

## Aufgabe 5 (Check-Up)

Sie dürfen im Folgenden davon ausgehen, dass keinerlei Under- oder Overflows auftreten.

Gegeben sei die folgende Methode mit Vorbedingung  $P := x \geq 0 \wedge y \geq 0$  und Nachbedingung  $Q := x \cdot y = z$ .

```
1  int mul (int x , int y) {  
2      /* P */  
3      int z = 0, i = 0;  
4      while (i++ != x)  
5          z += y;  
6      /* Q */  
7      return z;  
8  }
```

Betrachten Sie dazu die folgenden drei Prädikate:

- $I_1 := z + i \cdot y = x \cdot y$
- $I_2 := \text{false}$
- $I_3 := z + (x - i) \cdot y = x \cdot y$

- (a) Beweisen Sie formal für jedes der drei Prädikate, ob es unmittelbar vor Betreten der Schleife in `mul` gilt oder nicht.

$$\begin{aligned} \text{wp}(\text{"Code vor der Schleife"}, I_1) &\equiv \text{wp}(\text{"int z = 0, i = 0;"}, z + i \cdot y = x \cdot y) \\ &\equiv \text{wp}(\text{"", } 0 + 0 \cdot y = x \cdot y) \\ &\equiv 0 = x \cdot y \\ &\equiv \text{falsch} \end{aligned}$$

$$\begin{aligned} \text{wp}(\text{"Code vor der Schleife"}, I_2) &\equiv \text{wp}(\text{"int z = 0, i = 0;"}, \text{false}) \\ &\equiv \text{wp}(\text{"", false}) \\ &\equiv \text{false} \\ &\equiv \text{falsch} \end{aligned}$$

$$\begin{aligned}
\text{wp}(\text{"Code vor der Schleife"}, I_3) &\equiv \text{wp}(\text{"int } z = 0, i = 0; ", z + (x - i) \cdot y = x \cdot y) \\
&\equiv \text{wp}("", 0 + (x - 0) \cdot y = x \cdot y) \\
&\equiv x \cdot y = x \cdot y \\
&\equiv \text{wahr}
\end{aligned}$$

- (b) Weisen Sie formal nach, welche der drei Prädikate Invarianten des Schleifenrumpfs in `mul` sind oder welche nicht.

Für den Nachweis muss der Code etwas umformuliert werden:

```

1  int mul (int x , int y) {
2      /* P */
3      int z = 0, i = 0;
4      while (i != x) {
5          i = i + 1;
6          z = z + y;
7      }
8      /* Q */
9      return z;
10 }
```

$$\begin{aligned}
\text{wp}(\text{"Code Schleife"}, I_1 \wedge i \neq x) &\equiv \text{wp}("i = i + 1; z = z + y;", z + i \cdot y = x \cdot y \wedge i \neq x) \\
&\equiv \text{wp}("i = i + 1;", z + y + i \cdot y = x \cdot y \wedge i \neq x) \\
&\equiv \text{wp}("", z + y + (i + 1) \cdot y = x \cdot y \wedge i + 1 \neq x) \\
&\equiv z + y + (i + 1) \cdot y = x \cdot y \wedge i + 1 \neq x \\
&\equiv z + i \cdot y + 2 \cdot y = x \cdot y \wedge i + 1 \neq x \\
&\equiv \text{falsch} \wedge i + 1 \neq x \\
&\equiv \text{falsch}
\end{aligned}$$

$$\begin{aligned}
\text{wp}(\text{"Code Schleife"}, I_2 \wedge i \neq x) &\equiv \text{wp}("i = i + 1; z = z + y;", \text{false} \wedge i \neq x) \\
&\equiv \text{wp}("", \text{false} \wedge i \neq x) \\
&\equiv \text{falsch} \wedge i \neq x \\
&\equiv \text{falsch}
\end{aligned}$$

$$\begin{aligned}
\text{wp}(\text{"Code Schleife"}, I_3 \wedge i \neq x) &\equiv \text{wp}(\text{"i = i + 1; z = z + y;"}, z + (x - i) \cdot y = x \cdot y \wedge i \neq x) \\
&\equiv \text{wp}(\text{"i = i + 1;"}, z + y + (x - i) \cdot y = x \cdot y \wedge i \neq x) \\
&\equiv \text{wp}(\text{"", } z + y + (x - i + 1) \cdot y = x \cdot y \wedge i + 1 \neq x) \\
&\equiv z + y + x \cdot y - i \cdot y + y = x \cdot y \wedge i + 1 \neq x \\
&\equiv z + 2 \cdot y + x \cdot y - i \cdot y = x \cdot y \wedge i + 1 \neq x \\
&\equiv \text{wahr}
\end{aligned}$$

- (c) Beweisen Sie formal, aus welchen der drei Prädikate die Nachbedingung gefolgert werden darf bzw. nicht gefolgert werden kann.

$$I_1 := z + i \cdot y = x \cdot y \quad I_2 := \text{false} \quad I_3 := z + (x - i) \cdot y = x \cdot y$$

$$\begin{aligned}
\text{wp}(\text{"Code nach Schleife"}, I_1 \wedge i = x) &\equiv \text{wp}(\text{"", } z + i \cdot y = x \cdot y \wedge i = x) \\
&\equiv z + i \cdot y = x \cdot y \wedge i = x \\
&\equiv z + x \cdot y = x \cdot y \\
&\neq Q
\end{aligned}$$

$$\begin{aligned}
\text{wp}(\text{"Code nach Schleife"}, I_2 \wedge i = x) &\equiv \text{wp}(\text{"", } \text{false} \wedge i = x) \\
&\equiv \text{false} \wedge i = x \\
&\equiv \text{falsch} \\
&\neq Q
\end{aligned}$$

$$\begin{aligned}
\text{wp}(\text{"Code nach Schleife"}, I_3 \wedge i = x) &\equiv \text{wp}(\text{"", } z + (x - i) \cdot y = x \cdot y \wedge i = x) \\
&\equiv z + (x - i) \cdot y = x \cdot y \wedge i = x \\
&\equiv z + (x - x) \cdot y = x \cdot y \\
&\equiv z + 0 \cdot y = x \cdot y \\
&\equiv z + 0 = x \cdot y \\
&\equiv z = x \cdot y \\
&\equiv Q
\end{aligned}$$

- (d) Skizzieren Sie den Beweis der totalen Korrektheit der Methode `mul`. Zeigen Sie dazu auch die Terminierung der Methode.

Aus den Teilaufgaben folgt der Beweis der partiellen Korrektheit mit Hilfe der Invariante  $i_3$ .  $i$  steigt streng monoton von 0 an so lange gilt

$i \neq x$ .  $i = x$  ist die Abbruchbedingung für die bedingte Wiederholung. Dann terminiert die Methode. Die Methode `mul` ist also total korrekt.