

EECS3342 System Specification and Refinement
(Winter 2022)

Q&A - Week 7 Lectures

Thursday, March 10

Announcements

WA (4).

- + No Lecture W8 released
- + Written Test 3

Towards the end of this lecture, you stated that there had to be a concrete representation of ML_in.

I was wondering how this would work since $c = 0$ in this case.

For the abstract model, we can execute ML_in since $n = 1$ after the ML_out event, but in the case for $m1$, $c = 0$ since the bridge is one way.

Bridge Controller: Abstract vs. Concrete State Transitions

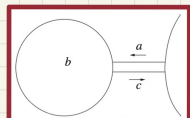
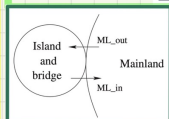
Abstract m0

variables: n

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

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

invariants:
inv0.1: $n \in \mathbb{N}$
inv0.2: $n \leq d$



Concrete m1

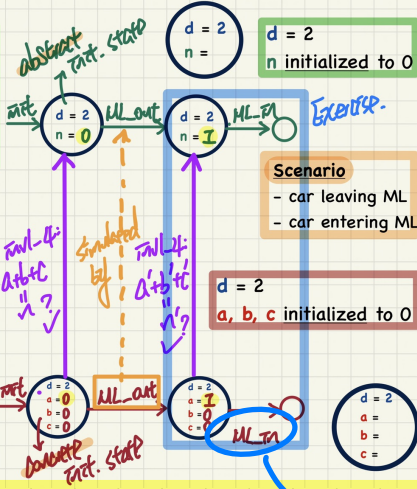
variables: a, b, c

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

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

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: $a = 0 \vee c = 0$

invariants involving both ab & c variables



$d = 2$
 n initialized to 0

$d = 2$
 a, b, c initialized to 0

$d = 2$
 $a =$
 $b =$
 $c =$

Scenario
- car leaving ML
- car entering ML

1. disabled $\because c = 0$
2. try adding some transitions by IL_in & IL_out

For the following dischargement,
 you used EQ_LR twice to achieve $n < d \vdash n < d$.
 I was wondering if it would also be valid to use EQ_RL the second time
 to achieve $a + b < d \vdash a + b < d$?
 Would this be bad practice?
 How would that be marked in a test setting?

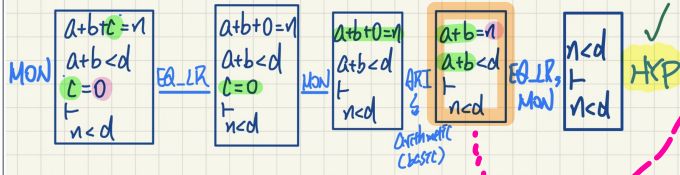
Discharging POs of m1: Guard Strengthening in Refinement

ML_out/GRD

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

when applying MON IX,
 guide yourself by the
 goal to see
 hypothesis to drop

| | | | |
|---|-----|--------------------------|-----|
| $\frac{H1 \vdash G}{H1, H2 \vdash G}$ | MON | $\frac{}{H, P \vdash P}$ | HYP |
| $\frac{H(F), E = F \vdash P(F)}{H(E), E = F \vdash P(E)}$ | | | |
| EQ_LR | | | |



$a + b = n$
 $a + b < d$
 \vdash
 $n < d$

EQ_RL
 MON

$a + b = n$
 $a + b < d$
 \vdash
 $a + b < d$

HYP

$$\frac{H, \neg P \vdash Q}{H \vdash \boxed{P \vee Q}} \quad \text{OR_R}$$

↓
disjunctive goal

$$H \Rightarrow \underline{P \vee Q}$$

$$\equiv H \wedge \neg P \Rightarrow \underline{Q}$$

↓
extra hypothesis

(\neg of one of the goal(s))

$$\begin{array}{l} d > 0 \\ a \in \mathbb{N} \\ b \in \mathbb{N} \\ \vdash \\ \quad \cdot a + b < d \wedge 0 = 0 \\ \vee \cdot 0 > 0 \\ \vee \boxed{a > 0} \\ \vee \cdot b > 0 \wedge a = 0 \end{array}$$

OR_R

$$\begin{array}{l} d > 0 \\ \boxed{a \in \mathbb{N}} \cdot \\ b \in \mathbb{N} \cdot \\ \boxed{\neg(a > 0)} \\ \vdash \\ \quad a + b < d \wedge 0 = 0 \\ \vee 0 > 0 \\ \vee b > 0 \wedge a = 0 \end{array}$$

$a = 0$