

## Aufgabe 1: Grundwissen

(a) Geben Sie zwei verschiedene Möglichkeiten der formalen Verifikation an.

- 1. Möglichkeit: formale Verifikation mittels *vollständiger Induktion* (eignet sich bei *rekursiven* Programmen).
- 2. Möglichkeit: formale Verifikation mittels *wp-Kalkül* oder *Hoare-Kalkül* (eignet sich bei *iterativen* Programmen).

(b) Erläutern Sie den Unterschied von partieller und totaler Korrektheit.

- partielle Korrektheit:  
Das Programm verhält sich spezifikationsgemäß, *falls* es terminiert.
- totale Korrektheit:  
Das Programm verhält sich spezifikationsgemäß und es *terminiert immer*.

(c) Gegeben sei die Anweisungssequenz  $A$ . Sei  $P$  die Vorbedingung und  $Q$  die Nachbedingung dieser Sequenz. Erläutern Sie, wie man die (partielle) Korrektheit dieses Programmes nachweisen kann.

Vorgehen	Hoare-Kalkül	wp-Kalkül
Wenn die Vorbedingung $P$ zutrifft, gilt nach der Ausführung der Anweisungssequenz $A$ die Nachbedingung $Q$ .	$\{P\} A \{Q\}$	$P \Rightarrow wp(A, Q)$

(d) Gegeben sei nun folgendes Programm:

```

1  A_1
2  while(b):
3      A_2
4  A_3

```

wobei  $A_1, A_2, A_3$  Anweisungssequenzen sind. Sei  $P$  die Vorbedingung und  $Q$  die Nachbedingung des Programms. Die Schleifeninvariante der while-Schleife wird mit  $I$  bezeichnet. Erläutern Sie, wie man die (partielle) Korrektheit dieses Programmes nachweisen kann.

Vorgehen	Hoare-Kalkül	wp-Kalkül
Die Invariante $I$ gilt vor Schleifeneintritt.	$\{P\}A_1\{I\}$	$P \Rightarrow \text{wp}(A_1, I)$
$I$ ist invariant, d. h. $I$ gilt nach jedem Schleifendurchlauf.	$\{I \wedge b\}A_2\{I\}$	$I \wedge b \Rightarrow \text{wp}(A_2, I)$
Die Nachbedingung $Q$ wird erfüllt.	$\{I \wedge \neg b\}A_3\{Q\}$	$I \wedge \neg b \Rightarrow \text{wp}(A_3, I)$

- (e) Beschreiben Sie, welche Voraussetzungen eine Terminierungsfunktion erfüllen muss, damit die totale Korrektheit gezeigt werden kann.

Mit einer Terminierungsfunktion  $T$  kann bewiesen werden, dass eine Wiederholung terminiert. Sie ist eine Funktion, die

- ganzzahlig,
  - nach unten beschränkt (die Schleifenbedingung ist *false*, wenn  $T = 0$ ) und
  - streng monoton fallend (jede Ausführung der Wiederholung verringert ihren Wert)
- ist.

Im Hoare-Kalkül muss  $\{I \wedge b \wedge (T = n)\}A\{T < n\}$  gezeigt werden, im wp-Kalkül  $I \Rightarrow T \geq 0$ .<sup>a</sup>

<sup>a</sup>[https://osg.informatik.tu-chemnitz.de/lehre/aup/aup-07-AlgorithmenEntwurf-script\\_de.pdf](https://osg.informatik.tu-chemnitz.de/lehre/aup/aup-07-AlgorithmenEntwurf-script_de.pdf)