Technische Universität Berlin
Software and Embedded Systems Engineering Group
Prof. Dr. Sabine Glesner
www.sese.tu-berlin.de Sekr. TEL 12-4 Ernst-Reuter-Platz 7 10587 Berlin

Softwaretechnik und Programmierparadigmen WiSe 2022/2023

Prof. Dr. Sabine Glesner
Milko Monecke
Simon Schwan

Übungsblatt 14

Beispiellösung

Aufgabe 1: Partielle Korrektheit

Beweist mithilfe des Hoare Kalküls die *partielle* Korrektheit folgender Programme.

a) `max(int a,int b):`

$\{true\}$ — $\{P\}$

`if a > b then`

$\{a > b \wedge true\}$ — Regel (4) $\{B \wedge P\}$

$\Rightarrow \{a \geq b \wedge true\}$ — Regel (6)

$\Rightarrow \{true \wedge a \geq b \wedge (true \vee a = b)\}$ — Regel (6)

$\Rightarrow \{a \geq a \wedge a \geq b \wedge (a = a \vee a = b)\}$ — Regel (6) (2)$[m \leftarrow a]$

`m := a`

$\{m \geq a \wedge m \geq b \wedge (m = a \vee m = b)\}$ — Regel (4) $\{Q\}$

`else`

$\{a \leq b \wedge true\}$ — Regel (4) $\{\neg B \wedge P\}$

$\Rightarrow \{b \geq a \wedge true \wedge (b = a \vee true)\}$ — Regel (6)

$\Rightarrow \{b \geq a \wedge b \geq b \wedge (b = a \vee b = b)\}$ — Regel (6) (2)$[m \leftarrow b]$

`m := b`

$\{m \geq a \wedge m \geq b \wedge (m = a \vee m = b)\}$ — Regel (4) $\{Q\}$

`fi`

$\{m \geq a \wedge m \geq b \wedge (m = a \vee m = b)\}$ — $\{Q\}$

b) `trinumber(int n)`[1]:

$\{n \geq 0\}$ $\quad\{P\}$

$\Rightarrow \{0 \leq n \land 0 = 0\}$ $\quad$ Regel (6) (2)

`s := 0;`

$\{0 \leq n \land s = 0\}$ $\quad$ Regel (6)

$\Rightarrow \left\{0 \leq n \land s = \Sigma_{j=0}^{0}\, j\right\}$ $\quad$ Regel (3) (2) $\{I\}$

`i := 0;`

$\left\{i \leq n \land s = \Sigma_{j=0}^{i}\, j\right\}$ $\quad$ Regel (3) (5) $\{I\}$

`while i < n do`

$\quad\left\{i < n \land i \leq n \land s = \Sigma_{j=0}^{i}\, j\right\}$ $\quad$ Regel (5) $\{B \land I\}$

$\quad\Rightarrow \left\{i < n \land s = \Sigma_{j=0}^{i}\, j\right\}$ $\quad$ Regel (6)

$\quad\Rightarrow \left\{i < n \land s + (i+1) = \left(\Sigma_{j=0}^{i}\, j\right) + (i+1)\right\}$ $\quad$ Regel (6)

$\quad\Rightarrow \left\{i < n \land s + (i+1) = \Sigma_{j=0}^{i+1}\, j\right\}$ $\quad$ Regel (6)

$\quad\Rightarrow \left\{i + 1 \leq n \land s + (i+1) = \Sigma_{j=0}^{i+1}\, j\right\}$ $\quad$ Regel (6) (2)$[i \leftarrow i+1]$

`    i := i + 1;`

$\quad\left\{i \leq n \land s + i = \Sigma_{j=0}^{i}\, j\right\}$ $\quad$ Regel (3) (2)$[s \leftarrow s+i]$

`    s := s + i`

$\quad\left\{i \leq n \land s = \Sigma_{j=0}^{i}\, j\right\}$ $\quad$ Regel (5) $\{I\}$

`od`

$\left\{i \geq n \land i \leq n \land s = \Sigma_{j=0}^{i}\, j\right\}$ $\quad$ Regel (5) $\{\neg B \land I\}$

$\Rightarrow \left\{i = n \land s = \Sigma_{j=0}^{i}\, j\right\}$ $\quad$ Regel (6)

$\Rightarrow \left\{s = \Sigma_{j=0}^{n}\, j\right\}$ $\quad$ Regel (6) $\{Q\}$

[1] Berechnet die sogennanten “Triangular Numbers”.

c) `rest(int x, int y):`

$\{x \geq 0\}$	$\{P\}$
$\Rightarrow \{x \geq 0 \land x = x\}$	Regel (6)
$\Rightarrow \{x \geq 0 \land x = 0 * y + x\}$	Regel (6) (2)$[q \leftarrow 0]$
`q := 0;`	
$\{x \geq 0 \land x = q * y + x\}$	Regel (3) (2)$[r \leftarrow x]$
`r := x;`	
$\{r \geq 0 \land x = q * y + r\}$	Regel (3) (5) $\{I\}$
`while r >= y do`	
$\quad\{r \geq y \land r \geq 0 \land x = q * y + r\}$	Regel (5) $\{B \land I\}$
$\quad\Rightarrow \{r \geq y \land x = q * y + r\}$	Regel (6)
$\quad\Rightarrow \{r \geq y \land x = (q * y + y) + r - y\}$	Regel (6)
$\quad\Rightarrow \{r \geq y \land x = (q + 1) * y + r - y\}$	Regel (6)
$\quad\Rightarrow \{r - y \geq 0 \land x = (q + 1) * y + r - y\}$	Regel (6) (2)$[r \leftarrow r - y]$
`    r := r - y;`	
$\quad\{r \geq 0 \land x = (q + 1) * y + r\}$	Regel (3) (2)$[q \leftarrow q + 1]$
`    q := q + 1`	
$\quad\{r \geq 0 \land x = q * y + r\}$	Regel (5) $\{I\}$
`od`	
$\{r < y \land r \geq 0 \land x = q * y + r\}$	Regel (5) $\{\neg B \land I\}$
$\Rightarrow \{r < y \land x = q * y + r \land r \geq 0\}$	Regel (6) $\{Q\}$

d) **Zusatzaufgabe zum knobeln** (einschließlich totaler Korrektheit):

`mod(int x, int y):`

$\{x = m \land y = n \land x \geq 0 \land y > 0\}$	$\{P\}$
$\Rightarrow \{m \texttt{ mod } n = x \texttt{ mod } y \land x \geq 0 \land y > 0\}$	Regel (6) (5) $\{I\}$
`while(x >= y) do`	
$\quad\{x \geq y \land m \texttt{ mod } n = x \texttt{ mod } y \land x \geq 0 \land y > 0\}$	Regel (5) $\{B \land I\}$
$\quad\Rightarrow \{m \texttt{ mod } n = (x - y) \texttt{ mod } y \land x - y \geq 0 \land y > 0\}$	Regel (6) (2) $\{P[x \leftarrow x - y]\}$
`    x := x - y`	
$\quad\{m \texttt{ mod } n = x \texttt{ mod } y \land x \geq 0 \land y > 0\}$	Regel (5) $\{I\}$
`od;`	
$\{x < y \land m \texttt{ mod } n = x \texttt{ mod } y \land x \geq 0 \land y > 0\}$	Regel (3) (5) $\{\neg B \land I\}$
$\Rightarrow \{x = m \texttt{ mod } n\}$	Regel (6) (2) $\{P[erg \leftarrow x]\}$
`erg := x`	
$\{erg = m \texttt{ mod } n\}$	$\{Q\}$

Terminierung: $t = x - y$

1. $\{x \geq y \wedge ... \wedge x \geq 0 \wedge y > 0\} \Rightarrow x - y \geq 0$ Regel (7) $B \wedge I \Rightarrow x - y \geq 0$
2. `while x >= y do`

   $\{... \wedge y > 0 \wedge (x - y = m)\}$ Regel (7) $\{B \wedge I \wedge (t = m)\}$

   $\Rightarrow \{... \wedge (x - y - y < m)\}$ Regel (6) (2) $\{P[x \leftarrow x - y]\}$

   `x := x - y`

   $\{... \wedge (x - y < m)\}$ Regel (7) $\{I \wedge (t < m)\}$

   `od`

Referenz: Hoare Kalkül

(1) Skip-Axiom: $\{P\}$ `skip` $\{P\}$

(2) Zuweisungsaxiom: $\{P[x \leftarrow E]\}$ `x := E` $\{P\}$

(3) Sequenzregel:
$$\frac{\{P\}\ S_1\ \{R\} \quad \{R\}\ S_2\ \{Q\}}{\{P\}\ S_1; S_2\ \{Q\}}$$

(4) if-then-else-Regel:
$$\frac{\{B \wedge P\}\ S_1\ \{Q\} \quad \{\neg B \wedge P\}\ S_2\ \{Q\}}{\{P\}\ \texttt{if}\ B\ \texttt{then}\ S_1\ \texttt{else}\ S_2\ \texttt{fi}\ \{Q\}}$$

(5) while-Regel:
$$\frac{\{B \wedge I\}\ S\ \{I\}}{\{I\}\ \texttt{while}\ B\ \texttt{do}\ S\ \texttt{od}\ \{\neg B \wedge I\}}$$

(6) Konsequenzregel:
$$\frac{\{P \Rightarrow P'\} \quad \{P'\}\ S\ \{Q'\} \quad \{Q' \Rightarrow Q\}}{\{P\}\ S\ \{Q\}}$$

(7) Terminierung:
$$\frac{\{B \wedge I \wedge (t = m)\}\ S\ \{I \wedge (t < m)\},\ B \wedge I \Rightarrow t \geq 0}{\{I\}\ \texttt{while}\ B\ \texttt{do}\ S\ \texttt{od}\ \{\neg B \wedge I\}}$$

Vorgehen: finde Terminierungsfunktion $t \mapsto \mathbb{N}$, sodass

1. $B \wedge I \Rightarrow t \geq 0$ und
2. $\{B \wedge I \wedge (t = m)\}\ S\ \{I \wedge (t < m)\}$ gilt.