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 5** 17. Mai 2004

Thema: `SMC-RESP`, `SET-FEASIBLE`

Ausgabetermin: 17. Mai 2004

Abgabe: 24. Mai 2004 (vor der Vorlesung im Schrein oder in der Vorlesung)

Aufgabe 1 (3 Punkte) Calculate `SMC-RESP`$(\mathcal{D}, \pi_1 = T_1, \pi_1 = C_1)$ (the first version, which does not print the counterexample) where $\mathcal{D}$ is given by $\mathcal{D} = \langle V, \{\pi_1, \pi_2, y\}, \Theta, \rho, \mathcal{J}, \mathcal{C}\rangle$ with

- $V:\ \pi_1 : \{N_1, T_1, C_1\}, \pi_2 : \{N_2, T_2, C_2\}, y : \{0, 1\}$
- $\Theta:\ \pi_1 = N_1 \wedge \pi_2 = N_2 \wedge y = 1$
- $\rho:\ (\pi_1' = \pi_1 \wedge \pi_2' = \pi_2 \wedge y' = y) \vee$
  $(\pi_1 = N_1 \wedge \pi_1' = T_1 \wedge \pi_2' = \pi_2 \wedge y' = y) \vee$
  $(\pi_1 = T_1 \wedge \pi_1' = C_1 \wedge \pi_2' = \pi_2 \wedge y' = 0 \wedge y = 1) \vee$
  $(\pi_1 = C_1 \wedge \pi_1' = N_1 \wedge \pi_2' = \pi_2 \wedge y' = 1) \vee$
  $(\pi_2 = N_2 \wedge \pi_2' = T_2 \wedge \pi_1' = \pi_1 \wedge y' = y) \vee$
  $(\pi_2 = T_2 \wedge \pi_2' = C_2 \wedge \pi_1' = \pi_1 \wedge y' = 0 \wedge y = 1) \vee$
  $(\pi_2 = C_2 \wedge \pi_2' = N_2 \wedge \pi_1' = \pi_1 \wedge y' = 1)$
- $\mathcal{J} : \{\neg\pi_1 = C_1, \neg\pi_2 = C_2\}$
- $\mathcal{C} : \{(\pi_1 = T_1 \wedge y = 1, \pi_1 = C_1), (\pi_2 = T_2 \wedge y = 1, \pi_2 = C_2)\}$.

Write down the values of *cycles*, *pending* and return value. Furthermore, give also the values for $next^i_3$, $next^i_{5,5}$ and $next^i_{7,5}$ for the corresponding `SET-FEASIBLE` execution.

Aufgabe 2 (3 Punkte) Suppose ρ is a transition relation of an `FDS` and A and B are formulas over the `FDS` variable set V, i.e., A and B describe sets of states. Define $\tilde{\rho}$ that restricts ρ to transitions between the two sets described by A and B. Show that your definition satisfies the requirement.

Aufgabe 3 (6 Punkte) Consider `SMC-RESP` that includes the counterexample construction.

1. Show that the **while** loop terminates and computes an MSCS. You may assume the correctness of the algorithm `SET-FEASIBLE`.
2. Suppose the line $(psize, period[1], period[2]) := (2, s, sat(s \diamond R))$ would be replaced by $(psize, period[1]) := (1, s)$. Present an `FDS` such that the modified algorithm does not yield a valid counterexample.