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

◆SESE

Softwaretechnik und Programmierparadigmen WiSe 2023/2024

Prof. Dr. Sabine Glesner
Simon Schwan
Julian Klein

Übungsblatt 10   Beispiellösung

Aufgabe 1: Partielle Korrektheit

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

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

$\{true\}$ $\hspace{6cm}$ $\{P\}$

   `if a > b then`

$\hspace{2cm}\{a > b \wedge true\}$ $\hspace{4cm}$ Regel (4) $\{B \wedge P\}$

$\hspace{2cm}\Rightarrow \{a \geq b \wedge true\}$ $\hspace{4cm}$ Regel (6)

$\hspace{2cm}\Rightarrow \{true \wedge a \geq b \wedge (true \vee a = b)\}$ $\hspace{2.5cm}$ Regel (6)

$\hspace{2cm}\Rightarrow \{a \geq a \wedge a \geq b \wedge (a = a \vee a = b)\}$ $\hspace{1.5cm}$ Regel (6) (2)$[m \leftarrow a]$

$\hspace{2.2cm}$`m := a`

$\hspace{2cm}\{m \geq a \wedge m \geq b \wedge (m = a \vee m = b)\}$ $\hspace{2cm}$ Regel (4) $\{Q\}$

   `else`

$\hspace{2cm}\{a \leq b \wedge true\}$ $\hspace{4cm}$ Regel (4) $\{\neg B \wedge P\}$

$\hspace{2cm}\Rightarrow \{b \geq a \wedge true \wedge (b = a \vee true)\}$ $\hspace{2cm}$ Regel (6)

$\hspace{2cm}\Rightarrow \{b \geq a \wedge b \geq b \wedge (b = a \vee b = b)\}$ $\hspace{1.5cm}$ Regel (6) (2)$[m \leftarrow b]$

$\hspace{2.2cm}$`m := b`

$\hspace{2cm}\{m \geq a \wedge m \geq b \wedge (m = a \vee m = b)\}$ $\hspace{2cm}$ Regel (4) $\{Q\}$

   `fi`

$\{m \geq a \wedge m \geq b \wedge (m = a \vee m = b)\}$ $\hspace{4cm}$ $\{Q\}$

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

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

$\Rightarrow \{0 \leq n \wedge 0 = 0\}$ $\hfill$ Regel (6) (2)

`s := 0;`

$\{0 \leq n \wedge s = 0\}$ $\hfill$ Regel (6)

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

`i := 0;`

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

`while i < n do`

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

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

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

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

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

$\quad$ `i := i + 1;`

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

$\quad$ `s := s + i`

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

`od`

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

$\Rightarrow \left\{i = n \wedge s = \Sigma_{j=0}^{i} j\right\}$ $\hfill$ Regel (6)

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

---

[1]Berechnet die sogennanten "Triangular Numbers".

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

$$\{x \geq 0\} \hfill \{P\}$$
$$\Rightarrow \{x \geq 0 \land x = x\} \hfill \text{Regel (6)}$$
$$\Rightarrow \{x \geq 0 \land x = 0 * y + x\} \hfill \text{Regel (6) (2)}[q \leftarrow 0]$$

```
q := 0;
```

$$\{x \geq 0 \land x = q * y + x\} \hfill \text{Regel (3) (2)}[r \leftarrow x]$$

```
r := x;
```

$$\{r \geq 0 \land x = q * y + r\} \hfill \text{Regel (3) (5) } \{I\}$$

```
while r >= y do
```

$$\{r \geq y \land r \geq 0 \land x = q * y + r\} \hfill \text{Regel (5) } \{B \land I\}$$
$$\Rightarrow \{r \geq y \land x = q * y + r\} \hfill \text{Regel (6)}$$
$$\Rightarrow \{r \geq y \land x = (q * y + y) + r - y\} \hfill \text{Regel (6)}$$
$$\Rightarrow \{r \geq y \land x = (q + 1) * y + r - y\} \hfill \text{Regel (6)}$$
$$\Rightarrow \{r - y \geq 0 \land x = (q + 1) * y + r - y\} \hfill \text{Regel (6) (2)}[r \leftarrow r - y]$$

```
    r := r - y;
```

$$\{r \geq 0 \land x = (q + 1) * y + r\} \hfill \text{Regel (3) (2)}[q \leftarrow q + 1]$$

```
    q := q + 1
```

$$\{r \geq 0 \land x = q * y + r\} \hfill \text{Regel (5) } \{I\}$$

```
od
```

$$\{r < y \land r \geq 0 \land x = q * y + r\} \hfill \text{Regel (5) } \{\neg B \land I\}$$
$$\Rightarrow \{r < y \land x = q * y + r \land r \geq 0\} \hfill \text{Regel (6) } \{Q\}$$

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

`mod(int x, int y):`

$$\{x = m \land y = n \land x \geq 0 \land y > 0\} \hfill \{P\}$$
$$\Rightarrow \{m \bmod n = x \bmod y \land x \geq 0 \land y > 0\} \hfill \text{Regel (6) (5) } \{I\}$$

```
while(x >= y) do
```

$$\{x \geq y \land m \bmod n = x \bmod y \land x \geq 0 \land y > 0\} \hfill \text{Regel (5) } \{B \land I\}$$
$$\Rightarrow \{m \bmod n = (x - y) \bmod y \land x - y \geq 0 \land y > 0\} \text{Regel (6) (2) } \{P[x \leftarrow x - y]\}$$

```
    x := x - y
```

$$\{m \bmod n = x \bmod y \land x \geq 0 \land y > 0\} \hfill \text{Regel (5) } \{I\}$$

```
od;
```

$$\{x < y \land m \bmod n = x \bmod y \land x \geq 0 \land y > 0\} \hfill \text{Regel (3) (5) } \{\neg B \land I\}$$
$$\Rightarrow \{x = m \bmod n\} \hfill \text{Regel (6) (2) } \{P[erg \leftarrow x]\}$$

```
erg := x
```

$$\{erg = m \bmod n\} \hfill \{Q\}$$

Terminierung: $t = x - y$

1. $\{\textcolor{magenta}{x \geq y} \wedge \ldots \wedge x \geq 0 \wedge y > 0\} \Rightarrow x - y \geq 0$ $\qquad$ $\textcolor{blue}{\text{Regel (7) } B \wedge I \Rightarrow x - y \geq 0}$

2. ```
while x >= y do
```
$\qquad\{\ldots \wedge y > 0 \wedge (x - y = m)\}$ $\qquad$ $\textcolor{blue}{\text{Regel (7) } \{B \wedge I \wedge (t = m)\}}$
$\qquad\Rightarrow \{\ldots \wedge (\textcolor{cyan}{x - y} - y < m)\}$ $\qquad$ $\textcolor{blue}{\text{Regel (6) (2) } \{P[x \leftarrow x - y]\}}$
$\qquad$ ```x := x - y```
$\qquad\{\ldots \wedge (x - y < m)\}$ $\qquad$ $\textcolor{blue}{\text{Regel (7) } \{I \wedge (t < m)\}}$
```
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:
$$\frac{\{B \wedge P\}\, S_1\, \{Q\} \quad \{\neg B \wedge P\}\, S_2\, \{Q\}}{\{P\}\ \text{if } B \text{ then } S_1 \text{ else } S_2 \text{ fi}\ \{Q\}}$$

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

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

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

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.