Verifikation nach dem Hoare-Kalkül — ein Beispiel

Christoph Lüth, 27.06.01

Gegeben seien `int x, int y` und folgendes Codefragment, welches den ganzzahligen Teiler von `x` und `y` berechnet:

```
int r= x;
int q= 0;
while (r >= y) {
  r= r-y;
  q= q+1;
  }
```

Zu zeigen:

1. Partielle Korrektheit.
2. Termination.

Notation

Die geltenden Zusicherungen werden an das Programm annotiert. Dabei können wir die Sequenzregel und die Konsequenzregel implizit anwenden, indem wir zum Beispiel schreiben:

$\backslash\backslash\ \{P\}$
`r`
$\backslash\backslash\ \{Q\}$
$\backslash\backslash\ \{Q'\}$ (wenn $Q \Rightarrow Q'$ gilt)
`s`
$\backslash\backslash\ \{R\}$

Implizit heißt hier, dass uns die Sequenzregel erlaubt, wenn $\{P\}$`r`$\{Q\}$ und $\{Q\}$`s`$\{R\}$ gilt, daraus $\{P\}$`r; s`$\{R\}$ zu schliessen, d.h. in der Darstellung oben, dass nach allen Schritten (und nicht nur nach dem letzten) auch R gilt. Die Konsequenzregel erlaubt es, die Zusicherungen beliebig abzuschwächen, oder logisch äquivalent umzuformen, also oben Q durch Q' zu ersetzen, *wenn Q nach den Regeln der formalen Logik Q' impliziert, also $Q \Rightarrow Q'$ gilt.* Die Regeln der formalen Logik umfassen hier elementare Arithmetik (also z.B. $x + 0 = x$), die Möglichkeit, einzelne Vorbedingungen wegzulassen, da $A \wedge B \Rightarrow B$ gilt, und wahre Aussagen hinzuzufügen (z.B. $0 = 0$).

Bei der Zuweisungsregel wird der Teil in der Vorbedingung annotiert, der nach der Zuweisung ersetzt wird. Beispiel:

$\backslash\backslash\ \{x = 2\}$
$\backslash\backslash\ \{\underline{x+1} = 3\}$ (weil $2 + 1 = 3$)
`x= x+1`
$\backslash\backslash\ \{x = 3\}$

1. Partielle Korrektheit

Zuerst müssen wir die Anforderung spezifizieren: der ganzzahlige Teiler von x und y sind zwei Zahlen q, r so dass

$$x = q \cdot y + r \wedge 0 \leq r \wedge r < y \tag{1}$$

Als Anfangsbedingung nehmen wir an, dass $x \geq 0, y > 0$ gilt.

$\backslash\backslash\ \{x \geq 0 \wedge y > 0\}$ (Annahme)
$\backslash\backslash\ \{x = \underline{x} \wedge \underline{x} \geq 0 \wedge y > 0\}$ ($x = x$ gilt immer)
`r= x;`
$\backslash\backslash\ \{x = r \wedge r \geq 0 \wedge y > 0 \wedge \underline{0} = 0\}$ ($0 = 0$ gilt immer)
`q= 0;`
$\backslash\backslash\ \{x = r \wedge r \geq 0 \wedge y > 0 \wedge q = 0\}$
$\backslash\backslash\ \{x = q \cdot y + r \wedge r \geq 0\}$
(mit $q = 0$ folgt $q \cdot y + r = r$; die Vorbedingung $y \geq 0$ kann entfallen)
`while (r >= y) {`
Anwendung der Schleifenregel:
die Schleifeninvariante ist $P \equiv x \cdot y + r \wedge r \geq 0$;
die Abbruchbedingung $b \equiv r \geq y$
$\backslash\backslash\ \{x = q \cdot y + r \wedge r \geq 0 \wedge r \geq y\}$
$\backslash\backslash\ \{x = (q+1) \cdot y + \underline{r - y} \wedge \underline{r - y} \geq 0\}$
(mit Gleichungen (2) und (3) unten;
die Vorbedingung $r \geq 0$ kann entfallen)
`r= r-y;`
$\backslash\backslash\ \{x = (\underline{q+1}) \cdot y + r \wedge r \geq 0\}$
`q= q+1;`
$\backslash\backslash\ \{x = q \cdot y + r \wedge r \geq 0\}$
`}`
$\backslash\backslash\ \{x = q \cdot y + r \wedge r \geq 0 \wedge \neg(r \geq y)\}$
$\backslash\backslash\ \{x = q \cdot y + r \wedge 0 \leq r \wedge r < y\}$ (mit $\neg(r \geq y) r \Leftrightarrow r < y$, und $r \geq 0 \Leftrightarrow 0 \leq r$)

□

Hierbei haben wir folgende Gleichungen benutzt:

$$q \cdot y + r = (q+1) \cdot y + r - y \tag{2}$$

Gilt wegen $q \cdot y + r = q \cdot y + y - y + r = (q+1) \cdot y + r - y$.

$$r \geq y \Leftrightarrow r - y \geq 0 \tag{3}$$

Beweis durch Subtraktion von y auf beiden Seiten links.

2. Termination

$\backslash\backslash\ \{y > 0\}$ (Annahme)

```
x= r;
q= 0;
```

$\backslash\backslash\ \{y > 0\}$

```
while (r >= y) {
```

Wir setzen $T \stackrel{def}{=} r$ und $t \stackrel{def}{=} r$

$\backslash\backslash\ \{y > 0 \wedge T = r\}$

$\backslash\backslash\ \{y > 0 \wedge T - y = \underline{r - y}\}$

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

$\backslash\backslash\ \{y > 0 \wedge T - y = r\}$

$\backslash\backslash\ \{y > 0 \wedge T = r + y\}$

```
q= q+1;
```

$\backslash\backslash\ \{y > 0 \wedge T = r + y\}$ (*)

```
}
```

Es bleibt zu zeigen:

- Nach dem Schleifendurchlauf gilt $t < T$:

  Nach Definition ist $t = r$, und nach dem Schleifendurchlauf ist oben (an der Stelle (*)) $T = r + y$. Ferner gilt $r < r + y$ wegen $y > 0$, also folgt

  $$t = r < r + y = T$$

  Man beachte, dass diese Ungleichung *nach* dem Schleifendurchlauf gelten muß. In T merken wir uns den Wert von r, und damit von t, vor dem Schleifendurchlauf. Dieser Wert ändert sich nicht, sondern nur der von r, und damit von t.

- Vor dem Schleifendurchlauf gilt $y > 0 \wedge r \geq y \Rightarrow t \geq 0$

  Aus $y > 0, r \geq y$, folgt $r > 0$, also (mit $t = r$) $t \geq 0$.

□