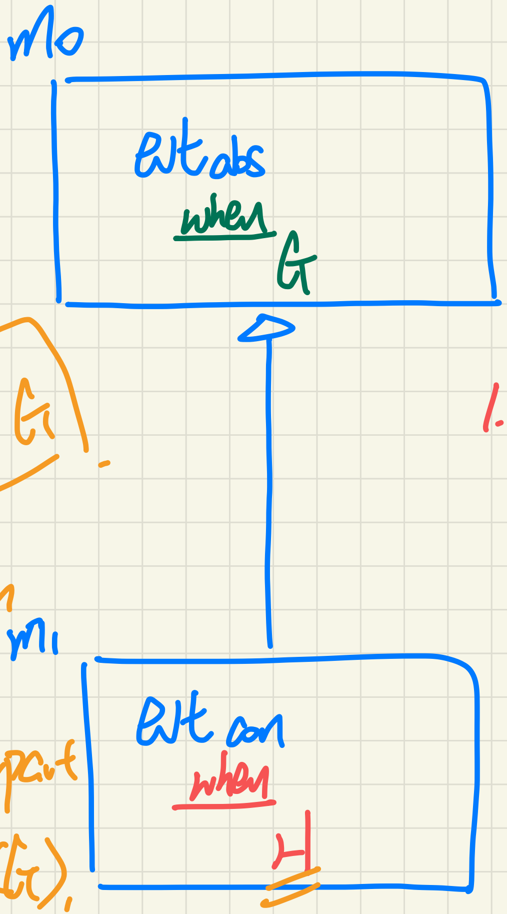
$q(x) = x \geq 0$

$P(x) \Rightarrow q(x)$ ✓





the stronger a pred is, the more values it filters out



$H \Rightarrow G$

① If a conc. transition is enabled (H), then its abs. counterpart is also enabled (G).

② $\neg G \Rightarrow \neg H$

What's not allowed in the abs. transition is also not allowed for con. transition. (In the con. model, no new behaviour is created)

1. When a refinement is created, guards of each event can only be strengthened/stronger

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
```

$A(c)$ axioms
$I(c, v)$ abs. invariants
$J(c, v, w)$ con. invariants
$H(c, w)$ → concrete guard
$\vdash$ ..
$G_i(c, v)$ → abstract guard

i → index of abs. guard.

Concrete m1

Exercise: Formulat guard strengthening PO of ML_in.

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
```

ML_in/GRD

ML_out/GRD

$$
\begin{array}{ll}
d \in \mathbb{N} & axm0\_1 \\
d > 0 & axm0\_2 \\
n \in \mathbb{N} & inv0\_1 \\
n \leq d & inv0\_2 \\
a \in \mathbb{N} & a+b+c=n \\
b \in \mathbb{N} & a=0 \lor c=0 \\
c \in \mathbb{N} & a+b<d \\
 & c=0
\end{array}
\vdash n < d
$$

] con. guards of ML_out

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

→ 2 (# abs. guards)

Discharging POs of m1: Guard Strengthening in Refinement

ML_out/GRD

axioms

$d \in \mathbb{N}$

$d > 0$

abs. I

$n \in \mathbb{N}$

$n \leq d$

con. I.

$a \in \mathbb{N}$

$b \in \mathbb{N}$

$c \in \mathbb{N}$

$a + b + c = n$

$a = 0 \lor c = 0$

con. gu. of ML_out

$a + b < d$

$c = 0$

$\vdash$

abs. gu. of ML_out

$n < d$

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

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

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

MON

$a+b+c=n$

$a+b<d$

$c=0$

$\vdash$

$n<d$

EQ_LR

$a+b+0=n$

$a+b<d$

$c=0$

$\vdash$

$n<d$

MON

$a+b+0=n$

$a+b<d$

$\vdash$

$n<d$

ARI

$a+b=n$

$a+b<d$

$\vdash$

$n<d$

EQ_LR, MON

$n<d$

$\vdash$

$n<d$

HYP

Discharging POs of m1: Guard Strengthening in Refinement

ML_in/GRD

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

con. guard of ML_in

abs. guard of ML_in

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

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

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

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

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