Lecture 12 - Oct. 22

Bridge Controller

Event Action vs. Before-After Predicate

Before- vs. After-States

Sequents: Syntax and Semantics

Announcements/Reminders

- ProgTest1 results to be released around next Monday.
- WrittenTest1 tomorrow during your enrolled lab session
- Lab4 released (ProgTest2 on November 6)
  - + Try to complete Part 1 by Friday.
  - + Follow the proof steps in Part 2 & collect questions.
  - + Scheduled lab session on October 30.

Before-After Predicates of Event Actions

Events	ML_out $n := n + 1$	ML_in $n := n - 1$
before–after predicates	$n' = n + 1$	$n' = n - 1$

for Rodin

pre-state value +1

post-state value n

becomes

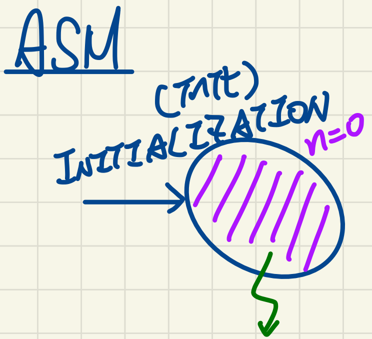
for reasoning

post

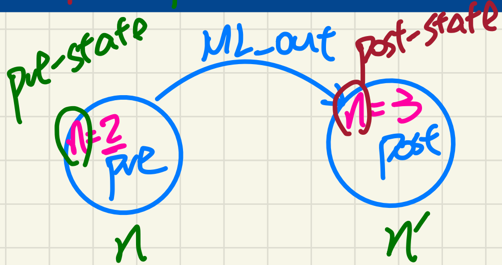
pre

- Pre-State
- Post-State
- Sate Transition

P.O.



Invariant must be established



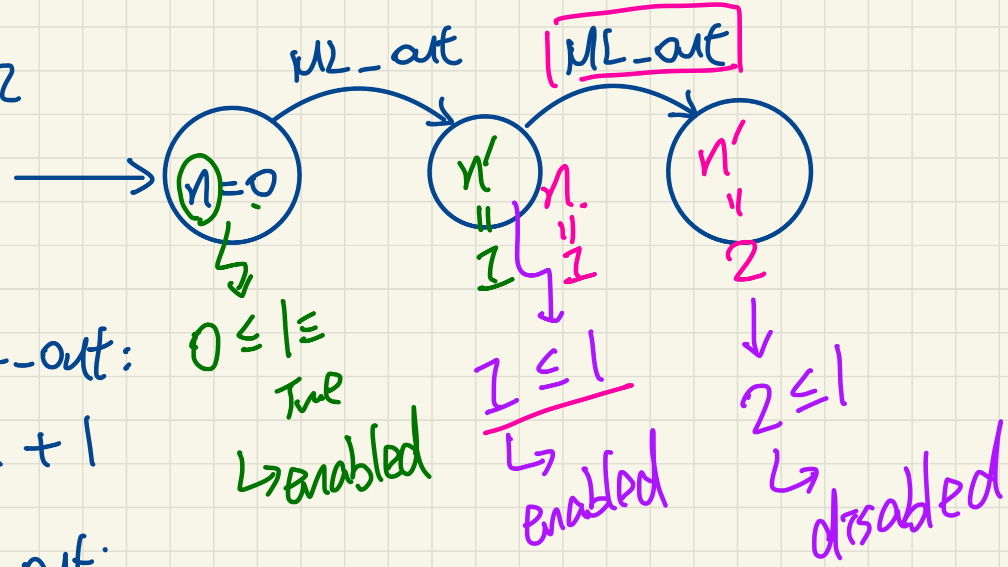
For each variable x:

(1) Write x to denote its pre-state value.

(2) Write x' to denote its post-state value.

$\langle init, ML\_out, ML\_out \rangle$

d=2



action for ML_out:

$n := n + 1$

guard for ML_out:

~~true~~ say: $n \leq 1$

(~~always enabled~~)

Transition of an Event

$b \in Account \nrightarrow \mathbb{N}$

Pre-State:

I

Post-State:

$\boxed{I}$ remains to be true

$\forall a \cdot a \in dom(\boxed{b})$
$\Rightarrow$
$\boxed{b}(a) \geq -C$

withdraw

$a : Account$

$v : \mathbb{N}$

where

$a \in dom(b)$

1. guard of withdraw

2. I must be true

enabling condition of event

begin

* effect of event action.

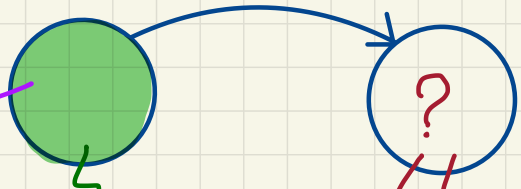
$b := \boxed{b \mathbin{\lhd\!\!+} \{a \mapsto b(a) - v\}}$

*

end

$I: \forall a \cdot a \in dom(b) \Rightarrow b(a) \geq -C$

withdraw (must be enabled to occur).



pre-state

post-state

Is the post-state, after the event's action takes effect, still safe?

Is I maintained?

Invariant I in pre-state:

$$\forall x \cdot x \in dom(\underline{b}) \Rightarrow x \geq -C$$

event action

$$b := \boxed{b \mathbin{<\!\!+} \{a \mapsto b(a) - v\}}$$

I in post-state:

$$\forall x \cdot x \in dom(\underbrace{b \mathbin{<\!\!+} \{a \mapsto b(a) - v\}}_{\text{new value of } b \text{ in post-state of withdraw.}}) \Rightarrow x \geq -C$$

Exercise: Event Actions vs. Before-After Predicates

Q. Are the following event actions suitable for a swap between x and y?

```
swap
  begin
    temp := x
    x := y
    y := temp
  end
```

Inappropriate

↳ := should not be considered as seq. assignment

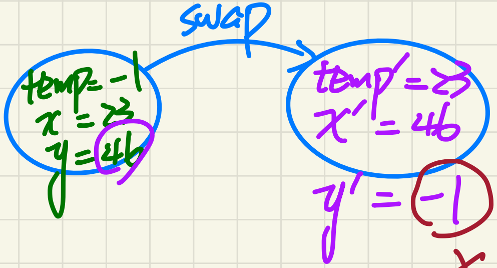
BAP:

$temp' = x$ ✓

$\wedge\ x' = y$

$\wedge\ y' = temp$

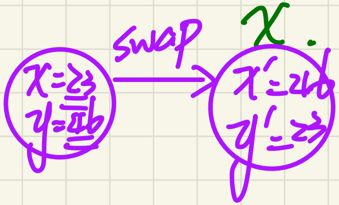
↓ pre-state value, which has no connection to



Correct: $x := y$
$y := x$

BAP:

$\left(x' = y \wedge y' = x \right.$



Design of Events: Invariant Preservation

to be formulated as a proof obligation

variables: n

```
ML_out
  begin
    n := n + 1
  end
```

```
ML_in
  begin
    n := n − 1
  end
```

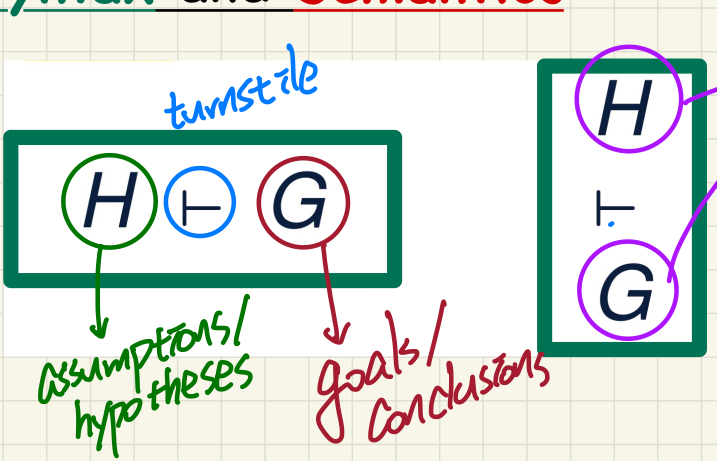
invariants:
- **inv0_1** : $n \in \mathbb{N}$
- **inv0_2** : $n \leq d$

Desire: $\forall \overset{n}{\underline{state}} \cdot state \in \overset{n \in \mathbb{N}}{\underline{StateSpace}} \Rightarrow \boxed{I(state)}$

To disprove this: find $state \in \overset{n \leq d}{StateSpace}$ but $\neg I(state)$.

Sequents: Syntax and Semantics

Syntax



each is a set of predicates

e.g.

$$d \in \mathbb{N}$$
$$n \in \mathbb{N}$$
$$n \leq d$$
$$\vdash$$
$$n+1 \leq d$$

Semantics

$H \vdash G \iff H \Rightarrow G$

predicate

↳ assuming that H is true, G is provable.

Q. What does it mean when **H** is empty/absent?

$\vdash G$

① $\boxed{\text{True} \vdash G} \equiv \text{True} \Rightarrow G \equiv \boxed{G}$

② $\boxed{\text{False} \vdash G} \equiv \text{False} \Rightarrow G \equiv \boxed{\text{True}}$ ⇝ nothing to prove!

PO/VC Rule of Invariant Preservation

Exercise ML_in/INV

constants: d

variables: n

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

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

ML_out True
begin
$n := n + 1$
end $n' = n+1$

ML_in
begin
$n := n - 1$
end

$* \; n+1 \in \mathbb{N}$
$\land$
$n+1 \leq d$

$d \in \mathbb{N}$
$n \in \mathbb{N}$
$n \leq d$
true
$\vdash$
$n+1 \in \mathbb{N}$
$n+1 \leq d$

Axioms
Invariants Satisfied at ***Pre-State***
Guards of the Event
$\vdash$
Invariants Satisfied at ***Post-State***

INV

name of Proof obligation

✓ ML_out/INV

$d \in \mathbb{N}$
$n \in \mathbb{N}$ pre-state
true $n \leq d$
$\vdash$ post-state
$* \; n' \in \mathbb{N} \land n' \leq d$