Christian-Albrechts-Universität zu Kiel
Institut für Informatik und Praktische Mathematik
Prof. Dr. W.-P. de Roever
Harald Fecher · Ben Lukoschus · Immo Grabe

Verifikation nebenläufiger Programme

Sommersemester 2004 **Serie 6** 24. Mai 2004

Thema: Mittsemestertest – Bitte einzeln bearbeiten und abgeben!

Ausgabetermin: 24. Mai 2004

Abgabe: 7. Juni 2004 (vor der Vorlesung im Schrein oder in der Vorlesung)

Aufgabe 1 (7 Punkte) Consider the following program $P^{(n)}$ parametrized over $n \geq 1$.

$$y : \textbf{natural initially } y = 1$$

$$P_1 \parallel \cdots \parallel P_n$$

where

$$P_i :: \left[\begin{array}{l} l_0^i : \textbf{loop forever do} \\ \qquad \left[\begin{array}{l} l_1^i : \textbf{Non-Critical} \\ l_2^i : \textbf{request } y \\ l_3^i : \textbf{Critical} \\ l_4^i : \textbf{release } y \end{array}\right] \end{array}\right]$$

Show the mutal exclusion property for all $P^{(n)}$ by using TLV.

Hint: Use an abstraction which counts the number of processes at each of the l_j locations. Use a further abstraction to get rid of n. Use TLV for model checking and show by hand that the mutal exclusion property for all $P^{(n)}$ follows from the result obtained by TLV.

Send a text file with the SMV code and another text file with the the proof commands for TLV by email to `bls+serie06@informatik.uni-kiel.de` before the deadline.

Aufgabe 2 (5 Punkte) Show or disprove the validity of each of the following formulas:

$$\Box u \equiv u$$
$$\neg\Diamond u \equiv \Box\neg u$$
$$(u_1 \mathcal{U} u_2) \wedge (u_2 \mathcal{U} u_3) \equiv u_1 \mathcal{U} u_3$$
$$\Diamond u_1 \wedge \Box u_2 \equiv \Diamond(u_1 \wedge \Box u_2)$$
$$\Diamond u_1 \wedge \Box u_2 \equiv \Box(\Diamond u_1 \wedge u_2)$$

Aufgabe 3 (9 Punkte) In the following we want to prove Claim 7 of the lecture:

1. Suppose an FDS has the property that
   - $\mathrm{pres}(V) \rightarrow \rho$,

- $\forall s : p(s) \Rightarrow \exists s' : \rho(s, s') \wedge q(s')$ holds for any of its compassion requirements (p, q) and
- $\forall s : \neg q(s) \Rightarrow \exists s' : \rho(s, s') \wedge q(s')$ holds for any of its justice requirements q.

Show that any such FDS is viable.

2. Show that every FDS derived from an SPL program is viable.