Verifikation nebenläufiger Programme WS 2004/2005

Ulrich Hannemann Jan Bredereke

Übungsserie 2

Abgabe: Mittwoch, 1.12.2004

Aufgabe 1 Etwas Mathematik als Hintergrund

Die Relation "kleiner als" $\prec_{I\!N} \subseteq I\!N \times I\!N$ ist eine irreflexive, transitive Ordnung auf $I\!N$, sie ist total und wohlfundiert. Auf Basis dieser Relation definieren wir folgende Ordnungen:

(i) $\prec_{lex(k)} \subseteq I\!N^k \times I\!N^k : (n_1, \ldots, n_k) \prec_{lex(k)} (m_1, \ldots, m_k) \Longleftrightarrow$
$\exists 1 \leq i \leq k. \forall 1 \leq j < i. n_j = m_j \wedge n_i \prec_{I\!N} m_i$

(ii) $\prec_{lex(I\!N)} \subseteq \bigcup_{k \in I\!N \setminus \{0\}} I\!N^k \times \bigcup_{k \in I\!N \setminus \{0\}} I\!N^k$
$\prec_{lex(I\!N)} := \bigcup_{k \in I\!N \setminus \{0\}} \prec_{lex(k)}$

(iii) $\prec_{lex} \subseteq \bigcup_{k \in I\!N \setminus \{0\}} I\!N^k \times \bigcup_{k \in I\!N \setminus \{0\}} I\!N^k :$
$(n_1, \ldots, n_r) \prec_{lex} (m_1, \ldots, m_s) \Longleftrightarrow \exists i \in I\!N \setminus \{0\}. \forall 1 \leq j < i.$
$(n_j = m_j \wedge n_i \prec_{I\!N} m_i) \vee (r \prec_{I\!N} s \wedge \forall 1 \leq j \leq r.(n_j = m_j))$

Beweist oder widerlegt die folgenden Behauptungen:

1. $\prec_{lex(k)} \subseteq I\!N^k \times I\!N^k$ ist wohlfundiert.
2. $\prec_{lex(I\!N)} \subseteq \bigcup_{k \in I\!N \setminus \{0\}} I\!N^k \times \bigcup_{k \in I\!N \setminus \{0\}} I\!N^k$ ist wohlfundiert.
3. $\prec_{lex} \subseteq \bigcup_{1 \leq k \leq n} I\!N^k \times \bigcup_{1 \leq k \leq n} I\!N^k$ ist wohlfundiert für beliebiges $n \in I\!N$.
4. $\prec_{lex} \subseteq \bigcup_{k \in I\!N \setminus \{0\}} I\!N^k \times \bigcup_{k \in I\!N \setminus \{0\}} I\!N^k$ ist wohlfundiert

Aufgabe 2 Korrektheitsbeweis

Zeigt, daß das Verfahren, die Abwesenheit von Laufzeitfehlern nachzuweisen, korrekt ist.

Sei $P = (L, T, s, t)$ ein Programm. Falls φ eine totale $\{tt, f\!f\}$-wertige boole'sche Funktion ist, ein Zusicherungsnetz aus Prädikaten $\mathcal{Q}_l$, die total und $\{tt, f\!f\}$-wertig sind, existiert, so daß für jede Transition $(l, c \to f, l') \in T$ gilt

$$\models \mathcal{Q}_l \wedge c \to (\mathcal{Q}_{l'} \circ f) \wedge \mathit{Def}(f),$$

und ferner $\models \varphi \to \mathcal{Q}_s$ gilt, so ist P frei von Laufzeitfehlern.

Aufgabe 3 Parallele Komposition

Beweist: Die parallele Komposition von Transitionssystemen ist assoziativ und kommutativ, d.h., für Transitionssysteme P_1, P_2, and P_3 gilt

- $[[P_1 \parallel P_2] \parallel P_3]$ ist äquivalent zu $[P_1 \parallel [P_2 \parallel P_3]]$,
- $[P_1 \parallel P_2]$ ist äquivalent zu $[P_2 \parallel P_1]$.