66116 / 2017 / Frühjahr

Thema 2 / Teilaufgabe 2 / Aufgabe 4 *(wp-Kalkül mit Invariante bei Methode „mul()“)*

Stichwörter: wp-Kalkül, Invariante, Totale Korrektheit

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:

- $I_1 := z + i \cdot y = x \cdot y$
- $I_2 :=$ 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.

Lösungsvorschlag

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

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

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

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

Lösungsvorschlag

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;
  }
  /* Q */
  return z;
}
```

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

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

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

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

Lösungsvorschlag

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

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

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

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

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

Lösungsvorschlag

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.