Design of a traffic control system for cars

Multiple choice quiz

Abstract model

- Q1: Which requirements are considered? Select the right answer(s)

N°	Statement	Identifier*
1	The system is to control cars on a bridge connecting a mainland and an island	FUN-1
2	The system controls the entrance to the bridge at both ends of it	FUN-2
3	The system is equipped with two traffic lights with two colors : *green* and *red*	EQP-1
4	The driver shall pass only on a green traffic light	EQP-2
5	The system is equipped with four sensors with two states: *on* and *off*	EQP-3
6	The sensors are used to detect the presence of a car entering or leaving the bridge: "*on*" means that a car is willing to enter the bridge or to leave it	EQP-4
7	The number of cars on the bridge and island is limited	FUN-3
8	Two opposite cars are not allowed to pass the bridge at the same time	SAF-1

** The identifiers are slightly different from those in Statement_study-case-car.pdf file. It does not matter, use these identifiers instead*

Abstract model

- Q2: How many invariants are there ?

a) 1

b) 2

c) 3

d) 4

Abstract model

- Q3: Find out the correct ML_out/inv1/INV Proof Obligation rule (type invariant)?

$a)$ $(n+1) \in \mathbb{N}$

$b)$ $\vdash$

c) $\mathrm{n} \leq d$

d) $n \in \mathbb{N}$

$e)$ $d \in \mathbb{N}$

f) $n > 0$

g) $n > d$

h) $n < d$

__Warning:__ use a blank space between characters only (in alphabetical order)

- *Example: "a b e f" stands for*

$(n+1) \in \mathbb{N} \vdash d \in \mathbb{N} \wedge n > 0$

Abstract model

- Q4: What is the sequence of validated inference rules for the proof of ML_out/inv1/INV?

a) OR_R

b) MON

c) DEC

d) $P3$

e) $P2$

<u>Warning:</u> use a blank space after ";" only

- *Example: "a; b; e" stands for* $OR\_R; MON; P2$

Abstract model

- Q5: What is the derived requirement on limitation?

a) The number of cars on the bridge and island is limited but positive
b) No cars can enter the island
c) The number of cars on the bridge and island is limited
d) The number of cars on the bridge and island is limited but lower than 10

First refined model

- Q6: Find the 7 errors. Type the numbers in **ascending order**

Example: 6; 7; 11; 13

EVENTS

INITIALISATION $\hat{=}$

1 a := 0
2 b := 10
3 c := 0
4 n := 10

ML_out $\hat{=}$
REFINES
5 ML_out
WHEN
6 a+b ≤ d
THEN
7 n:= n+1
END

ML_in $\hat{=}$
REFINES
8 ML_out
WHEN
9 c > 0
THEN
10 c:= c - 1
END

IL_in $\hat{=}$
WHEN
11 a ∈ ℕ
12 a > 0
THEN
13 a := a – 1
14 c := c + 1
END

IL_out $\hat{=}$
WHEN
15 a = 0
16 b > 0
THEN
17 b := b – 1
18 c := c + 1
END

First refined model

- Q7: Write down the invariant property expressing the requirement SAF-1

a) a
b) b
c) c
d) d
e) n
f) =

g) >
h) <
i) 0
j) 1

k) $\wedge$
l) $\vee$
m) $\neq$
n) $\in$

Example: "a h j" stands for $a < 1$

First refined model

- Q8: Find out the correct PO refinement rule ML_out/grd1/GRD_REF ?

a) $0 < d$

b) $\vdash$

c) $\mathrm{n} \leq d$

d) $n \in \mathbb{N}$

e) $d \in \mathbb{N}$

f) $n > 0$

g) $n > d$

h) c = 0

i) a + b < d

j) a + b + c = n

k) n < d

l) a=0 ∨ c=0

m) a ∈ $\mathbb{N}$, b ∈ $\mathbb{N}$, $c \in \mathbb{N}$

n) c > 0

<u>Warning:</u> use brackets and coma for hypotheses, and put them in alphabetical order

- *Example: "(a, c, d) b e" stands for*

0<d, n≤d, n∈ℕ ⊢ $d \in \mathbb{N}$

First refined model

- Q9: Type the proof by applying inference rules for ML_out/grd1/GRD_REF

First refined model

- Q10: Type the proof of the invariant preservation rule ML_in/inv1/INV_REF?

Appendix

- First Peano (P1) axiom is: $\vdash\ \mathbf{0}\in\mathbb{N}$
- Second Peano (P2) axiom is: $\boldsymbol{n}\in\mathbb{N} \vdash \boldsymbol{n}+\mathbf{1}\in\mathbb{N}$
- and a derived second Peano axiom (P2') is:

  $\boldsymbol{n}\in\mathbb{N},\quad 0<\boldsymbol{n} \vdash \boldsymbol{n}-\mathbf{1}\in\mathbb{N}$
- Third Peano (P3) axiom is: $\boldsymbol{n}\in\mathbb{N} \vdash \mathbf{0}\leq\boldsymbol{n}$
- INC axiom is: $\boldsymbol{n}\in\mathbb{N}, \boldsymbol{m}\in\mathbb{N},\ \boldsymbol{n}<\boldsymbol{m} \vdash \boldsymbol{n}+\mathbf{1}\leq\boldsymbol{m}$
- DEC axiom is: $\boldsymbol{n}\in\mathbb{N}, \boldsymbol{m}\in\mathbb{N},\ \boldsymbol{n}\leq\boldsymbol{m} \vdash \boldsymbol{n}-\mathbf{1}\leq\boldsymbol{m}$

Appendix

$\dfrac{H \vdash \mathrm{P}}{H \vdash P \vee Q}$ OR_R	$\dfrac{H, P \vdash R \qquad H, Q \vdash R}{H, P \vee Q \vdash R}$ OR_L
$\dfrac{}{P \vdash P}$ HYP	$\dfrac{}{\bot \vdash P}$ $CNTR$
$\dfrac{H(F), E = F \vdash \mathrm{P(F)}}{H(E), E = F \vdash P(E)}$ EQ_LR where P(E) is a predicate depending on an expression E (idem for H(E) and H(F))	$\dfrac{}{\vdash E = E}$ EQL

Appendix

$$\frac{H, \neg P \ \vdash \mathrm{Q}}{H \ \vdash P \ \vee Q} \quad NEG$$	
$$\frac{H, P, Q \ \vdash \mathrm{R}}{H, P \ \wedge Q \vdash R} \quad AND\_L$$	$$\frac{H \vdash \mathrm{P} \qquad H \vdash \mathrm{Q}}{H \vdash P \ \wedge Q} \quad AND\_R$$
$$\frac{}{H, P, \neg P \vdash Q} \quad NOT\_L$$	$$\frac{H, P \vdash Q \qquad H, P \vdash \neg Q}{H \vdash \neg P} \quad NOT\_R$$
$$\frac{H, P, Q \ \vdash \mathrm{R}}{H, P, P \ \Rightarrow Q \vdash R} \quad IMP\_L$$	$$\frac{H, P \ \vdash \mathrm{Q}}{H \vdash P \ \Rightarrow Q} \quad IMP\_R$$