EECS3342 System Specification and Refinement (Winter 2022)

Q&A - Week 4 Lecture

Thursday, February 10

Announcements

- Written Test 2 next Tuesday
- Revised Written Test 2 start time
- Example questions for Written Test 2

- Lecture W5 postponed

reduced intensity
1. fewer questions
or
2. same # but easier

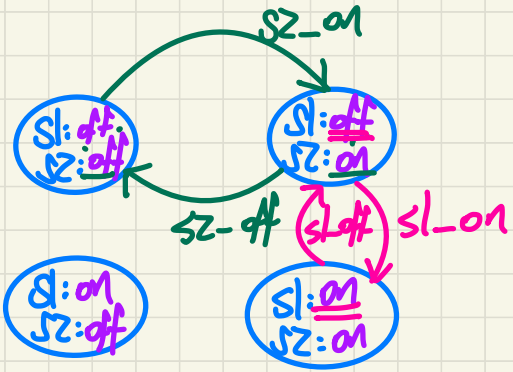
Lab 1
1. How can. preservation PO is formulated.
2. To determine such POs, what event guards are needed?

EECS4313

Is there any state space for which it is possible to generate JUnit test cases?
i.e., is there any state space that does not have combinatorial explosion?

Example 1: Exhaustive Testing

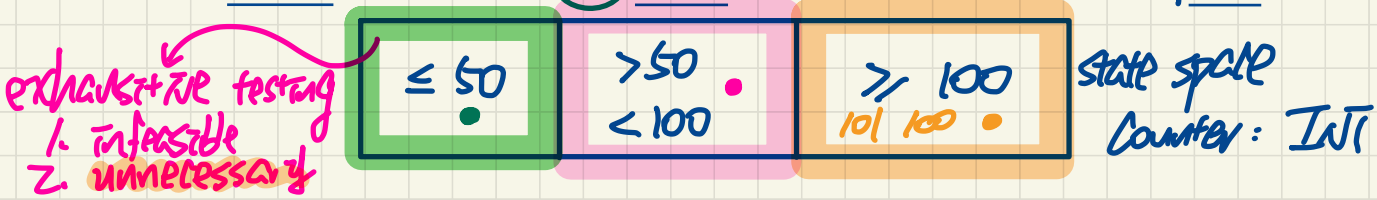
+ sensor_1 : {on, off}
+ sensor_2 : {on, off}



Example 2: Equivalence Classes

+ counter: INT → 2^{32}
+ inc when counter < 100 then counter := counter + 1 end
+ dec when counter > 50 then counter := counter - 1 end

these two values can partition the state space into 3 classes of values



When applying the MON inference rule, how do we decide what hypotheses to drop?

1. Look at the goal.
2. Picture how the goal should be ultimately proved.

Discharging POs of revised m0: Invariant Preservation

ML_out/inv0_1/INV

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

MON

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

P2

→ only var. n is relevant

ML_in/inv0_1/INV

$d \in \mathbb{N}$
$n \in \mathbb{N}$
$n \leq d$
$n > 0$
$\vdash$
$n - 1 \in \mathbb{N}$

MON

$n > 0 \vdash n-1 \in \mathbb{N}$

P2'

ML_out/inv0_2/INV

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

MON

$n < d \vdash n+1 \leq d$

INC

ML_in/inv0_2/INV

$d \in \mathbb{N}$
$n \in \mathbb{N}$
$n \leq d$
$n > 0$
$\vdash$
$n - 1 \leq d$

MON

$n \leq d \vdash n-1 \leq d$

$n-1 < d \vee n-1 = d$

OR_R1

$n \leq d \vdash n-1 < d$

DEC

Iterative process:
if the proof gets stuck, go back to see if some useful hypotheses were dropped