TECHNISCHE UNIVERSITÄT DRESDEN

PROGRAMMIERUNG

Übung 12: Hoare-Kalkül

Eric Kunze
eric.kunze@mailbox.tu-dresden.de

TU Dresden, 05. Juli 2019

HOARE-Kalkül

- Beweis / Verifikation von Programmeigenschaften
- Verifikationsformeln der Form $\{P\}\mathbf{A}\{Q\}$
  - P und Q sind Zusicherungen (prädikatenlogische Ausdrücke)
  - P heißt **Vorbedingung**, Q heißt **Nachbedingung**
  - Beschreibung der Veränderung von Zusicherungen
  - **Bedeutung**: Wenn die Variablenwerte vor Ausführung von $\mathbf{A}$ die Zusicherung P erfüllen und $\mathbf{A}$ terminiert, dann erfüllen die Variablen nach Ausführung von $\mathbf{A}$ die Zusicherung Q
- Aufstellen eines Beweisbaumes mit zur Verfügung stehenden Regeln

HOARE-Kalkül – Regeln

- Zuweisungsaxiom
- Sequenzregel
- CompRegel
- Iterationsregel
- (erste und zweite) Alternativregel
- Konsequenzregeln
  - stärkere Vorbedingung
  - schwächere Nachbedingung

Schleifeninvariante

Für die Iterationsregel benötigen wir die Schleifeninvariante SI. In den meisten unserer Fälle ist diese von der Form $SI = A \land B$, wobei

- A den Zusammenhang zwischen Zählvariable und Akkumulationsvariablen beschreibt. Führe dazu einige Iterationen der Schleife durch und leite daraus einen Zusammenhang her.
- B die abgeschwächte Schleifenbedingung ist. Dabei nehmen wir die letztmögliche Variablenbelegung, für die die Schleifenbedingung π noch wahr ist und führen den Schleifenrumpf noch einmal darauf aus ($\rightarrow \pi'$).
  $\Rightarrow B = \pi \cup \pi'$.

Aufgabe 1

Verfikationsformel:

$\{(x \geq 0) \wedge (x = x1) \wedge (z = 0) \wedge (y \geq 0)\}$ `while (x1 > 0) {x1 = x1-1; z = z+y;}` $\{(z = y \cdot x)\}$

Schleifeninvariante:

#	x1	z
0	x	0
1	$x-1$	y
2	$x-2$	$2y$
N	$x-N$	Ny

`x1 = x - N`
`z = N * y`

$\Rightarrow A = ($`z = (x-x1) * y`$)$

abgeschwächte Schleifenbedingung:

- Schleifenbedingung $\pi = ($`x1 > 0`$)$
- Schleifenbedingung letztmalig wahr für `x1 = 1`
- Wert nach nochmaligem Schleifendurchlauf: $\pi' = ($`x1 = 0`$)$
- $B = \pi \cup \pi' = ($`x1` $\geq$ `0`$)$

$\Longrightarrow SI = A \wedge B = ($`z=(x-x1)*y`$) \wedge ($`x1` $\geq$ `0`$)$

Aufgabe 1

Verfikationsformel:

$\{(x \geq 0) \wedge (x = x1) \wedge (z = 0) \wedge (y \geq 0)\}$ `while (x1 > 0) {x1 = x1-1; z = z+y;}` $\{(z = y \cdot x)\}$

Sei $SI = A \wedge B =$ (`z=(x-x1)*y`) $\wedge$ (`x1` $\geq$ `0`) und $\pi =$ `x1 > 0`.

$$A = C = D = G = SI$$

$$B = SI \ \wedge \ \neg\pi = (\texttt{z=(x-x1)*y}) \ \wedge \ (\texttt{x1} \geq \texttt{0}) \ \wedge \ \neg(\texttt{x1 > 0})$$

$$E = SI \ \wedge \ \pi = (\texttt{z=(x-x1)*y}) \ \wedge \ (\texttt{x1} \geq \texttt{0}) \ \wedge \ (\texttt{x1 > 0})$$

Aufgabe 2

$$
\begin{aligned}
A &= \text{true} \ \wedge \ (y < 0) \\
B &= \text{true} \ \wedge \ \neg(y < 0) \\
C &= A \\
D &= A \\
E &= -(3 \cdot y) + 1 \geq 0 \\
F &= E
\end{aligned}
$$

$$
\begin{aligned}
G &= E \\
H &= -x + 1 \geq 0 \\
J &= H \\
K &= (y \geq 0) \\
L &= \text{stärkere Vorbedingung} \\
M &= \text{Sequenzregel}
\end{aligned}
$$

zu zeigen: true $\wedge \ (y < 0) \ \Rightarrow \ (-3 \cdot y + 1 \geq 0)$

$$
\begin{aligned}
\text{true} \ \wedge \ (y < 0) \ &\Rightarrow \quad y < 0 \\
&\Rightarrow \quad -3 \cdot y > 0 \\
&\Rightarrow \quad -3 \cdot y + 1 > 1 \\
&\Rightarrow \quad -3 \cdot y + 1 \geq 0
\end{aligned}
$$