Prof. Dr. A. Podelski, Dr. B. Westphal
D. Gauß

Sommersemester 2013

Real-Time Systems

http://swt.informatik.uni-freiburg.de/teaching/SS2013/rtsys

Exercise Sheet 2

Early submission: Tuesday, 2013-05-13, 14:00 Regular submission: Wednesday, 2012-05-14, 14:00

Exercise 1 (5/20 Points)

A traffic light for pedestrians is modelled by the observables 'Light' of data type {red, yellow, green} and 'Button' of data type {press, release}.
Consider an interpretation $\mathcal{I}$ of these observables as given by the timing diagrams in Figure 1.

(i) Calculate the truth value of the DC formulae

$$(true \,;\, \int \mathsf{Light} = \mathsf{green} = \ell) \,;\, true \tag{B}$$

and

$$\int \mathsf{Button} = \mathsf{press} \wedge \mathsf{Light} = \mathsf{red} \leq 1 \tag{C}$$

in the interval $[1, 5]$. [OD08] (4)

(ii) Are the chop points you need unique? (1)

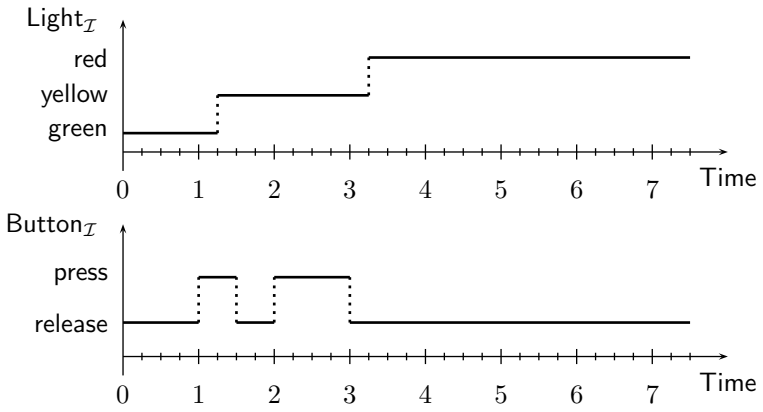

Figure 1: Interpretation of 'Light' and 'Button'.

Exercise 2 (5/20 Points)

A traffic light for pedestrians is modelled by the observables 'Light' of data type {red, yellow, green} and 'Button' of data type {press, release}.
Formalise the following requirements using Duration Calculus:

- The button is not pressed when the lights show green. (1)
- The yellow lights is used at least once. (1)
- If the button is pressed, it takes at most 120 time units until green is shown. (1)
- Green phases are at least 10 time units long. (1)
- Within 3600 time units, the lights should not show green for more than 1000 time units. (1)

Hint: Explain your understanding of the requirement in natural language as precise as you can. Formalise your understanding. Explain.

Exercise 3 (10/20 Points)

We can abstractly model a rail-road level crossing by the observables

- 'Track' with domain {empty, appr, cross},
- 'Gate' with domain {open, moving, closed}.

The track observable represents the presence of the train with two logical regions of the crossing. It is 'empty' if there is no train near or on the crossing, it is 'appr' if a train is near the crossing, and 'cross' if the train is in the area where road and tracks intersect.
The gate can be open, moving (up or down), or closed.
We use the following abbreviations:

E stands for $\mathsf{Track} = \mathsf{empty}$
A stands for $\mathsf{Track} = \mathsf{appr}$
X stands for $\mathsf{Track} = \mathsf{cross}$

O stands for $\mathsf{Gate} = \mathsf{open}$
C stands for $\mathsf{Gate} = \mathsf{closed}$

Consider the following DC properties:

$$\Box(\lceil X \rceil \implies \lceil C \rceil) \quad \text{('Safety')}$$
$$(\lceil E \rceil \,;\, true) \vee \lceil \rceil \quad \text{('Init')}$$
$$\Box((\lceil E \rceil \,;\, true \,;\, \lceil X \rceil) \implies \ell \geq \varepsilon) \quad \text{('T-Fast')}$$
$$\Box((\lceil \neg E \rceil \wedge \ell \geq \varepsilon) \implies true \,;\, \lceil C \rceil) \quad \text{('G-Close')}$$

(i) Explain informally the meaning of each of these formulae. [OD08] (4/10)

(ii) We distinguished requirements, design decisions, and assumptions.
Which of the formulae serves which purpose here? Briefly explain. (1/10)

(iii) Prove the following implication by using the DC semantics: [OD08] (5/10)

$$\mathsf{Init} \wedge \mathsf{T\text{-}Fast} \wedge \mathsf{G\text{-}Close} \implies \mathsf{Safety}$$

References

[OD08] Ernst-Rüdiger Olderog and Henning Dierks. *Real-Time Systems - Formal Specification and Automatic Verification.* Cambridge University Press, 2008.