

Lecture 17 - Nov 6

Bridge Controller

***Concrete Guards: ML_out, ML_in
Guard Strengthening: Intuition, PO***

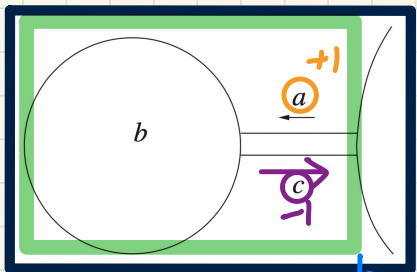
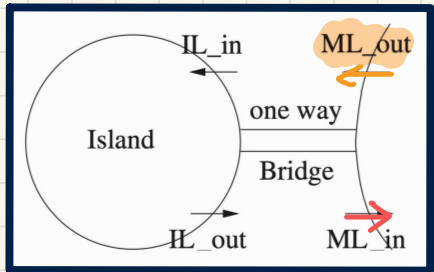
Announcements/Reminders

- Today's class: [notes template](#) posted
- **WrittenTest2** next Wednesday (November 12):
 - + **Guide** released
 - + **Practice Questions** released
 - + **Lab3** solution to be release soon (for **WrittenTest2**)

* if this sequent is provable $\rightarrow a=0$ not necessary. (hmt. OR-L)

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

$n < d$



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

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

(a) From ML , observe guard of ML_out :
 $n < d$
(b) linking ML :
 $a + b + c = n$
(c) concrete $guard$:
 $c = 0$

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 : $a = 0 \vee c = 0$

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

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

Q. Is it necessary to add a guard:
 $d = 0$?
 $c > 0$ /* guard */
 $a = 0 \vee c = 0$ /* inv1-5 */
 $a = 0$

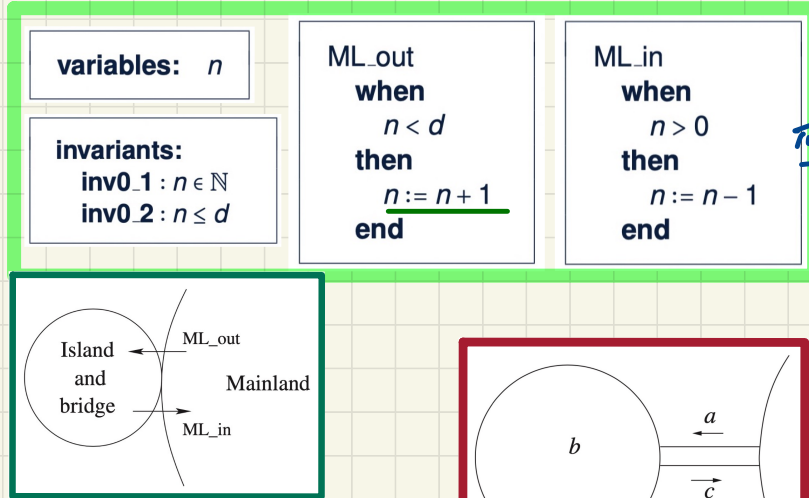
m_0

m_1

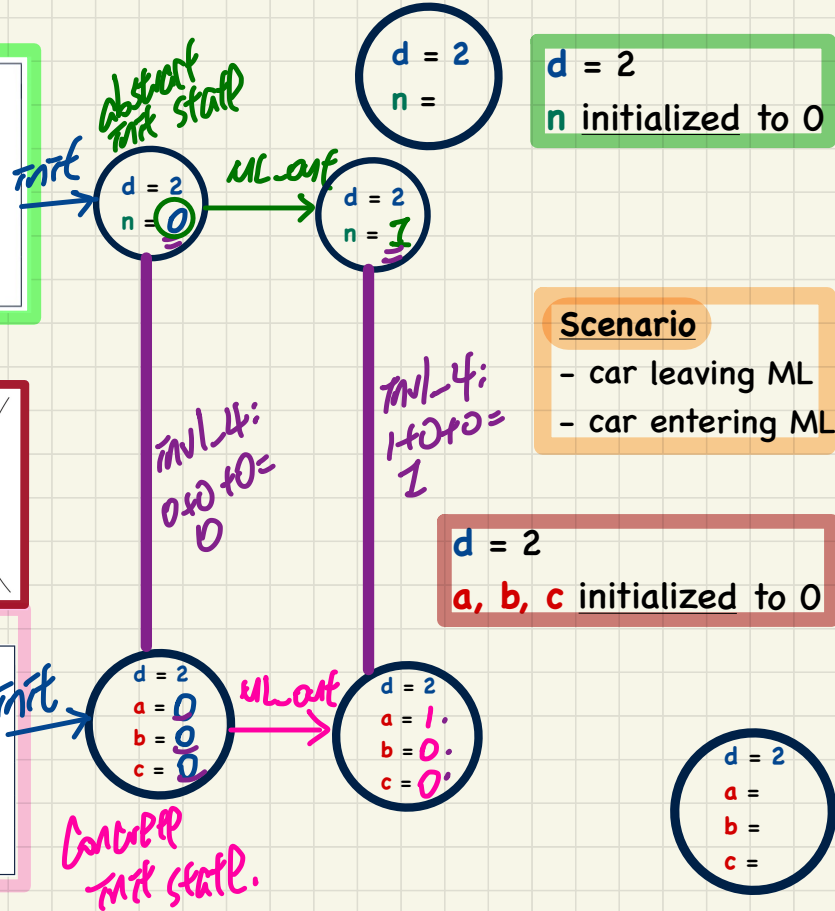
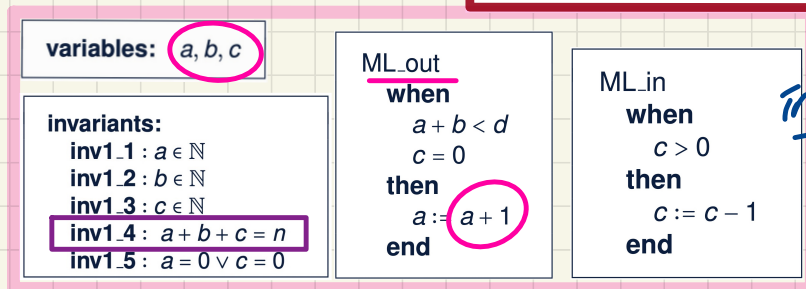
Trace: $\langle \text{init}, \text{ML_out}, \text{ML_in} \rangle$

Bridge Controller: Abstract vs. Concrete State Transitions ?

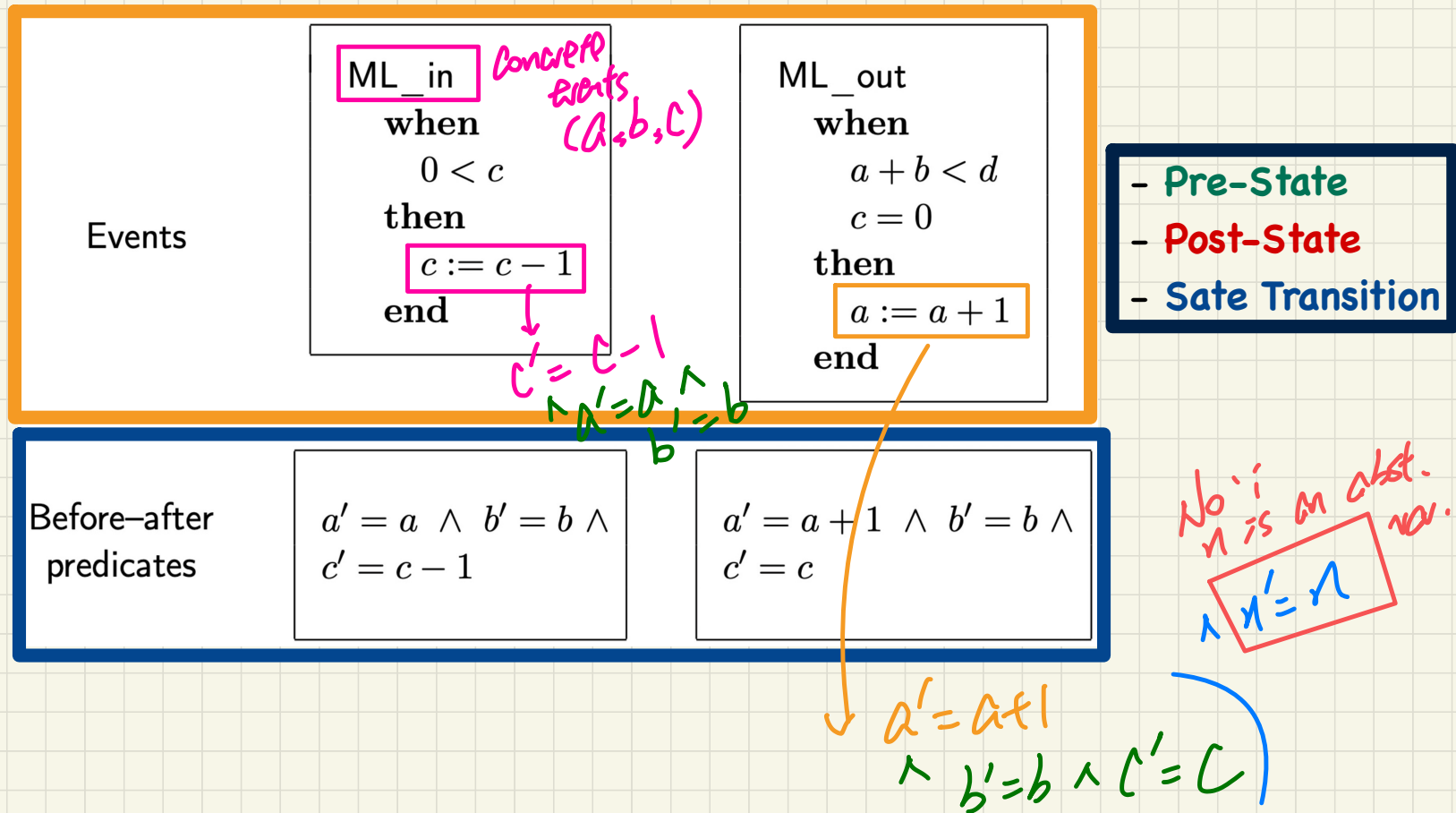
Abstract m_0



Concrete m_1



Before-After Predicates of Event Actions: 1st Refinement



States, Invariants, Events: Abstract vs. Concrete

Abstract m0

abstract var

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

abstract guard

constants: d

axioms:

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

axm0_2 : $d > 0$

Concrete m1

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

ML_out

when

$a + b < d$

$c = 0$

then

$a := a + 1$

end

ML_in

when

$c > 0$

then

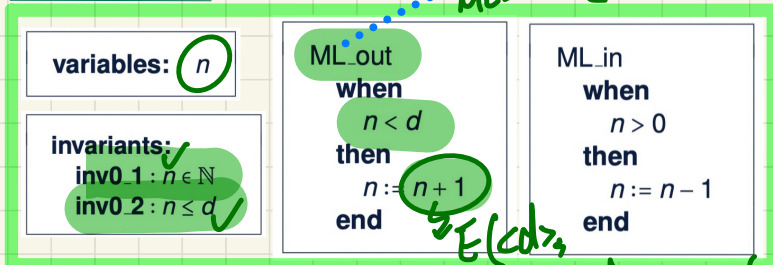
$c := c - 1$

end

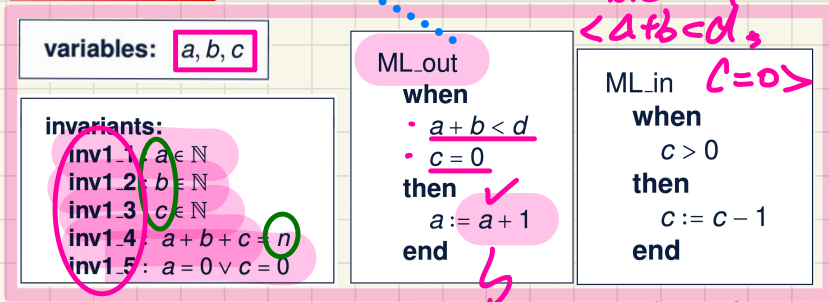
concrete guards.

PO Rule of Invariant Preservation in Refinement: Components

Abstract m0



Concrete m1



$v = \langle n \rangle$ $v' = \langle n' \rangle$ $\langle n \rangle$ of ML-out
 $w = \langle a, b, c \rangle$ $w' = \langle a', b', c' \rangle$

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
 $H(\underline{c}, \underline{w})$: a **concrete** event's guards

$I(\underline{c}, \underline{v})$: list of **abstract** invariants

$J(\underline{c}, \underline{v}, \underline{w})$: list of **concrete** invariants

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

$F(\underline{c}, \underline{w})$: a **concrete** event's effect

$I(\langle d \rangle, \langle n \rangle) = \langle \text{inv0.1}, \text{inv0.2} \rangle$

$J(\langle d \rangle, \langle n \rangle, \langle a, b, c \rangle) = \langle \text{inv1.1}, \dots, \text{inv1.5} \rangle$

Predicates: Weaker vs. Stronger

$$P \Rightarrow Q$$

↳ P is "stronger" than Q

↳ Q is "weaker" than P

Weakest predicate: True
 $\{x \mid \text{True}\}$

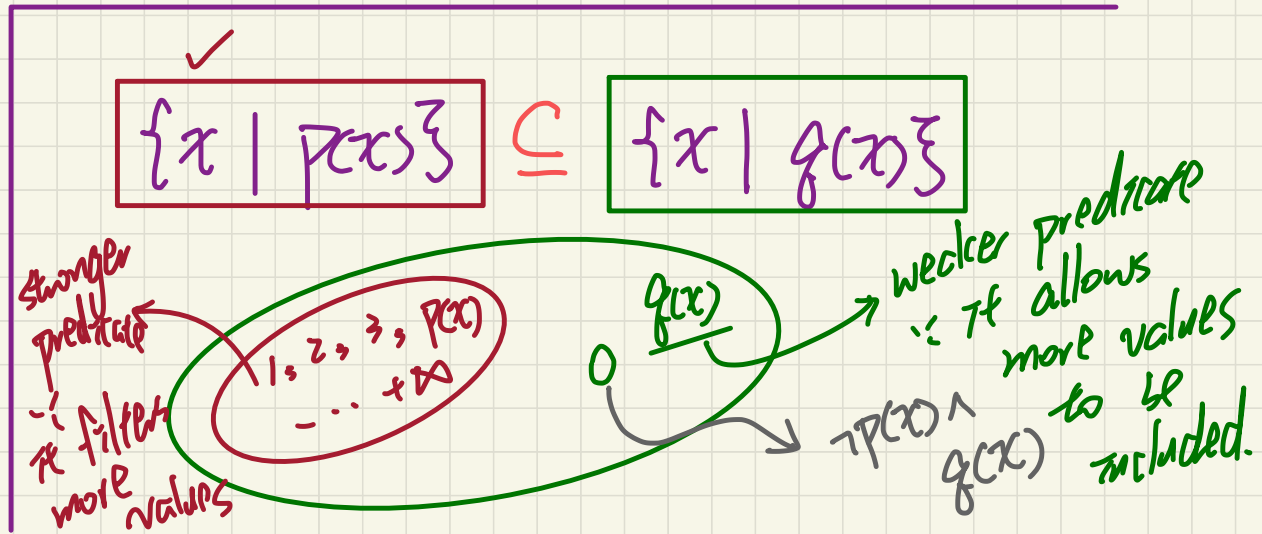
Strongest predicate: False
 $\{x \mid \text{False}\} = \emptyset$

$$p(x) \triangleq x > 0$$

$$q(x) \triangleq x \geq 0$$

$$p(x) \Rightarrow q(x) \checkmark$$

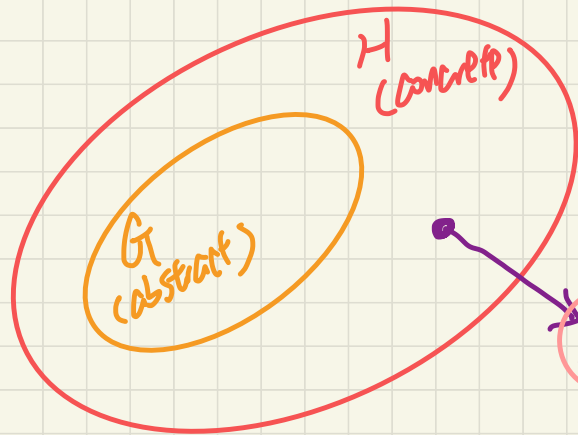
$$q(x) \Rightarrow p(x) \times$$



Refinement: Why Guard Strengthening

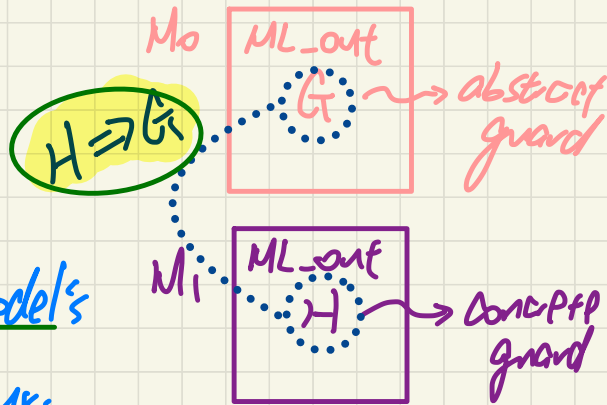
Principle: a refinement's ^{M_1} behaviour should be consistent with the abstract model's ^{M_0} behaviour.

Why is it wrong: ^{abstract} $G \Rightarrow$ ^{concrete} H



concrete event is enabled.

$\neg G \wedge H$
abstract event is disabled



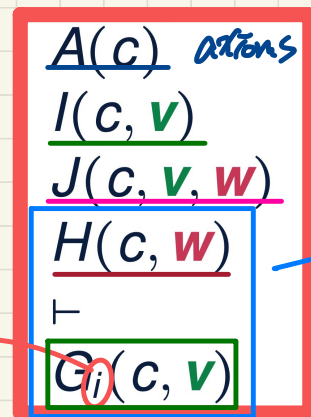
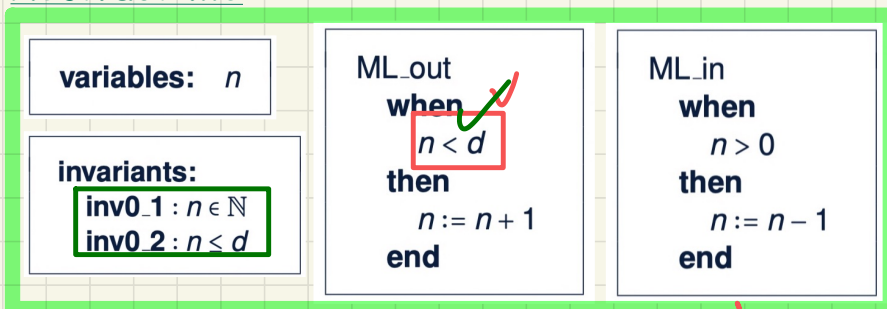
$\Rightarrow$ no new behaviour

introduced by the concrete event).

e.g. for some value, ^{new behaviour (not acceptable)} ML-out is disabled in M_0 but enabled in M_1

PO/VC Rule of Guard Strengthening: Sequents

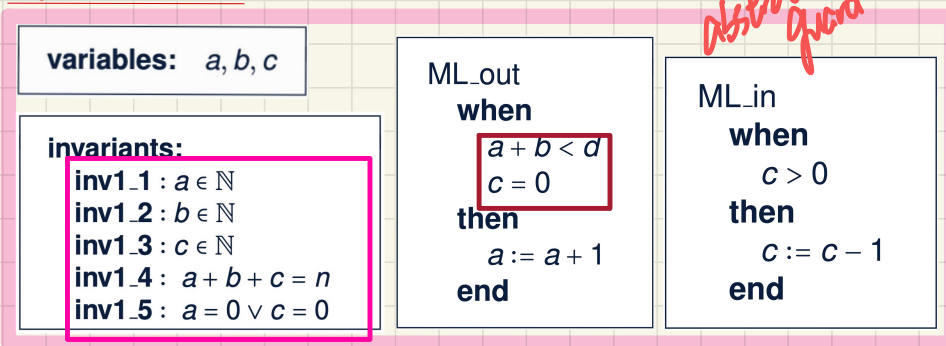
Abstract m0



concrete grd
 $\Rightarrow$ abstract grd

each abstract guard

Concrete m1



ML_out/GRD

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

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

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

exercise:
ML_in/GRD

$\vdash n < d$

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

Written Test 2
~ slide 58.

ML-out

$$n < d$$

ML-out

$$c = 0$$

$$a + b \leq d$$