Partial Correctness Assertions

Matthias Springer

11. Januar 2011

Inhalt

Korrektheit

- Aus Vorbedingung P folgt Nachbedindung Q
- **Partielle Korrektheit:** Programm *muss nicht* terminieren
- **Totale Korrektheit:** Programm *muss* terminieren

Hoare-Kalkül

- Korrektheit von imperativen Computer-Programmen
- Hoare-Tripel: $\{P\}S\{Q\}$
  - P, Q Zusicherungen (assertions): prädikatenlogische Formeln
  - S Programmsegment
  - P Vorbedingung
  - Q Nachbedingung

Zuweisungsaxiom

- $\frac{P \Rightarrow Q[v/t]}{\{P\} v := t \{Q\}}$
- $Q[v/t]$: Substitution von v durch t in Q
- Beispiel: $\{x + 1 = 42\}\ y := x + 1\ \{y = 42\}$
  $\{x + 1 = 42\}\{x + 1 = 42\}$
  $x + 1 = 42 \Rightarrow x + 1 = 42 \equiv$ wahr

Kompositions- oder Sequenzregel

- $\frac{\{P\}\ S\ \{R\}\ ,\ \{R\}\ T\ \{Q\}}{\{P\}\ S;T\ \{Q\}}$
- Beispiel: $\{x+1=42\}\ y := x+1; z := y\ \{z=42\}$
  $\{x+1=42\}\ y := x+1\ \{y=42\}$ und
  $\{y=42\}\ z := y\ \{z=42\}$
  $\{x+1=42\}\{x+1=42\}$ und $\{y=42\}\{y=42\}$

Auswahlregel (if-then-else-Regel) (1)

- $\dfrac{\{P \wedge B\}\ S\ \{Q\}\ ,\ \{P \wedge \neg B\}\ T\ \{Q\}}{\{P\}\ \text{if}\ B\ \text{then}\ S\ \text{else}\ T\ \{Q\}}$
- $\{x = a\}$
  if $x > 0$ **then**
  $z \leftarrow x$
  else
  $z \leftarrow -x$
  end if
  $\{z = |a|\}$

Auswahlregel (if-then-else-Regel) (2)

- $\{x = a \wedge x > 0\}$
  $z \leftarrow x$
  $\{z = |a|\}$
- $\{x = a \wedge x > 0\}$
  $\{x = |a|\}$
- $\{x = a \wedge x \leq 0\}$
  $z \leftarrow -x$
  $\{z = |a|\}$
- $\{x = a \wedge x \leq 0\}$
  $\{-x = |a|\}$

Kompositions- oder Sequenzregel

- $$\frac{\{I \wedge B\}\ S\ \{I\}}{\{I\}\ \text{while}\ B\ :\ S\ \{I \wedge \neg B\}}$$

Beispiel (1)

$\{a \geq 0\}$
$y \leftarrow 0$
$z \leftarrow 0$
while $y \neq a$ **do**
    $z \leftarrow z + 2y + 1$
    $y \leftarrow y + 1$
end while
$\{z = a^2\}$

Beispiel (2)

$\{a \geq 0 \wedge y = 0 \wedge z = 0\}$
while $y \neq a$ **do**
$\quad z \leftarrow z + 2y + 1$
$\quad y \leftarrow y + 1$
end while
$\{z = a^2\}$

Beispiel (3)

- Invariante: $z = y^2$
- $a \geq 0 \wedge y = 0 \wedge z = 0 \Rightarrow z = y^2$
- $\{z = y^2 \wedge y \neq a\}$
  $z \leftarrow z + 2y + 1$
  $y \leftarrow y + 1$
  $\{z = y^2\}$

Beispiel (4)

- $\{z = y^2 \wedge y \neq a\}$
  $z \leftarrow z + 2y + 1$
  $\{z = (y+1)^2\}$
- $\{z = y^2 \wedge y \neq a\}$
  $\{z + 2y + 1 = (y+1)^2\}$
- $z = y^2 \wedge y \neq a$
  $\Rightarrow z + 2y + 1 = y^2 + 2y + 1 = (y+1)^2$
- $I \wedge \neg B \equiv z = y^2 \wedge y = a \Rightarrow z = a^2$

Ergänzungen

- Programmverifizierer (Invarianten schwierig)
- Alternative: wp-Kalkül
- Zuweisung, Addition, Subtraktion, sequentielle Ausführung, `WHILE`-Schleife genügt für Turing-Berechenbarkeit

Quellen

- Gumm, H. P.; Sommer, M.: Einführung in die Informatik. 8. Auflage. München: Oldenbourg Wissenschaftsverlag GmbH, 2009
- Ohlbach, H. J.; Eisinger, N.; Hammer, M.: Programmverifikation mit dem Hoare-Kalkül. URL: `http://www.pst.ifi.lmu.de/lehre/SS06/infoII/material/hoare-kalkuel.pdf` Stand: 10.01.2011