

Verifikation nach dem Hoare-Kalkül — ein Beispiel

Christoph Lüth, 21.04.16

Notation

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

```
// {P}
r
// {Q}
// {Q'} (wenn  $Q \Rightarrow Q'$  gilt)
s
// {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:

```
// {x = 2}
// {x + 1 = 3}    (weil  $2 + 1 = 3$ )
x= x+1
// {x = 3}
```

Beispiel: Ganzzahliger Teiler

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

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

Wir zeigen partielle Korrektheit.

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

$$x = q \cdot y + r \wedge 0 \leq r \wedge r < y \quad (1)$$

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

```
// {x ≥ 0 ∧ y > 0} (Annahme)
// {x = x ∧ x ≥ 0 ∧ y > 0}
r = x;
// {x = r ∧ r ≥ 0 ∧ y > 0 ∧ q = 0}
q = 0;
// {x = r ∧ r ≥ 0 ∧ y > 0 ∧ q = 0}
// {x = q · y + r ∧ r ≥ 0} (wegen q = 0 ist r = q · y + r; y > 0 kann entfallen)
while (r >= y) {
    // {x = q · y + r ∧ r ≥ 0 ∧ r ≥ y}
    // {x = (q + 1) · y + r - y ∧ r - y ≥ 0} (mit Gleichungen (2) und (3) unten)
    r = r - y;
    // {x = (q + 1) · y + r ∧ r ≥ 0}
    q = q + 1;
    // {x = q · y + r ∧ r ≥ 0}
}
// {x = q · y + r ∧ r ≥ 0 ∧ ¬(r ≥ y)}
// {x = q · y + r ∧ 0 ≤ r ∧ r < y} (mit ¬(r ≥ y)r ⇔ r < y, und r ≥ 0 ⇔ 0 ≤ r)
```

□

Hierbei haben wir folgende Gleichungen benutzt:

$$q \cdot y + r = (q + 1) \cdot y + r - y \quad (2)$$

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

$$r \geq y \Leftrightarrow r - y \geq 0 \quad (3)$$

Beweis durch Subtraktion von y auf beiden Seiten links.