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 3

Early submission: Monday, 2013-06-03, 14:00 Regular submission: Wednesday, 2013-06-05, 14:00

Exercise 1: Validity [1] (5/20 Points)

Let P, Q, R be state assertions. ***Choose*** one of the following blocks (i) or (ii).

Which of the formulae (a) – (c) (in your chosen block) is valid?
Explain your argument or give a counterexample. Prove that (d) (in your chosen block) is valid.

(i)
a) $\neg\lceil P\rceil \implies \lceil\neg P\rceil$
b) $(\lceil P\rceil \wedge \lceil Q\rceil) \impliedby \lceil P \wedge Q\rceil$
c) $\Diamond(\lceil P\rceil \wedge \lceil Q\rceil) \implies (\Diamond\lceil P\rceil \wedge \Diamond\lceil Q\rceil)$
d) $\lceil\rceil \implies \int P = 0$

(ii)
a) $\neg\lceil P\rceil \impliedby \lceil\neg P\rceil$
b) $(\lceil P\rceil \wedge \lceil Q\rceil) \implies \lceil P \wedge Q\rceil$
c) $\Diamond(\lceil P\rceil \wedge \lceil Q\rceil) \impliedby (\Diamond\lceil P\rceil \wedge \Diamond\lceil Q\rceil)$
d) $\lceil\neg P\rceil \implies \int P = 0$

Exercise 2 (Standard Forms) [1] (3/20 Points)

Consider an interpretation of P as shown in the timing diagram in Figure 1. Give a (non-trivial) interpretation of Q and R such that

(i) $\lceil R\rceil \longrightarrow \lceil P\rceil$,

(ii) $\lceil P\rceil \xrightarrow{2.5} \lceil Q\rceil$,

are satisfied.

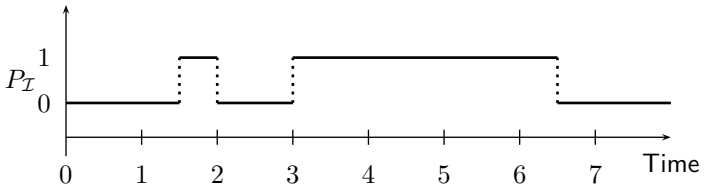

Figure 1: Timing diagram for Exercise 2.

Exercise 3 (Stability) [1] (2/20 Points)

Discuss the difference between the stability patterns:

$$\lceil\neg\pi\rceil \,;\, \lceil\pi\rceil \xrightarrow{\leq\theta} \lceil\pi\rceil \quad \text{and} \quad \lceil\pi\rceil \xrightarrow{\leq\theta} \lceil\pi\rceil.$$

Hint: If possible give examples of interpretations that satisfy only one of the patterns.

Exercise 4 (Duty Cycle) (10/20 Points)

A usual requirement for Radio-Frequency transmitters is the compliance with so called *Duty Cycle* restrictions. A restricted duty cycle specifies the maximum relative amount of time a transceiver is allowed to transmit over a given communication channel.

For example, the European norm EN-300-200-1 specifies the use of the 863 Mhz to 870 Mhz frequencies (the SRD band) to a maximum duty cycle of 0,1%. I.e., the total transmission time of a device operating in that band should not exceed 0,1% in a period of one hour.

An outdoor weather station should relay its measurements wirelessly. It consists of two components: A sensor unit, that gathers data about the current weather conditions, and an RF module, that transmits the collected data when it is available. The sensor unit registers and analyzes different weather factors and produces data asynchronously and passes it to the RF module for transmission. The RF module operates on the SRD band and should comply with the duty cycle restrictions, the transmission of a data packet uses the RF-channel for 100ms. Additionally, it should relay the received data immediately if there has been no transmission for at least 100s, otherwise, the data are ignored and no transmission takes place.

(i) Define a set of observables for the scenario (including their domain) and briefly state why they are a reasonable model.

Which of the observables you consider are input/local/output? (2)

(ii) Formalize the requirements in DC using those observables.

Hint: What are the *requirements on the controller? State them in natural language first.* (3)

(iii) Propose a controller design and specify its intended timed behaviour in DC implementables.

Argue why your controller specification indeed satisfies the requirements. (5)

Exercise 5: Safe Leakage (5 Bonus)

How are the formulae

$$F_1 := \ell \geq 60 \implies \int L \leq \frac{\ell}{20}$$

and

$$F_2 := \ell = 60 \implies \int L \leq \frac{\ell}{20}$$

related? Are they equivalent or is one strictly stronger than the other, i.e. do we have $F_1 \implies F_2$ but not $F_2 \implies F_1$ (or the other way round)?

Prove your claim.

Hint: For each claimed implication, a proof is required; if you claim that one implication does not hold, a counter-example is sufficient, i.e. an interpretation where one formula is satisfied but not the other one.

Plus (just for curiosity): What is the longest continuous leakage that is considered safe according to F_1?

References

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