Christian-Albrechts-Universität zu Kiel
Institut für Informatik und Praktische Mathematik

Prof. Dr. W.-P. de Roever
Harald Fecher, Immo Grabe

Verifikation nebenläfiger Programme

Sommer 2005 **Serie 13** 28. Juni 2005

Thema: Endsemestertest

Ausgabetermin: 28. Juni 2005

Abgabe: **Dienstag 12. Juli (10:00 im Schrein) harte deadline!!!**

Everybody should make this test completely on his own!

Aufgabe 1 (6 Punkte) Gegeben sind die Programme P_1 und P_2 gemäß dem Diagram aus Bild 1, wobei t_i^6 vom Zustand rechts unten (Ziel von t_i^3) zu s_i zeigt und wobei

$$
\begin{aligned}
t_1^1 &= i_1 \leq n \wedge ((a[x_1] \leq a[i_1] \wedge a[x_1] \neq -1) \vee a[i_1] = -1) \rightarrow i_1 := i_1 + 1 \\
t_1^2 &= i_1 \leq n \wedge (a[x_1] > a[i_1] \vee a[x_1] = -1) \wedge a[i_1] \neq -1 \rightarrow x_1 := i_1 \\
t_1^3 &= i_1 > n \wedge l < u \rightarrow l := l + 1 \\
t_1^4 &= a[x_1] \neq -1 \rightarrow b[l] := a[x_1]; a[x_1] := -1; i_1 := 1 \\
t_1^5 &= id \\
t_1^6 &= a[x_1] = -1 \rightarrow i_1 := 1
\end{aligned}
$$

$$
\begin{aligned}
t_2^1 &= i_2 \geq 1 \wedge a[x_2] \geq a[i_2] \rightarrow i_2 := i_2 - 1 \\
t_2^2 &= i_2 \geq 1 \wedge a[x_2] < a[i_2] \rightarrow x_2 := i_2 \\
t_2^3 &= i_2 < 1 \wedge l < u \rightarrow u := u - 1 \\
t_2^4 &= a[x_2] \neq -1 \rightarrow b[u] := a[x_2]; a[x_2] := -1; i_2 := n \\
t_2^5 &= id \\
t_2^6 &= a[x_2] = -1 \rightarrow i_2 := n
\end{aligned}
$$

Zeigen Sie mittels dem Owicky-Gries Verfahren, dass $P_1 \| P_2$ das geordnete array von a im array b abspeichert, wobei a ein array von $1..n$ ist und nur (paarweise verschiedene) positive Werte enthählt. Bestimmen Sie angemässene Variableninitialisierungen. Es reicht aus partial correctness zu zeigen.

Aufgabe 2 (6 Punkte) Gegeben sind die Programme P_0, P_1 und P_2 gemäß dem Diagram aus Bild 2, wobei

$$
\begin{aligned}
t_1^1 &= z_1 := \text{Position innerhalb } \{1, .., n\} \text{ wo } y_1 \text{ kleinste positive Zahl ist} \\
t_2^1 &= z_2 := \text{Position innerhalb } \{1, .., n\} \text{ wo } y_2 \text{ grösste Zahl ist} \\
t_i^2 &= d_i!y_i[z_i] \rightarrow y_i[z_i] := -1.
\end{aligned}
$$

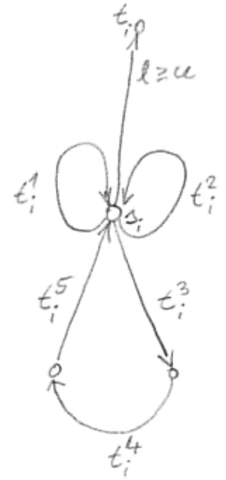

Figure 1:

Außerdem sollte in Bild 2 bei P_0 im linken Flügel oben a[l] statt a[u] stehen. Zeigen Sie mittels dem AFR Verfahren, dass $P_0 \| P_1 \| P_2$ das geordnete array von a im array a abspeichert, wobei a ein array von $1..n$ ist und nur positive Werte enthählt. Bestimmen Sie angemässene Variableninitialisierungen. Es reicht aus partial correctness zu zeigen.

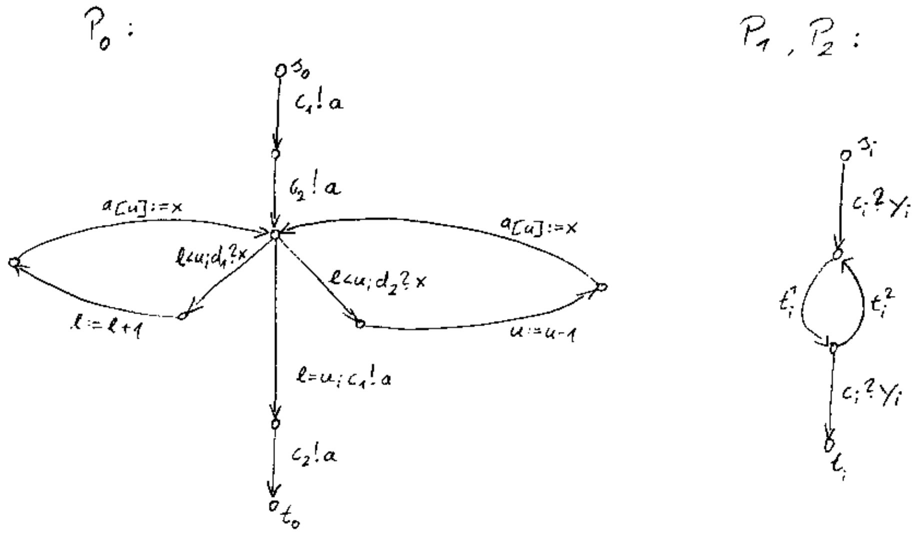

Figure 2:

Aufgabe 3 (4 Punkte) Give stailed proofs for Example 7.40. (Exercise 7.10 auf S. 435).

Aufgabe 4 (6 Punkte) Exercise 7.13 without (c):
(Independence of the prefix-invariance axiom)

The purpose of this exercise is to prove that the prefix-invariance axiom is independent of the other axioms and proof rules of the proof method given in Section 7.4. To this end we define an alternative semantics $\mathcal{O}_{alt}$ in which all these other axioms and rules are valid, but not the prefix-invariance axiom.

Since in Section 7.4.4 we have proved soundness of our proof method , and this proof method includes the prefix-invariance axiom, we have two semantics in one of which this axiom holds, whereas in the other one it does not hold. Had it been possible to derive the prefix-invariance axiom from the other axioms and rules of our proof method, then this would not have been the case by the soundness of our method. Consequently, this proves that the prefix-invariance axiom is independent from those other axioms and rules.

The fact that in $\mathcal{O}_{alt}$ the prefix-invariance axiom does not hold implies that there exists a composite system whose executions according to $\mathcal{O}_{alt}$ changes its initial communication history. We define this to be the case for $D!o \| E!o$, where $D, E \in \mathit{CHAN}$ are specially selected.

$\mathcal{O}_{alt}$ is defined as follows:

- $\mathcal{O}_{alt}(C!e) \stackrel{\text{def}}{=} \{(\sigma, (\sigma : h \mapsto \mathit{shuffle}(\sigma(h))), (C, e(\sigma))) \mid C \in \{D, E\}\}$, with $\mathit{shuffle}(\theta)$ defined by:
  - $\mathit{shuffle}(\theta) \stackrel{\text{def}}{=} \theta$, for $\mathit{length}(\theta) \leq 1$, and
  - $\mathit{shuffle}(\langle (C_1, v_1), (C_2, v_2)\rangle \cdot \theta) \stackrel{\text{def}}{=}$
    $$\begin{cases} \langle (C_2, v_2), (C_1, v_1)\rangle \cdot \mathit{shuffle}(\theta), & \text{if } (C_1 = E \wedge C_2 = D \vee \\ & \qquad C_1 = D \wedge C_2 = E), \text{ and} \\ \langle (C_1, v_1), (C_2, v_2)\rangle \cdot \mathit{shuffle}(\theta), & \text{otherwise.} \end{cases}$$
- $\mathcal{O}_{alt}(D!o \| E!o) \stackrel{\text{def}}{=} \{(\sigma, \sigma', \theta) \mid \text{s.t.}$
  $(\sigma, \sigma', \theta \downarrow D) \in \mathcal{O}_{alt}(D!o) \wedge$
  $(\sigma, \sigma', \theta \downarrow E) \in \mathcal{O}_{alt}(E!o) \wedge$
  $\theta = \theta \downarrow \{D, E\}\}$.
- $\mathcal{O}_{alt}(P) \stackrel{\text{def}}{=} \emptyset$, for all remaining systems.

Validity $\models \{\varphi\} P \{\psi\}$ under semantics $\mathcal{O}_{alt}$ is defined as follows:

for every $(\sigma, \sigma', \theta) \in \mathcal{O}_{alt}(P)$ such that $\sigma \models \varphi$,
we have $(\sigma' : h \mapsto \mathit{shuffle}(\sigma(h)) \cdot \theta) \models \psi$.

1. Check that the prefix-invariance axiom does not hold in semantics $\mathcal{O}_{alt}$.
2. Prove that all remaining axioms and rules are valid under semantics $\mathcal{O}_{alt}$, in particular, the parallel composition rule 7.8 and the invariance rule 7.10.