Aufgabe 1-1

Gegeben sei folgendes Programmstück `S`:

```
tmp := x;
x   := y;
y   := tmp;
```

Überprüfen Sie durch Anwenden entsprechender Regeln des HOARE-Kalküls die Zusicherung

$$\{x = x_0 \wedge y = y_0\} \;\; \mathtt{S} \;\; \{x = y_0 \wedge y = x_0\}$$

Lösungsvorschlag zu 1-1

Das Programmstück `S` besteht aus einer Folge von Zuweisungen. Dementsprechend sind folgende zwei Ableitungsregeln in `S` zur Überprüfung der Zusicherung anzuwenden:

$$\text{[Zuweisung]} \qquad \{P[x \leftarrow e]\}\, \mathtt{x\ :=\ e}\, \{P\}$$

$$\text{[sequentielle Komposition]} \qquad \frac{\{P\}\,\mathtt{S1}\,\{R\} \quad \{R\}\,\mathtt{S2}\,\{Q\}}{\{P\}\,\mathtt{S1;S2}\,\{Q\}}.$$

Die Ableitung für `S` ist dann, bei impliziter Anwendung der sequentiellen Komposition in den Schritten (2) und (3), wie folgt:

$$\begin{array}{rll}
 & \{x = x_0 \wedge y = y_0\} & \\
\mathtt{tmp\ :=\ x;} & \text{[Zuweisung]} & (1) \\
 & \{x = x_0 \wedge y = y_0 \wedge tmp = x_0\} & \\
\mathtt{x\ :=\ y;} & \text{[Zuweisung]} & (2) \\
 & \{y = y_0 \wedge tmp = x_0 \wedge x = y_0\} & \\
\mathtt{y\ :=\ tmp;} & \text{[Zuweisung]} & (3) \\
 & \{tmp = x_0 \wedge x = y_0 \wedge y = x_0\} = Q_1 &
\end{array}$$

Mit Hilfe der Folgerung– oder Abschwächungsregel und $Q_1 \Longrightarrow Q$ läßt sich zeigen, daß $\{P\}\,\mathtt{S}\,\{Q\}$ gilt:

$$\text{[Abschwächung]} \qquad \frac{P \Longrightarrow P_1 \quad \{P_1\}\,\mathtt{S}\,\{Q_1\} \quad Q_1 \Longrightarrow Q}{\{P\}\,\mathtt{S}\,\{Q\}}.$$

Aufgabe 1-2

Überprüfen Sie die Zusicherung $\{-2 \leq y \leq -1\}$ `S` $\{y > 0\}$ für das folgende Programmstück `S`:

```
x := -y;
IF x >= 5 THEN y := x + y
          ELSE y := x - y
END;
```

Lösungsvorschlag zu 1-2

Die `IF-THEN-ELSE` Ableitungsregel lautet:

$$[\text{bedingte Anweisung}] \qquad \frac{\{P \wedge C\}\,\mathtt{S}_1\,\{Q\} \quad \{P \wedge \neg C\}\,\mathtt{S}_2\,\{Q\}}{\{P\}\,\mathtt{IF}\ C\ \mathtt{THEN}\ \mathtt{S}_1\ \mathtt{ELSE}\ \mathtt{S}_2\,\{Q\}}.$$

Die Ableitung für `S` ist dann bei Anwendung der Regeln für Zuweisung und bedingter Anweisung wie folgt (die sequentielle Komposition wird hier implizit angewendet):

$$\begin{array}{rl}
 & \{-2 \leq y \leq -1\} \\
\texttt{x := -y;} & [\text{Zuweisung}] \\
 & \{-2 \leq y \leq -1 \wedge 2 \geq x \geq 1\} \\
\texttt{IF x >= 5 THEN y := x + y} & \\
\texttt{ELSE y := x - y} & [\text{bedingte Anweisung}] \\
\texttt{END;} & \\
\text{Fall 1}\,(x >= 5): & \{-2 \leq y \leq -1 \wedge \underbrace{2 \geq x \geq 1 \wedge x >= 5}_{\text{FALSE}}\} \\
 & = \text{FALSE} \\
\text{Fall 2}\,(x < 5): & \{-2 \leq y \leq -1 \wedge 2 \geq x \geq 1 \wedge x < 5\} \\
\texttt{y := x - y} & [\text{Zuweisung}] \\
 & \{-2 \leq x - y \leq -1 \wedge 2 \geq x \geq 1 \wedge x < 5\} \\
 & = \{-2 - x \leq -y \leq -1 - x \wedge 2 \geq x \geq 1 \wedge x < 5\} \\
 & = \{2 + x \geq y \geq 1 + x \wedge 2 \geq x \geq 1 \wedge x < 5\} \\
 & = \{2 + x \geq y \geq 1 + x \wedge 3 \geq 1 + x \geq 2 \wedge x < 5\} \\
 & = \{2 + x \geq y \geq 1 + x \geq 2 \wedge 3 \geq 1 + x \geq 2 \wedge x < 5\} \\
 & = Q_1
\end{array}$$

Mit Hilfe der Abschwächungsregel und $Q_1 \Longrightarrow Q$ läßt sich zeigen, daß $\{P\}\,\mathtt{S}\,\{Q\}$ gilt.

Aufgabe 1-3

Gegeben sei folgendes Programmstück `S` zur ganzzahligen Division:

```
a := 0;
b := x;
WHILE b >= y DO BEGIN
  b := b - y;
  a := a + 1
END;
```

Zeigen Sie mit Hilfe des Hoare-Kalküls die Gültigkeit der Zusicherung

$$\{x \geq 0\} \;\; \texttt{S} \;\; \{ay + b = x \wedge 0 \leq b < y\}$$

Lösungsvorschlag zu 1-3

Die Ableitung für `S` ist bei impliziter Anwendung der Abschwächungsregel wie folgt:

$\{x \geq 0\}$	
`a:=0`	[Zuweisung]
	$\{ay + x = x \wedge x \geq 0\}$ da
	$\{0y + x = x \wedge x \geq 0\} = \{x \geq 0\}$
$\{ay + x = x \wedge x \geq 0\}$	
`b:=x`	[Zuweisung]
	$\{ay + b = x \wedge b \geq 0\}$ und
	$x \geq 0 \wedge y \geq 0 \Longrightarrow x \geq 0$
$\{x \geq 0 \wedge y \geq 0\}$	
`a:=0; b:=x`	[Komposition]
	$\{ay + b = x \wedge b \geq 0\}$
$\{(a+1)y + (b-y) = x \wedge b \geq 0\}$	
`b:=b-y`	[Zuweisung]
	$\{(a+1)y + b = x \wedge b \geq 0\}$
$\{(a+1)y + b = x \wedge b \geq 0\}$	
a:=a+1	[Zuweisung]
	$\{ay + b = x \wedge b \geq 0\}$
	$ay + b = x \wedge b \geq 0 \wedge b \geq y$
	$\Longrightarrow (a+1)y + (b-y) = x \wedge b - y \geq 0$
$\{ay + b = x \wedge b \geq 0 \wedge b \geq y\}$	

`b:=b-y; a:=a+1`	[Komposition]
	$\{ay + b = x \land b \geq 0\}$ (Schleifeninvariante)
$\{ay + b = x \land b \geq 0\}$	
`while b≥y do`	
`b:=b-y; a:=a+1`	[While–Schleife]
	$\{ay + b = x \land b \geq 0 \land b < y\}$ da $\neg b \geq y = b < y$
$\{x \geq 0 \land y \geq 0\}$	
`S`	[Komposition]
	$\{ay + b = x \land 0 \leq b < y\}$

Damit ist die Zusicherung bewiesen.

Aufgabe 1-4

Wie könnte man im HOARE-Kalkül eine Ableitungsregel für die `REPEAT-UNTIL`-Schleife formulieren? (**Hinweis:** Orientieren Sie sich an der Regel für die `WHILE`-Schleife.)

Lösungsvorschlag zu 1-4

Die Ableitungsregel für `WHILE`–Schleifen lautet:

$$\text{[While–Schleife]} \qquad \frac{\{P \wedge B\}\,\mathtt{S}\,\{P\}}{\{P\}\,\mathtt{WHILE}\ B\ \mathtt{DO}\ \mathtt{S}\ \{P \wedge \neg B\}}.$$

Die Anweisung `REPEAT S UNTIL` E kann durch folgende simuliert werden:
`S; WHILE` $\neg E$ `DO S`.

Die `REPEAT`–Schleife läßt sich damit wie folgt ausdrücken:

$$\text{(Repeat als While–Schleife)} \qquad \frac{\{P\}\,\mathtt{S}\,\{Q\} \quad \{Q\}\,\mathtt{WHILE}\ \neg B\ \mathtt{DO}\ \mathtt{S}\,\{Q \wedge B\}}{\{P\}\,\mathtt{REPEAT}\ \mathtt{S}\ \mathtt{UNTIL}\ B\,\{Q \wedge B\}}$$

Durch Anwendung der While–Ableitungsregel folgt:

$$\text{(Anwendung der While–Ableitung)} \qquad \frac{\{P\}\,\mathtt{S}\,\{Q\} \quad \dfrac{\{Q \wedge \neg B\}\,\mathtt{S}\,\{Q\}}{\{Q\}\,\mathtt{WHILE}\ \neg B\ \mathtt{DO}\ \mathtt{S}\,\{Q \wedge B\}}}{\{P\}\,\mathtt{REPEAT}\ \mathtt{S}\ \mathtt{UNTIL}\ B\,\{Q \wedge B\}}$$

Mit Hilfe einer Abschwächung von $\{Q \wedge \neg B\}$ ergibt sich folgendes:

$$\text{(Abschwächung)} \qquad \frac{\{P\}\,\mathtt{S}\,\{Q\} \quad \dfrac{\dfrac{Q \wedge \neg B \Longrightarrow P \quad \{P\}\,\mathtt{S}\,\{Q\}}{\{Q \wedge \neg B\}\,\mathtt{S}\,\{Q\}}}{\{Q\}\,\mathtt{WHILE}\ \neg B\ \mathtt{DO}\ \mathtt{S}\,\{Q \wedge B\}}}{\{P\}\,\mathtt{REPEAT}\ \mathtt{S}\ \mathtt{UNTIL}\ B\,\{Q \wedge B\}}$$

Letztendlich ist also:

$$\text{[Repeat–Schleife]} \qquad \frac{\{P\}\,\mathtt{S}\,\{Q\} \quad Q \wedge \neg B \Longrightarrow P}{\{P\}\,\mathtt{REPEAT}\ \mathtt{S}\ \mathtt{UNTIL}\ B\,\{Q \wedge B\}}$$