Aufgabe 5 (Check-Up)

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

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

```
int mul (int x , int y) {
    /* P */
    int z = 0, i = 0;
    while (i++ != x)
    z += y;
    /* Q */
    return z;
}
```

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;", false}) \\ & \equiv \text{wp}(\text{"", false}) \\ & \equiv \text{false} \\ & \equiv \text{falsch} \end{aligned}
```

```
\begin{aligned} \text{wp("Code vor der Schleife", } I_3) &\equiv \text{wp("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 ${\tt mul}$ sind oder welche nicht.

```
Für den Nachweis muss der Code etwas umformuliert werden:
     int mul (int x , int y) {
        /* P */
       int z = 0, i = 0;
        while (i != x) {
          i = i + 1;
          z = z + y;
7
        /* Q */
       return z;
     wp("\texttt{Code Schleife"}, I_1 \land i \neq x) \equiv wp("\texttt{i=i+1}; \texttt{z=z+y};", \texttt{z}+i \cdot \texttt{y} = \texttt{x} \cdot \texttt{y} \land i \neq \texttt{x})
                                                 \equiv \operatorname{wp}("i = i + 1;", z + y + i \cdot y = x \cdot y \land i \neq x)
                                                 \equiv \operatorname{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 falsch \wedge i + 1 \neq x
                                                 \equiv falsch
     wp("Code Schleife", I_2 \land i \neq x) \equiv wp("i = i + 1; z = z + y;", false \land i \neq x)
                                                 \equiv wp("", false \land i \neq x)
                                                 \equiv falsch \land i \neq x
                                                 \equiv falsch
```

```
\begin{split} \operatorname{wp}(\text{"code Schleife"},\,I_3 \wedge i \neq x) &\equiv \operatorname{wp}(\text{"i = i + 1; z = z + y;"},\,z + (x - i) \cdot y = x \cdot y \wedge i \neq x) \\ &\equiv \operatorname{wp}(\text{"i = i + 1;"},\,z + y + (x - i) \cdot y = x \cdot y \wedge i \neq x) \\ &\equiv \operatorname{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 \operatorname{wahr} \end{split}
```

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

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

$$\text{wp("Code nach Schleife", } I_1 \wedge i = x) \equiv \text{wp("", } z + i \cdot y = x \cdot y \wedge i = x)$$

$$\equiv z + i \cdot y = x \cdot y \wedge i = x$$

$$\equiv z + x \cdot y = x \cdot y$$

$$\neq Q$$

$$\text{wp("Code nach Schleife", } I_2 \wedge i = x) \equiv \text{wp("", } \text{false } \wedge i = x)$$

$$\equiv \text{false } \wedge i = x$$

$$\equiv \text{falsch}$$

$$\neq Q$$

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

$$\equiv z + (x - i) \cdot y = x \cdot y \wedge i = x$$

$$\equiv z + (x - x) \cdot y = x \cdot y$$

$$\equiv z + 0 \cdot y = x \cdot y$$

$$\equiv z + 0 \cdot x \cdot y$$

$$\equiv z = x \cdot y$$

$$\equiv Q$$

(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.