Lecture 16 - Nov 4

Bridge Controller

DLF: Alternative Unprovable Sequent
1st Refinement: Abstraction
1st Refinement: State Space

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)

Discharging PO of DLF: Revisiting First Attempt

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

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

replace in the goal every free occurrence of the R by L

d n

$d \in \mathbb{N}$
$n \in \mathbb{N}$
$n \le d$
$\vdash$
$n < d \lor n > 0$

$\equiv$

$d \in \mathbb{N}$
$n \in \mathbb{N}$
$n < d \lor n = d$
$\vdash$
$n < d \lor n > 0$

MON

$n < d \lor n = d \vdash n < d \lor n > 0$ **OR_L**

- $n < d \vdash n < d \lor n > 0$ **OR_R1** $n < d \vdash n < d$ **HYP**
- * $n = d \vdash n < d \lor n > 0$ **EQ_LR**, **MON** $\vdash d < d \lor d > 0$ **OR_R2** $\vdash d > 0$ **?**

what if EQ_RL was used?

$n = d \vdash n < d \lor n > 0$ EQ_RL ✓✓

$n = d \vdash n < n \lor n > 0$ MON

$\vdash n < n \lor n > 0$ ARI

(1) $n < n \equiv F$
(2) $F \lor \_ \equiv \_$

$\vdash n > 0$

may not be a realistic hypothesis to add back to the model ∵ IB compound may not have any var.

Understanding the Failed Proof on DLF

constants: d

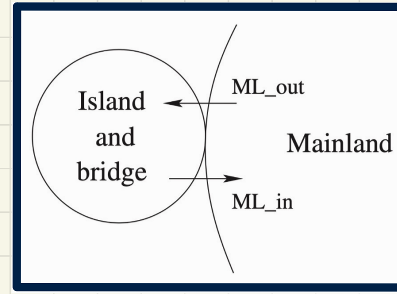
axioms:
axm0_1 : $\boxed{d \in \mathbb{N}}$ ② $d \geq 0$
axm0_2 : $d > 0$

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



Unprovable Sequent: $\vdash \boxed{d > 0}$ goal.

$\underbrace{0 < 0}_{F} \lor \underbrace{0 > 0}_{F}$

↳ system deadlocks right after init when $d = 0$

Not being able to prove $d > 0$

↳ current model may violate it : $\boxed{\neg(d > 0)}$ is true

① $d \leq 0$ ⇝ violating the goal

② $d \geq 0$ ⇝ typing constraint

↳ $\boxed{d = 0.}$

Say $d = 0$.

After init. $n = 0$

$\boxed{G(ML\_out)}$ $\overset{0}{n} < \overset{0}{d}$ ✗

$\boxed{G(ML\_in)}$ $\overset{0}{n} > 0$

Fix: add extra axiom $d > 0$

Discharging PO of DLF: Second Attempt

$d \in \mathbb{N}$ axm0_1
$n \in \mathbb{N}$ $d > 0$ /* axm0_2 */
$n \leq d$
$\vdash$
$n < d \vee n > 0$

$\equiv$

$d \in \mathbb{N}$
$n \in \mathbb{N}$ $d > 0$
$n < d \vee n = d$
$\vdash$
$n < d \vee n > 0$

MON

$d > 0$
$n < d \vee n = d$
$\vdash$
$n < d \vee n > 0$

OR_L

Case 1:

$d > 0$
$n < d$
$\vdash$
$n < d \vee n > 0$

OR_R1

$d > 0$
$n < d$
$\vdash$
$n < d$

HYP

Case 2:

$d > 0$
$n = d$
$\vdash$
$n < d \vee n > 0$

EQ_LR, MON

$d > 0$
$\vdash$
$d < d \vee d > 0$

OR_R2

HYP

$d > 0$
$\vdash$
$d > 0$

?

Discharging PO of DLF: Second Attempt

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

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

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

$$\frac{H \vdash P}{H \vdash P \vee Q} \text{ OR\_R1}$$

$$\frac{H \vdash Q}{H \vdash P \vee Q} \text{ OR\_R2}$$

$d \in \mathbb{N}$
$d > 0$
$n \in \mathbb{N}$
$n \leq d$
$\vdash$
$n < d \vee n > 0$

Summary of the Initial Model: Provably Correct

static

constants: d

axioms:
axm0_1 : $d \in \mathbb{N}$
$\boxed{\textbf{axm0\_2} : d > 0}$

fix for proving deadlock freedom

dynamic

variables: n

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

init
begin
$n := 0$
end

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

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

added for inv. preserva.

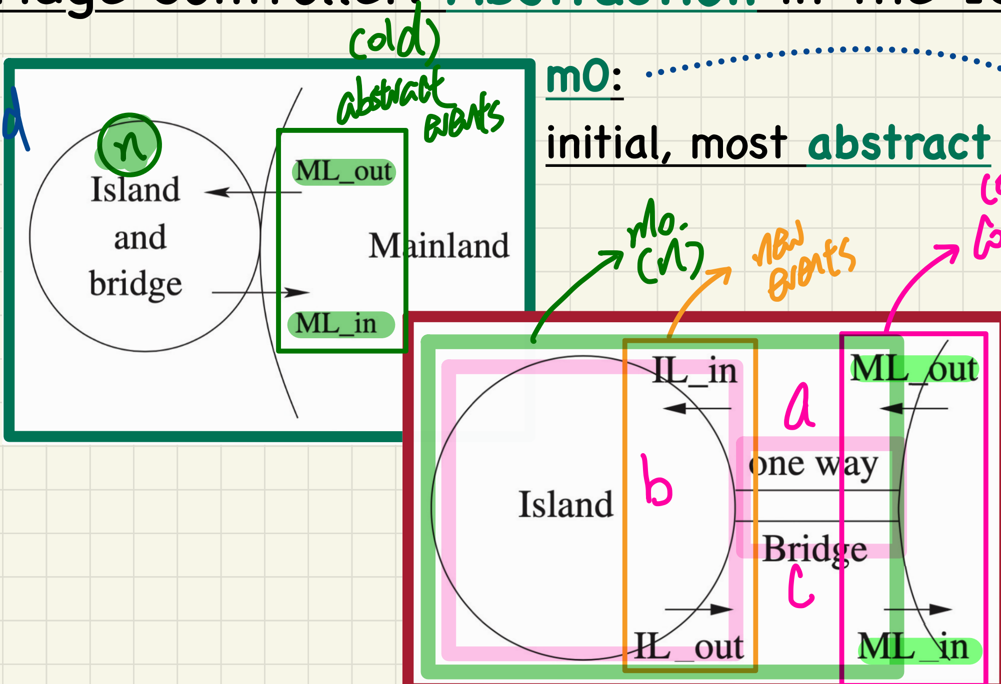
Correctness Criteria:

+ Invariant Establishment
+ Invariant Preservation
+ Deadlock Freedom

Bridge Controller: Abstraction in the 1st Refinement

ML - mainland

IL - Island



m0:

initial, most **abstract**

added "concreteness" (i.e., one-way bridge)

a, b, c

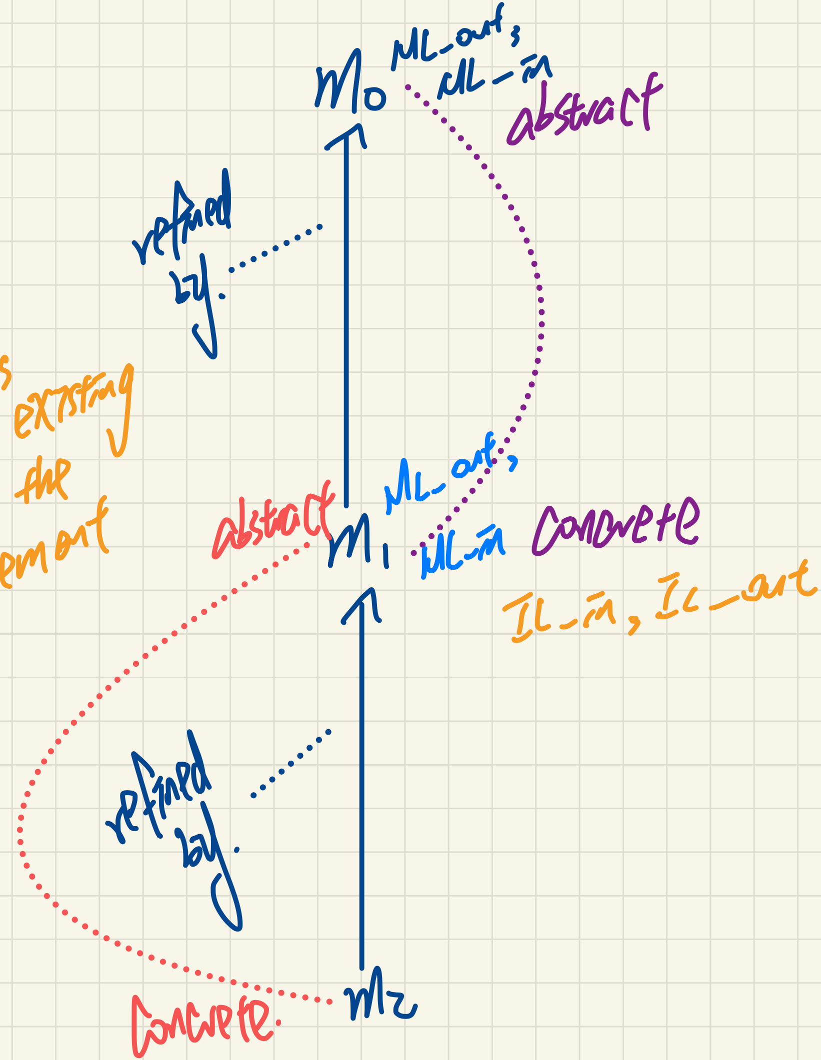
m1:

second, more **concrete**

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.

existence \ version	M0 abstract	M1 concrete
M0 old	ML_out, ML_in	ML_out, ML_in.
M1 new	n.a.	IL_in, IL_out

events only existing in the refinement



** $\boxed{a * c = 0}$ valid but hard to use as Hyp.* $(a>0 \wedge c=0) \vee (c>0 \wedge a=0)$

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.

** $c=0$

$\boxed{\cancel{a}+c=\cancel{a}}$

$\vee$

$a+\cancel{c}=\cancel{c}$

$a=0$

→ n (M_0)

Dynamic Part of Model

variables: a, b, c

linking/gluing invariant.

invariants:
- inv1_1 : $a \in \mathbb{N}$
- inv1_2 : $b \in \mathbb{N}$
- inv1_3 : $c \in \mathbb{N}$
- inv1_4 : ??
- inv1_5 :* ??

typing constraints

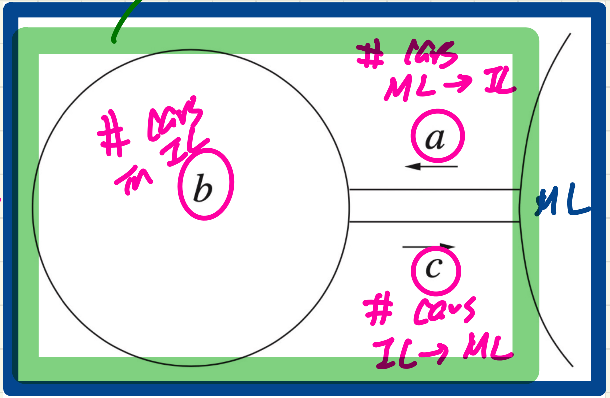
M_1

$n = a+b+c$

M_0

→ $a=0 \vee c=0$

safety inv.



Static Part of Model

constants: d

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

Exercises

Q. Can inv1_5 be $a \neq c$? (3, 2)

inv1_4: linking abstract & concrete states

inv1_5: bridge is one-way