Grundbegriffe der Informatik

Übung

Simon Wacker

Karlsruher Institut für Technologie

Wintersemester 2015/2016

Radler

Haben: Bierfass B, Limonadenfass L desselben Volumens

Wollen: Radler

Dazu: Wiederholen folgenden Prozess:

1. Schöpfen eine Kelle von B in L,
   rühren Gemisch in L perfekt um.
2. Schöpfen eine Kelle von L in B,
   rühren Gemisch in B perfekt um.

Am Ende: Verhältnis von Limonade in B zu Bier in L?

Invariante

Ganz am Anfang gilt

$$\text{Flüssigkeitsmenge in } B = \text{Gesamtmenge an Bier}$$

Flüssigkeitsmenge in B invariant

- das heißt, vor und nach jeder Iteration gleich

Gesamtmenge an Bier invariant

Zu Beginn und am Ende jeder Iteration gilt somit

$$\text{Flüssigkeitsmenge in } B = \text{Gesamtmenge an Bier}$$

Insbesondere am Ende des gesamten Vorgangs!

Verhältnis

Am Ende des gesamten Vorgangs gilt

$$\begin{aligned} &\text{Biermenge in } B \ + \ \text{Limonadenmenge in } B \\ &= \ \text{Flüssigkeitsmenge in } B \\ &= \ \text{Gesamtmenge an Bier} \\ &= \ \text{Biermenge in } B \ + \ \text{Biermenge in } L \end{aligned}$$

und folglich

$$\text{Limonadenmenge in } B \ = \ \text{Biermenge in } L$$

Verhältnis von Limonade in B zu Bier in L ist 1 zu 1

Übrigens: Bei unendlich vielen Iterationen perfekte 1 zu 1 Mischung in beiden Fässern

Schleifeninvariante

Schleife T

$$\textbf{while } B \textbf{ do } R \textbf{ od}$$

Formel I Schleifeninvariante für T gdw.

$$\{I \wedge B\}R\{I\}$$

gültiges Hoare-Tripel

In diesem Falle ist

$$\{I\}T\{I \wedge \neg B\}$$

gültiges Hoare-Tripel

Kombination von Regeln

Behauptung:

$$\{P\}$$
$$S$$
$$\textbf{while } B \textbf{ do}$$
$$\quad R$$
$$\textbf{od}$$
$$\{Q\}$$

gültig, wenn Formel I existiert so, dass

1. $\{P\}S\{I\}$ gültig
2. $\{I \land B\}R\{I\}$ gültig
3. $I \land \neg B \models Q$ wahr

Kombination von Regeln

Behauptung:

$\{P\}$

S

while B **do**

R

od

$\{Q\}$

gültig, wenn Formel I existiert so, dass

1. $\{P\}S\{I\}$ gültig
2. $\{I \wedge B\}R\{I\}$ gültig
3. $I \wedge \neg B \models Q$ wahr

Beweis: Gemäß der Schleifeninvariantenregel ist

$\{I\}$

while B **do**

R

od

$\{I \wedge \neg B\}$

gültig.

Kombination von Regeln

Behauptung:

$$\{P\}$$
$$S$$
$$\textbf{while } B \textbf{ do}$$
$$\quad R$$
$$\textbf{od}$$
$$\{Q\}$$

gültig, wenn Formel I existiert so, dass

1. $\{P\}S\{I\}$ gültig
2. $\{I \wedge B\}R\{I\}$ gültig
3. $I \wedge \neg B \models Q$ wahr

Beweis: Gemäß der Schleifeninvariantenregel ist

$$\{I\}$$
$$\textbf{while } B \textbf{ do}$$
$$\quad R$$
$$\textbf{od}$$
$$\{I \wedge \neg B\}$$

gültig. Aus der Sequenzenregel und der Abschwächungsregel folgt die Behauptung.

Fakultät

Behauptung:

$$
\begin{array}{l}
\{y \geq 0\} \\
z \leftarrow 1 \\
i \leftarrow 1 \\
\textbf{while } i \leq y \textbf{ do} \\
\qquad z \leftarrow z \cdot i \\
\qquad i \leftarrow i + 1 \\
\textbf{od} \\
\{z = y!\}
\end{array}
$$

ist gültig

Beweis: Es genügt für die Formel I

$$z = (i - 1)! \wedge i \leq y + 1$$

zu zeigen:

1. Hoare-Tripel

$$\{y \geq 0\} z \leftarrow 1; i \leftarrow 1 \{I\}$$

   ist gültig

2. Hoare-Tripel

$$\{I \wedge i \leq y\} z \leftarrow z \cdot i; i \leftarrow i + 1 \{I\}$$

   ist gültig

3. $I \wedge \neg(i \leq y) \models z = y!$

Fakultät — Vor Schleifeneintritt

Behauptung:

$$\{y \geq 0\}$$
$$z \leftarrow 1$$
$$i \leftarrow 1$$
$$\{z = (i-1)! \wedge i \leq y+1\}$$

ist gültig

Beweis: Nach Zuweisungsaxiom sind

$$\{z = 0! \wedge 1 \leq y+1\}$$
$$i \leftarrow 1$$
$$\{z = (i-1)! \wedge i \leq y+1\}$$

und

$$\{1 = 0! \wedge 1 \leq y+1\}$$
$$z \leftarrow 1$$
$$\{z = 0! \wedge 1 \leq y+1\}$$

gültig.

Fakultät — Vor Schleifeneintritt

Behauptung:

$$\{y \geq 0\}$$
$$z \leftarrow 1$$
$$i \leftarrow 1$$
$$\{z = (i-1)! \wedge i \leq y+1\}$$

ist gültig

Beweis: Nach Sequenzenregel ist

$$\{1 = 0! \wedge 1 \leq y+1\}$$
$$z \leftarrow 1$$
$$i \leftarrow 1$$
$$\{z = (i-1)! \wedge i \leq y+1\}$$

gültig.

Fakultät — Vor Schleifeneintritt

Behauptung:

$$\{y \geq 0\}$$
$$z \leftarrow 1$$
$$i \leftarrow 1$$
$$\{z = (i-1)! \land i \leq y+1\}$$

ist gültig

Beweis: Nach Sequenzenregel ist

$$\{1 = 0! \land 1 \leq y+1\}$$
$$z \leftarrow 1$$
$$i \leftarrow 1$$
$$\{z = (i-1)! \land i \leq y+1\}$$

gültig. Es gelten

$$1 = 0!$$

und

$$1 \leq y+1 \text{ gdw. } y \geq 0.$$

Fakultät — Vor Schleifeneintritt

Behauptung:

$$\{y \geq 0\}$$
$$z \leftarrow 1$$
$$i \leftarrow 1$$
$$\{z = (i-1)! \land i \leq y+1\}$$

ist gültig

Beweis: Nach Verstärkungsregel gilt Behauptung.

Fakultät — Schleifeninvariante

Behauptung:

$$\{z = (i-1)! \wedge i \leq y+1 \wedge i \leq y\}$$
$$z \leftarrow z \cdot i$$
$$i \leftarrow i+1$$
$$\{z = (i-1)! \wedge i \leq y+1\}$$

ist gültig

Beweis: Nach Zuweisungsaxiom sind

$$\{z = i! \wedge i+1 \leq y+1\}$$
$$i \leftarrow i+1$$
$$\{z = (i-1)! \wedge i \leq y+1\}$$

und

$$\{z \cdot i = i! \wedge i+1 \leq y+1\}$$
$$z \leftarrow z \cdot i$$
$$\{z = i! \wedge i+1 \leq y+1\}$$

gültig.

Fakultät — Schleifeninvariante

Behauptung:

$$\{z = (i-1)! \land i \leq y+1 \land i \leq y\}$$
$$z \leftarrow z \cdot i$$
$$i \leftarrow i+1$$
$$\{z = (i-1)! \land i \leq y+1\}$$

ist gültig

Beweis: Nach Sequenzenregel ist

$$\{z \cdot i = i! \land i+1 \leq y+1\}$$
$$z \leftarrow z \cdot i$$
$$i \leftarrow i+1$$
$$\{z = (i-1)! \land i \leq y+1\}$$

gültig.

Fakultät — Schleifeninvariante

Behauptung:

$$\{z = (i-1)! \wedge i \le y+1 \wedge i \le y\}$$
$$z \leftarrow z \cdot i$$
$$i \leftarrow i+1$$
$$\{z = (i-1)! \wedge i \le y+1\}$$

ist gültig

Beweis: Nach Sequenzenregel ist

$$\{z \cdot i = i! \wedge i+1 \le y+1\}$$
$$z \leftarrow z \cdot i$$
$$i \leftarrow i+1$$
$$\{z = (i-1)! \wedge i \le y+1\}$$

gültig. Es gelten

$$z \cdot i = i! \text{ gdw. } z = (i-1)!$$

und

$$\begin{aligned} i+1 \le y+1 &\text{ gdw. } i \le y \\ &\text{ gdw. } i \le y+1 \wedge i \le y. \end{aligned}$$

Fakultät — Schleifeninvariante

Behauptung:

$$\{z = (i-1)! \land i \leq y+1 \land i \leq y\}$$
$$z \leftarrow z \cdot i$$
$$i \leftarrow i+1$$
$$\{z = (i-1)! \land i \leq y+1\}$$

ist gültig

Beweis: Nach Verstärkungsregel gilt Behauptung.

Fakultät — Nach Schleifenaustritt

Behauptung:

$$z = (i-1)! \wedge i \leq y+1 \wedge \neg(i \leq y)$$

$$\models$$

$$z = y!$$

Beweis: Wegen

$$\begin{aligned} \neg(i \leq y) &\text{ gdw. } i > y \\ &\text{ gdw. } i \geq y+1, \end{aligned}$$

gilt

$$i \leq y+1 \wedge \neg(i \leq y) \text{ gdw. } i = y+1.$$

Damit gilt

$$\begin{aligned} &z = (i-1)! \wedge i \leq y+1 \wedge \neg(i \leq y) \\ &\text{gdw. } z = (i-1)! \wedge i = y+1 \\ &\text{gdw. } z = y! \wedge i = y+1. \end{aligned}$$

Schleifenvariante

Schleife T

$$\textbf{while } B \textbf{ do } R \textbf{ od}$$

Ganzzahliger arithmetischer Ausdruck V Schleifenvariante für T gdw.

- Für jedes $c \in \mathbb{Z}$ ist das Hoare-Tripel

$$\{V \geq 0 \land V = c \land B\}R\{V \geq 0 \land V \leq c - 1\}$$

  gültig

In diesem Falle gilt:
Wenn $V \geq 0$ vor Ausführung von T gilt,
dann terminiert T

- T wird höchstens n-mal durchlaufen,
- wobei n der Wert von V vor Ausführung von T sei

Beispiel

$$
\begin{array}{l}
z \leftarrow 1 \\
i \leftarrow 1 \\
\textbf{while } i \leq y \textbf{ do} \\
\qquad z \leftarrow z \cdot i \\
\qquad i \leftarrow i + 1 \\
\textbf{od}
\end{array}
$$

Eine Schleifenvariante ist $y + 1 - i$

Array und Formeln

Array a mit n ganzzahligen Einträgen

- $a[i]$ stehe für i-ten Eintrag

sorted($a[\xi, n-1]$) stehe für

$$\forall k \in \mathbb{Z}_n \; \forall \ell \in \mathbb{Z}_n : (\xi \leq k \leq \ell \rightarrow a[k] \leq a[\ell])$$

less_or_equal($a[0, \xi], a[\xi+1, n-1]$) stehe für

$$\forall k \in \mathbb{Z}_n \; \forall \ell \in \mathbb{Z}_n : (k \leq \xi < \ell \rightarrow a[k] \leq a[\ell])$$

less_or_equal($a[0, \xi-1], a[\xi]$) stehe für

$$\forall k \in \mathbb{Z}_n : (k \leq \xi - 1 \rightarrow a[k] \leq a[\xi])$$

Achtung

$$\{n \geq 0\}$$

$i \leftarrow 0$

while $i \leq n-1$ **do**

  $a[i] \leftarrow 0$

od

$$\{\text{sorted}(a[0, n-1])\}$$

ist gültiges Hoare-Tripel

Nach Ausführung eines Sortieralgorithmus soll

- Array (aufsteigend) sortiert sein
- Array genau die ursprünglichen Werte enthalten
  mit denselben Häufigkeiten

Erster Punkt ist einfach zu verifizieren

Zweiter Punkt ist schwierig zu verifizieren

Bubblesort

$$
\left.
\begin{array}{l}
i \leftarrow n - 1 \\
\textbf{while } i \geq 0 \textbf{ do} \\
\quad j \leftarrow 0 \\
\quad \left.\begin{array}{l}
\textbf{while } j \leq i - 1 \textbf{ do} \\
\quad \textbf{if } a[j] > a[j+1] \textbf{ do} \\
\quad\quad \left.\begin{array}{l}
x \leftarrow a[j] \\
a[j] \leftarrow a[j+1] \\
a[j+1] \leftarrow x
\end{array}\right\} \mathrm{swap}(a[j], a[j+1]) \\
\quad \textbf{fi} \\
\quad j \leftarrow j + 1 \\
\textbf{od}
\end{array}\right\} \mathrm{bubble\_to}(i) \\
\quad i \leftarrow i - 1 \\
\textbf{od}
\end{array}
\right.
$$

Partielle Korrektheit

$\{n \geq 0\}$

$i \leftarrow n - 1$

while $i \geq 0$ **do**

  $j \leftarrow 0$

  bubble_to(i)

  $i \leftarrow i - 1$

od

$\{\text{sorted}(a[0, n-1])\}$

Partielle Korrektheit

$\{n \geq 0\}$

$i \leftarrow n - 1$

while $i \geq 0$ **do**

  $j \leftarrow 0$

  $\text{bubble\_to}(i)$

  $i \leftarrow i - 1$

od

$\{\text{sorted}(a[0, n-1])\}$

Schleifeninvariante I raten

$\text{sorted}(a[i+1, n-1])$

$\land\ \text{less\_or\_equal}(a[0, i], a[i+1, n-1])$

$\land\ i \geq -1$

Partielle Korrektheit

$\{n \geq 0\}$

$i \leftarrow n - 1$

$\{I\}$

while $i \geq 0$ **do**

  $j \leftarrow 0$

  bubble_to(i)

  $i \leftarrow i - 1$

od

$\{I \land \neg(i \geq 0)\}$

$\{\text{sorted}(a[0, n-1])\}$

Schleifeninvariante I

$\text{sorted}(a[i+1, n-1])$
$\land\ \text{less\_or\_equal}(a[0, i], a[i+1, n-1])$
$\land\ i \geq -1$

- Oberes Hoare-Tripel ist gültig und $I \land \neg(i \geq 0) \models \text{sorted}(a[0, n-1])$
- *Ist I Schleifeninvariante*, so ist mittleres Hoare-Tripel gültig
- Gemäß Sequenzen- und Abschwächungsregel ist dann äußeres Hoare-Tripel gültig

Partielle Korrektheit

$\{I \wedge i \geq 0\}$

$j \leftarrow 0$

$\text{bubble\_to}(i)$

$i \leftarrow i - 1$

$\{I\}$

Schleifeninvariante I

$\text{sorted}(a[i+1, n-1])$

$\wedge \text{ less\_or\_equal}(a[0, i], a[i+1, n-1])$

$\wedge \; i \geq -1$

Code ausklappen

Partielle Korrektheit

$\{I \wedge i \geq 0\}$

$j \leftarrow 0$

while $j \leq i - 1$ **do**

  if $a[j] > a[j+1]$ **do**

    $\text{swap}(a[j], a[j+1])$

  fi

  $j \leftarrow j + 1$

od

$i \leftarrow i - 1$

$\{I\}$

Schleifeninvariante I

$\text{sorted}(a[i+1, n-1])$

$\wedge \text{ less\_or\_equal}(a[0, i], a[i+1, n-1])$

$\wedge\, i \geq -1$

Schleifeninvariante J raten

$\text{less\_or\_equal}(a[0, j-1], a[j])$

$\wedge\, j \leq i$

$\wedge\, I$

Partielle Korrektheit

$\{I \wedge i \geq 0\}$

$j \leftarrow 0$

$\{J\}$

while $j \leq i - 1$ **do**

  if $a[j] > a[j+1]$ **do**

    $\text{swap}(a[j], a[j+1])$

  fi

  $j \leftarrow j + 1$

od

$\{J \wedge \neg(j \leq i - 1)\}$

$i \leftarrow i - 1$

$\{I\}$

Schleifeninvariante I

$\text{sorted}(a[i+1, n-1])$

$\wedge \text{ less\_or\_equal}(a[0, i], a[i+1, n-1])$

$\wedge\ i \geq -1$

Schleifeninvariante J

$\text{less\_or\_equal}(a[0, j-1], a[j])$

$\wedge\ j \leq i$

$\wedge\ I$

- Oberes und unteres Hoare-Tripel ist gültig
- *Ist J Schleifeninvariante*, so ist mittleres Hoare-Tripel gültig
- Gemäß Sequenzen- und

Partielle Korrektheit

$\{J \land j \leq i - 1\}$

if $a[j] > a[j+1]$ **do**

  $\text{swap}(a[j], a[j+1])$

fi

$j \leftarrow j + 1$

$\{J\}$

Schleifeninvariante I

$\text{sorted}(a[i+1, n-1])$

$\land \text{less\_or\_equal}(a[0, i], a[i+1, n-1])$

$\land i \geq -1$

Schleifeninvariante J

$\text{less\_or\_equal}(a[0, j-1], a[j])$

$\land j \leq i$

$\land I$

Partielle Korrektheit

$\{J \wedge j \leq i - 1\}$

$\textbf{if } a[j] > a[j+1] \textbf{ do}$

$\quad \text{swap}(a[j], a[j+1])$

$\textbf{fi}$

$\{J[j/j+1]\}$

$j \leftarrow j + 1$

$\{J\}$

Schleifeninvariante I

$\text{sorted}(a[i+1, n-1])$

$\wedge \text{ less\_or\_equal}(a[0, i], a[i+1, n-1])$

$\wedge\, i \geq -1$

Schleifeninvariante J

$\text{less\_or\_equal}(a[0, j-1], a[j])$

$\wedge\, j \leq i$

$\wedge\, I$

- Unteres Hoare-Tripel ist gültig
- *Ist oberes Hoare-Tripel gültig*, so ist äußeres Hoare-Tripel gültig

Partielle Korrektheit

$\{J \land j \leq i - 1\}$

if $a[j] > a[j+1]$ **do**

  swap$(a[j], a[j+1])$

fi

$\{J[j/j+1]\}$

Schleifeninvariante I

$\text{sorted}(a[i+1, n-1])$
$\land \text{less\_or\_equal}(a[0, i], a[i+1, n-1])$
$\land i \geq -1$

Schleifeninvariante J

$\text{less\_or\_equal}(a[0, j-1], a[j])$
$\land j \leq i$
$\land I$

else-Teil ergänzen

Partielle Korrektheit

$\{J \wedge j \leq i - 1\}$

if $a[j] > a[j+1]$ **do**

  $\text{swap}(a[j], a[j+1])$

else

fi

$\{J[j/j+1]\}$

Schleifeninvariante I

$\text{sorted}(a[i+1, n-1])$
$\wedge \text{less\_or\_equal}(a[0, i], a[i+1, n-1])$
$\wedge i \geq -1$

Schleifeninvariante J

$\text{less\_or\_equal}(a[0, j-1], a[j])$
$\wedge j \leq i$
$\wedge I$

Formel $J[j/j+1]$

$\text{less\_or\_equal}(a[0, j], a[j+1]) \wedge j+1 \leq i \wedge$

Partielle Korrektheit

$\{J \wedge j \leq i - 1\}$

if $a[j] > a[j+1]$ **do**

$\{J \wedge j \leq i - 1 \wedge a[j] > a[j+1]\}$

swap$(a[j], a[j+1])$

$\{J[j/j+1]\}$

else

$\{J \wedge j \leq i - 1 \wedge \neg(a[j] > a[j+1])\}$

$\{J[j/j+1]\}$

fi

$\{J[j/j+1]\}$

Schleifeninvariante I

sorted$(a[i+1, n-1])$
$\wedge$ less_or_equal$(a[0, i], a[i+1, n-1])$
$\wedge\ i \geq -1$

Schleifeninvariante J

less_or_equal$(a[0, j-1], a[j])$
$\wedge\ j \leq i$
$\wedge\ I$

Formel $J[j/j+1]$

less_or_equal$(a[0, j], a[j{+}1]) \wedge j{+}1 \leq i$