Institut für Computersprachen
Technische Universität Wien
Prof. Dr. J. Knoop

A-1040 Wien
Argentinierstr. 8
Tel.: 01-58801-18510

"Analyse und Verifikation (185.276, VU 2.0, ECTS 3.0)" SS 2018

Übungsblatt 5 25.04.2018

Aufgabe 1 : (2+4+2+4 Punkte)

Überlegen Sie, ob $x \geq 0 \wedge y > 0$ die schwächste liberale Vorbedingung für das Programm

$$\pi \;\equiv\; q := 0;\; r := x;\; \textsf{while } r \geq y \textsf{ do } q := q + 1;\; r := r - y \textsf{ od}$$

zur ganzzahligen Division mit Rest und Nachbedingung

$$x = q * y + r \wedge 0 \leq r < y$$

ist?

Falls nein:

1. Geben Sie eine Vorbedingung wlp, $wlp \in$**Bexpr**, an, die die gesuchte schwächste liberale Vorbedingung beschreibt.

Beweisen Sie, dass wlp aus 1.) tatsächlich die gesuchte schwächste liberale Vorbedingung beschreibt, d.h. beweisen Sie:

$$wlp \iff wlp(\pi, x = q * y + r \wedge 0 \leq r < y) \qquad (*)$$

2. Zeigen Sie zum Beweis von $(*)$ insbesondere die partielle Korrektheit der Hoareschen Zusicherung

$$\{wlp\}\ \pi\ \{x = q * y + r \wedge 0 \leq r < y\}$$

d.h. zeigen Sie durch Angabe einer linearen Beweisskizze:

$$\models_{pk}\ \{wlp\}\ \pi\ \{x = q * y + r \wedge 0 \leq r < y\}$$

3. Was ist darüberhinaus zu zeigen, um $(*)$ und damit die Äquivalenz von wlp zur schwächsten liberalen Vorbedingung $wlp(\pi, x = q * y + r \wedge 0 \leq r < y)$ zu beweisen?

4. Beweisen Sie die zusätzliche(n) Eigenschaft(en) aus 3.).

Aufgabe 2: (Ohne Abgabe)

Installieren Sie das System KeY-Hoare (siehe Kapitel 4.9 der Vorlesungsunterlagen für die URL) und führen Sie damit Korrektheitsnachweise für folgende 3 Hoaresche Zusicherungen durch:

- $\models_{pk}\ \{true\}\ \ \textbf{while}\ true\ \textbf{do}\ skip\ \textbf{od}\ \ \{false\}$
- $\models_{pk}\ \{x = n\ \wedge y = m\}\ \ \textbf{while}\ x \neq 1\ \textbf{do}\ y := y + m;\ x := x - 1\ \textbf{od}\ \ \{y = n * m\}$
- $\models_{tk}\ [x = n\ \wedge y = m\ \wedge\ n > 1]\ \ \textbf{while}\ x \neq 1\ \textbf{do}\ y := y + m;\ x := x - 1\ \textbf{od}\ \ [y = n * m]$

Die Arbeit mit dem System soll in der Übungseinheit am 09.05.2018 “live” vorgeführt werden.

Abgabe: Mittwoch, 09.05.2018, vor der Vorlesung.