Kapitel L:V

V. Erweiterungen und Anwendungen zur Logik

- Produktionsregelsysteme
- Inferenz für Produktionsregelsysteme
- Produktionsregelsysteme mit Negation
- Regeln mit Konfidenzen
- Nicht-monotones Schließen
- Logik und abstrakte Algebren
- Verifikation
- Verifikation mit dem Hoare-Kalkül
- Hoare-Regeln und partielle Korrektheit
- Terminierung

Hoare-Regeln und partielle Korrektheit

Hoare-Regel für Zuweisungen

$$A: \quad \frac{-}{\{N[x/e]\}\ x := e;\ \{N\}}$$

(A steht für Assignment.)

- Die Zuweisungsregel legt die Semantik der Zuweisung fest.
- Die Zuweisungsregel ordnet jeder Nachbedingung eine schwächste Vorbedingung (weakest precondition (wp)) zu.
- Die Zuweisungsregel führt die Semantik der Zuweisung auf die Semantik der Substitution in der Prädikatenlogik zurück.
- Da die Zuweisungsregel keine Voraussetzungen hat, bezeichnet man sie auch als Axiom.

Hoare-Regeln und partielle Korrektheit

Beispiele für die Anwendung der Zuweisungsregel

Abgeleitete Hoare-Formel für die Anweisung $b := y;$

$$\{x, y \in \mathbf{N} \textit{ und } a = x \textit{ und } y = y\}$$
$$b := y;$$
$$\{x, y \in \mathbf{N} \textit{ und } a = x \textit{ und } b = y\}$$

Abgeleitete Hoare-Formel für die Anweisung $x := x + 1;$

$$\{x + 1 = a\}$$
$$x := x + 1;$$
$$\{x = a\}$$

Hoare-Regeln und partielle Korrektheit

Abschwächungsregeln

$$C1: \quad \frac{\{P\} \Rightarrow \{P'\} \qquad \{P'\}\ S\ \{Q\}}{\{P\}\ S\ \{Q\}} \qquad\qquad C2: \quad \frac{\{P\}\ S\ \{Q'\} \qquad \{Q'\} \Rightarrow \{Q\}}{\{P\}\ S\ \{Q\}}$$

P' ist eine Abschwächung der Zusicherung P, so dass ein Zustand, der P erfüllt, auch P' erfüllt, d.h. P' ist semantische Folgerung von P, $P \models P'$.

Q ist eine Abschwächung der Zusicherung Q', so dass ein Zustand, der Q' erfüllt, auch Q erfüllt, d.h. Q ist semantische Folgerung von Q', $Q' \models Q$.

- Die Abschwächungsregeln verändern nur die Zusicherungen.
- Die Abschwächungsregeln setzen voraus, dass die Hoare-Formel für das entsprechende Programmstück bereits hergeleitet wurde.

Hoare-Regeln und partielle Korrektheit

Beispiele für die Anwendung der Abschwächungsregeln

Herleitung von Hoare-Formeln für die Anweisung $b := y;$

$\{x, y \in \mathbf{N}$ *und* $a = x\}$

$\Rightarrow \{x, y \in \mathbf{N}$ *und* $a = x$ *und* $y = y\}$

$b := y;$

$\{x, y \in \mathbf{N}$ *und* $a = x$ *und* $b = y\}$

$\Rightarrow \{x, y \in \mathbf{N}$ *und* $a + b = x + y$ *und* $a \geq 0\}$

Weitere Abschwächungen:

- Streichen konjunktiv verknüpfter Teile:
  $\{Q_1$ *und* $Q_2\} \;\Rightarrow\; \{Q_1\}$
- Hinzufügen von Folgerungen:
  $\{Q_1$ *und* $(Q_1 \Rightarrow Q_2)\} \;\Rightarrow\; \{Q_1$ *und* $(Q_1 \Rightarrow Q_2)$ *und* $Q_2\}$
- Hinzufügen von tautologischen Aussagen:
  $\{Q\} \;\Rightarrow\; \{Q$ *und* $x = x\}$
- Hinzufügen disjunktiv verknüpfter Teile:
  $\{Q_1\} \;\Rightarrow\; \{Q_1$ *oder* $Q_2\}$

Hoare-Regeln und partielle Korrektheit

Anwendung der Zuweisungsregel

$$A: \quad \frac{-}{\{N[x/e]\}\ x := e;\ \{N\}}$$

Von der Nachbedingung zur Vorbedingung (rückwärts):

- Nachbedingung N ist bekannt.
- Ersetze alle Vorkommen von x in N durch e.
- Ergebnis ist die schwächste Vorbedingung $N[x/e]$.

Hoare-Regeln und partielle Korrektheit

Beispiele zur Anwendung der Zuweisungsregel

$x := 27;$

$\{x \in \mathbf{N}$ *und* $y \in \mathbf{N}$ *und* $a = x$ *und* $b = y\}$

$y := x;$

$\{x, y \in \mathbf{N}$ *und* $a = x$ *und* $b = y\}$

$x := x + 1;$

$\{x, y \in \mathbf{N}$ *und* $a = x$ *und* $b = y\}$

$y := x + y;$

$\{x, y \in \mathbf{N}$ *und* $a = x$ *und* $b = y\}$

Hoare-Regeln und partielle Korrektheit

Beispiele zur Anwendung der Zuweisungsregel

$x := 27;$

$\{x \in \mathbf{N}$ *und* $y \in \mathbf{N}$ *und* $a = x$ *und* $b = y\}$

$y := x;$

$\{x, y \in \mathbf{N}$ *und* $a = x$ *und* $b = y\}$

$x := x + 1;$

$\{x, y \in \mathbf{N}$ *und* $a = x$ *und* $b = y\}$

$y := x + y;$

$\{x, y \in \mathbf{N}$ *und* $a = x$ *und* $b = y\}$

Hoare-Regeln und partielle Korrektheit

Beispiele zur Anwendung der Zuweisungsregel

$\{27 \in \mathbf{N}$ *und* $y \in \mathbf{N}$ *und* $a = 27$ *und* $b = y\}$

$x := 27;$

$\{x \in \mathbf{N}$ *und* $y \in \mathbf{N}$ *und* $a = x$ *und* $b = y\}$

$y := x;$

$\{x, y \in \mathbf{N}$ *und* $a = x$ *und* $b = y\}$

$x := x + 1;$

$\{x, y \in \mathbf{N}$ *und* $a = x$ *und* $b = y\}$

$y := x + y;$

$\{x, y \in \mathbf{N}$ *und* $a = x$ *und* $b = y\}$

Hoare-Regeln und partielle Korrektheit

Beispiele zur Anwendung der Zuweisungsregel

$\{27 \in \mathbf{N}$ *und* $y \in \mathbf{N}$ *und* $a = 27$ *und* $b = y\}$

$x := 27;$

$\{x \in \mathbf{N}$ *und* $y \in \mathbf{N}$ *und* $a = x$ *und* $b = y\}$

$y := x;$

$\{x, y \in \mathbf{N}$ *und* $a = x$ *und* $b = y\}$

$x := x + 1;$

$\{x, y \in \mathbf{N}$ *und* $a = x$ *und* $b = y\}$

$y := x + y;$

$\{x, y \in \mathbf{N}$ *und* $a = x$ *und* $b = y\}$

Hoare-Regeln und partielle Korrektheit

Beispiele zur Anwendung der Zuweisungsregel

$\{27 \in \mathbf{N}$ *und* $y \in \mathbf{N}$ *und* $a = 27$ *und* $b = y\}$

$x := 27;$

$\{x \in \mathbf{N}$ *und* $y \in \mathbf{N}$ *und* $a = x$ *und* $b = y\}$

$\{x, x \in \mathbf{N}$ *und* $a = x$ *und* $b = x\}$

$y := x;$

$\{x, y \in \mathbf{N}$ *und* $a = x$ *und* $b = y\}$

$x := x + 1;$

$\{x, y \in \mathbf{N}$ *und* $a = x$ *und* $b = y\}$

$y := x + y;$

$\{x, y \in \mathbf{N}$ *und* $a = x$ *und* $b = y\}$

Hoare-Regeln und partielle Korrektheit

Beispiele zur Anwendung der Zuweisungsregel

$\{27 \in \mathbf{N}$ *und* $y \in \mathbf{N}$ *und* $a = 27$ *und* $b = y\}$

$x := 27;$

$\{x \in \mathbf{N}$ *und* $y \in \mathbf{N}$ *und* $a = x$ *und* $b = y\}$

$\{x, x \in \mathbf{N}$ *und* $a = x$ *und* $b = x\}$

$y := x;$

$\{x, y \in \mathbf{N}$ *und* $a = x$ *und* $b = y\}$

$\{x + 1, y \in \mathbf{N}$ *und* $a = x + 1$ *und* $b = y\}$

$x := x + 1;$

$\{x, y \in \mathbf{N}$ *und* $a = x$ *und* $b = y\}$

$y := x + y;$

$\{x, y \in \mathbf{N}$ *und* $a = x$ *und* $b = y\}$

Hoare-Regeln und partielle Korrektheit

Beispiele zur Anwendung der Zuweisungsregel

$\{27 \in \mathbf{N}$ *und* $y \in \mathbf{N}$ *und* $a = 27$ *und* $b = y\}$

$x := 27;$

$\{x \in \mathbf{N}$ *und* $y \in \mathbf{N}$ *und* $a = x$ *und* $b = y\}$

$\{x, x \in \mathbf{N}$ *und* $a = x$ *und* $b = x\}$

$y := x;$

$\{x, y \in \mathbf{N}$ *und* $a = x$ *und* $b = y\}$

$\{x + 1, y \in \mathbf{N}$ *und* $a = x + 1$ *und* $b = y\}$

$x := x + 1;$

$\{x, y \in \mathbf{N}$ *und* $a = x$ *und* $b = y\}$

$\{x, x + y \in \mathbf{N}$ *und* $a = x$ *und* $b = x + y\}$

$y := x + y;$

$\{x, y \in \mathbf{N}$ *und* $a = x$ *und* $b = y\}$

Hoare-Regeln und partielle Korrektheit

Anwendung der Zuweisungsregel (Fortsetzung)

$$A: \quad \frac{-}{\{N[x/e]\}\ x := e;\ \{N\}}$$

Von der Vorbedingung zur Nachbedingung (vorwärts):

Fall 1: x kommt in e nicht vor

- Vorbedingung V ist bekannt
- Schwäche Vorbedingung V ab:
  - Eliminiere *alle* Vorkommen von x in V.
  - (Erzeuge neue Vorkommen von e, z.B. $e = e$.)

  Ergebnis ist (abgeschwächte) Vorbedingung V'.
- Ersetze in V' *manche* Vorkommen von e durch x.
- Ergebnis ist die Nachbedingung N.

Hoare-Regeln und partielle Korrektheit

Beispiele zur Anwendung der Zuweisungsregel (Fortsetzung)

$\{x, y \in \mathbf{N}$ *und* $a = x\}$
$x := 27;$

Hoare-Regeln und partielle Korrektheit

Beispiele zur Anwendung der Zuweisungsregel (Fortsetzung)

$\{x, y \in \mathbf{N}$ *und* $a = x\}$

$x := 27;$

Hoare-Regeln und partielle Korrektheit

Beispiele zur Anwendung der Zuweisungsregel (Fortsetzung)

$\{x, y \in \mathbf{N}$ *und* $a = x\}$

$\Rightarrow \{y \in \mathbf{N}\}$

$x := 27;$

Hoare-Regeln und partielle Korrektheit

Beispiele zur Anwendung der Zuweisungsregel (Fortsetzung)

$\{x, y \in \mathbf{N}$ *und* $a = x\}$

$\Rightarrow \{y \in \mathbf{N}\}$

$\Rightarrow \{y \in \mathbf{N}$ *und* $27 \in \mathbf{N}$ *und* $27 = 27\}$

$x := 27;$

Hoare-Regeln und partielle Korrektheit

Beispiele zur Anwendung der Zuweisungsregel (Fortsetzung)

$\{x, y \in \mathbf{N}$ *und* $a = x\}$

$\Rightarrow \{y \in \mathbf{N}\}$

$\Rightarrow \{y \in \mathbf{N}$ *und* $27 \in \mathbf{N}$ *und* $27 = 27\}$

$x := 27;$

$\{x, y \in \mathbf{N}$ *und* $x = 27\}$

Hoare-Regeln und partielle Korrektheit

Beispiele zur Anwendung der Zuweisungsregel (Fortsetzung)

$\{x, y \in \mathbf{N}$ *und* $a = x\}$

$\Rightarrow \{y \in \mathbf{N}\}$

$\Rightarrow \{y \in \mathbf{N}$ *und* $27 \in \mathbf{N}$ *und* $27 = 27\}$

$x := 27;$

$\{x, y \in \mathbf{N}$ *und* $x = 27\}$

$\{x, y \in \mathbf{N}$ *und* $a = x\}$

$y := x;$

Hoare-Regeln und partielle Korrektheit

Beispiele zur Anwendung der Zuweisungsregel (Fortsetzung)

$\{x, y \in \mathbf{N}$ *und* $a = x\}$

$\Rightarrow \{y \in \mathbf{N}\}$

$\Rightarrow \{y \in \mathbf{N}$ *und* $27 \in \mathbf{N}$ *und* $27 = 27\}$

$x := 27;$

$\{x, y \in \mathbf{N}$ *und* $x = 27\}$

$\{x, y \in \mathbf{N}$ *und* $a = x\}$

$y := x;$

Hoare-Regeln und partielle Korrektheit

Beispiele zur Anwendung der Zuweisungsregel (Fortsetzung)

$\{x, y \in \mathbf{N}$ *und* $a = x\}$

$\Rightarrow \{y \in \mathbf{N}\}$

$\Rightarrow \{y \in \mathbf{N}$ *und* $27 \in \mathbf{N}$ *und* $27 = 27\}$

$x := 27;$

$\{x, y \in \mathbf{N}$ *und* $x = 27\}$

$\{x, y \in \mathbf{N}$ *und* $a = x\}$

$\Rightarrow \{x \in \mathbf{N}$ *und* $a = x\}$

$y := x;$

Hoare-Regeln und partielle Korrektheit

Beispiele zur Anwendung der Zuweisungsregel (Fortsetzung)

$\{x, y \in \mathbf{N}$ *und* $a = x\}$

$\Rightarrow \{y \in \mathbf{N}\}$

$\Rightarrow \{y \in \mathbf{N}$ *und* $27 \in \mathbf{N}$ *und* $27 = 27\}$

$x := 27;$

$\{x, y \in \mathbf{N}$ *und* $x = 27\}$

$\{x, y \in \mathbf{N}$ *und* $a = x\}$

$\Rightarrow \{x \in \mathbf{N}$ *und* $a = x\}$

$\Rightarrow \{x \in \mathbf{N}$ *und* $a = x$ *und* $x = x\}$

$y := x;$

Hoare-Regeln und partielle Korrektheit

Beispiele zur Anwendung der Zuweisungsregel (Fortsetzung)

$\{x, y \in \mathbf{N}$ *und* $a = x\}$

$\Rightarrow \{y \in \mathbf{N}\}$

$\Rightarrow \{y \in \mathbf{N}$ *und* $27 \in \mathbf{N}$ *und* $27 = 27\}$

$x := 27;$

$\{x, y \in \mathbf{N}$ *und* $x = 27\}$

$\{x, y \in \mathbf{N}$ *und* $a = x\}$

$\Rightarrow \{x \in \mathbf{N}$ *und* $a = x\}$

$\Rightarrow \{x \in \mathbf{N}$ *und* $a = x$ *und* $x = x\}$

$y := x;$

$\{x \in \mathbf{N}$ *und* $a = x$ *und* $y = x\}$

Hoare-Regeln und partielle Korrektheit

Anwendung der Zuweisungsregel (Fortsetzung)

$$A: \quad \frac{-}{\{N[x/e]\}\ x := e;\ \{N\}}$$

Von der Vorbedingung zur Nachbedingung (vorwärts):

Fall 2: x kommt in e vor

- Vorbedingung V ist bekannt
- Schwäche Vorbedingung V ab:
  - Wandle *alle* Vorkommen von x in V in Vorkommen von e um.

  Ergebnis ist (abgeschwächte) Vorbedingung V'.
- Ersetze in V' *alle* Vorkommen von e durch x.
- Ergebnis ist die Nachbedingung N.

Hoare-Regeln und partielle Korrektheit

Beispiele zur Anwendung der Zuweisungsregel (Fortsetzung)

$\{x, y \in \mathbf{N}$ *und* $a = x\}$

$x := x + 1;$

Hoare-Regeln und partielle Korrektheit

Beispiele zur Anwendung der Zuweisungsregel (Fortsetzung)

$\{x, y \in \mathbf{N}$ *und* $a = x\}$

$x := x + 1;$

Hoare-Regeln und partielle Korrektheit

Beispiele zur Anwendung der Zuweisungsregel (Fortsetzung)

$\{x, y \in \mathbf{N}$ *und* $a = x\}$

$\Rightarrow \{x + 1, y \in \mathbf{N}$ *und* $a + 1 = x + 1\}$

$x := x + 1;$

Hoare-Regeln und partielle Korrektheit

Beispiele zur Anwendung der Zuweisungsregel (Fortsetzung)

$\{x, y \in \mathbf{N}$ *und* $a = x\}$

$\Rightarrow \{x + 1, y \in \mathbf{N}$ *und* $a + 1 = x + 1\}$

$x := x + 1;$

$\{x, y \in \mathbf{N}$ *und* $a + 1 = x\}$

Hoare-Regeln und partielle Korrektheit

Beispiele zur Anwendung der Zuweisungsregel (Fortsetzung)

$\{x, y \in \mathbf{N}$ *und* $a = x\}$

$\Rightarrow \{x + 1, y \in \mathbf{N}$ *und* $a + 1 = x + 1\}$

$x := x + 1;$

$\{x, y \in \mathbf{N}$ *und* $a + 1 = x\}$

$\{x, y \in \mathbf{N}$ *und* $a = x\}$

$y := x + y;$

Hoare-Regeln und partielle Korrektheit

Beispiele zur Anwendung der Zuweisungsregel (Fortsetzung)

$\{x, y \in \mathbf{N}$ *und* $a = x\}$

$\Rightarrow \{x + 1, y \in \mathbf{N}$ *und* $a + 1 = x + 1\}$

$x := x + 1;$

$\{x, y \in \mathbf{N}$ *und* $a + 1 = x\}$

$\{x, y \in \mathbf{N}$ *und* $a = x\}$

$y := x + y;$

Hoare-Regeln und partielle Korrektheit

Beispiele zur Anwendung der Zuweisungsregel (Fortsetzung)

$\{x, y \in \mathbf{N}$ *und* $a = x\}$

$\Rightarrow \{x + 1, y \in \mathbf{N}$ *und* $a + 1 = x + 1\}$

$x := x + 1;$

$\{x, y \in \mathbf{N}$ *und* $a + 1 = x\}$

$\{x, y \in \mathbf{N}$ *und* $a = x\}$

$\Rightarrow \{x, x + y \in \mathbf{N}$ *und* $a = x\}$

$y := x + y;$

Hoare-Regeln und partielle Korrektheit

Beispiele zur Anwendung der Zuweisungsregel (Fortsetzung)

$\{x, y \in \mathbf{N}$ *und* $a = x\}$

$\Rightarrow \{x + 1, y \in \mathbf{N}$ *und* $a + 1 = x + 1\}$

$x := x + 1;$

$\{x, y \in \mathbf{N}$ *und* $a + 1 = x\}$

$\{x, y \in \mathbf{N}$ *und* $a = x\}$

$\Rightarrow \{x, x + y \in \mathbf{N}$ *und* $a = x\}$

$y := x + y;$

$\{x, y \in \mathbf{N}$ *und* $a = x\}$

Hoare-Regeln und partielle Korrektheit

Hoare-Regeln für Anweisungsfolgen

$$S: \quad \frac{\{P\}\ S_1\ \{Q\} \qquad \{Q\}\ S_2\ \{R\}}{\{P\}\ S_1 S_2\ \{R\}} \qquad B: \quad \frac{\{P\}\ S\ \{Q\}}{\{P\}\ \texttt{begin}\ S\ \texttt{end}\ \{Q\}}$$

- Die Regeln legen fest, wie Folgen und Blöcke von Anweisungen ausgeführt werden.
- Hoare-Formeln für Anweisungsfolgen müssen zusammenpassen.
- Die Strukturierung der Programme durch *begin* und *end* sorgt für eine eindeutige Aufteilung eines Programmes in Anweisungen. Aus Sicht der Verifikation wäre sie nicht erforderlich, da die Struktur des Programmes im Verifikationsbeweis festgelegt wäre.
- Die Blockung von Anweisungen erfordert keinen zusätzlichen Verifikationsaufwand.

Hoare-Regeln und partielle Korrektheit

Vorgehen bei der Verifikation eines Programmes

- Gegeben ist eine Spezifikation mit Vorbedingung $\{V\}$ und Nachbedingung $\{N\}$ sowie ein Programm P.
- P bestehe nur aus einer Folge von Zuweisungen.

Vorgehen im Hoare-Kalkül

0. Generelle Vereinfachung:
   Die Nachbedingung einer Anweisung wird durch Abschwächung zur Vorbedingung der nächsten.
1. Ergänze $\{V\}$ als Vorbedingung vor dem Programmtext.
2. Je nach Programmanweisung verfahre folgendermaßen:
   (a) `begin`
   Kopiere die Vorbedingung dieser Zeile vor die Anweisungsfolge.
   (b) `end`
   Kopiere die Nachbedingung der Anweisungsfolge hinter diese Zeile.
   (c) Zuweisung $x := e;$
   Wende Abschwächungsregeln und Zuweisungsregel auf die Vorbedingung so an, wie es die Zuweisung erfordert
   (Fall 1: x kommt in e nicht vor; Fall 2: x kommt in e vor).
3. Wende Abschwächungsregeln auf die Nachbedingung an, um die Nachbedingung $\{N\}$ der Spezifikation zu erreichen.

Hoare-Regeln und partielle Korrektheit

Beispiel zur Verifikation eines Programmes

Spezifikation:

Vorbedingung: $\{x, y \in \mathbf{N}\}$
Nachbedingung: $\{b = x + y\}$

(A)
(1) `begin`
(B)
(C)
(2) $a := x;$
(D)
(E)
(3) $b := y;$
(F)
(G)
(4) $b := b + a;$
(H)
(5) `end`
(I)
(J)

Hoare-Regeln und partielle Korrektheit

Beispiel zur Verifikation eines Programmes

Spezifikation:

Vorbedingung: $\{x, y \in \mathbf{N}\}$
Nachbedingung: $\{b = x + y\}$

(A)	$\{x, y \in \mathbf{N}\}$
(1)	`begin`
(B)	
(C)	
(2)	$a := x;$
(D)	
(E)	
(3)	$b := y;$
(F)	
(G)	
(4)	$b := b + a;$
(H)	
(5)	`end`
(I)	
(J)	

Hoare-Regeln und partielle Korrektheit

Beispiel zur Verifikation eines Programmes

Spezifikation:

Vorbedingung: $\{x, y \in \mathbf{N}\}$
Nachbedingung: $\{b = x + y\}$

(A)	$\{x, y \in \mathbf{N}\}$
(1)	`begin`
(B)	$\{x, y \in \mathbf{N}\}$
(C)	
(2)	$a := x;$
(D)	
(E)	
(3)	$b := y;$
(F)	
(G)	
(4)	$b := b + a;$
(H)	
(5)	`end`
(I)	
(J)	

Hoare-Regeln und partielle Korrektheit

Beispiel zur Verifikation eines Programmes

Spezifikation:

Vorbedingung: $\{x, y \in \mathbf{N}\}$
Nachbedingung: $\{b = x + y\}$

(A)	$\{x, y \in \mathbf{N}\}$
(1)	`begin`
(B)	$\{x, y \in \mathbf{N}\}$
(C)	$\Rightarrow \{x, y \in \mathbf{N}$ *und* $x = x\}$
(2)	$a := x;$
(D)	
(E)	
(3)	$b := y;$
(F)	
(G)	
(4)	$b := b + a;$
(H)	
(5)	`end`
(I)	
(J)	

Hoare-Regeln und partielle Korrektheit

Beispiel zur Verifikation eines Programmes

Spezifikation:

Vorbedingung: $\{x, y \in \mathbf{N}\}$
Nachbedingung: $\{b = x + y\}$

(A)	$\{x, y \in \mathbf{N}\}$
(1)	`begin`
(B)	$\{x, y \in \mathbf{N}\}$
(C)	$\Rightarrow \{x, y \in \mathbf{N}$ *und* $x = x\}$
(2)	$a := x;$
(D)	$\{x, y \in \mathbf{N}$ *und* $a = x\}$
(E)	
(3)	$b := y;$
(F)	
(G)	
(4)	$b := b + a;$
(H)	
(5)	`end`
(I)	
(J)	

Hoare-Regeln und partielle Korrektheit

Beispiel zur Verifikation eines Programmes

Spezifikation:

Vorbedingung: $\{x, y \in \mathbf{N}\}$
Nachbedingung: $\{b = x + y\}$

(A)	$\{x, y \in \mathbf{N}\}$
(1)	`begin`
(B)	$\{x, y \in \mathbf{N}\}$
(C)	$\Rightarrow \{x, y \in \mathbf{N}$ *und* $x = x\}$
(2)	$a := x;$
(D)	$\{x, y \in \mathbf{N}$ *und* $a = x\}$
(E)	$\Rightarrow \{x, y \in \mathbf{N}$ *und* $a = x$ *und* $y = y\}$
(3)	$b := y;$
(F)	$\{x, y \in \mathbf{N}$ *und* $a = x$ *und* $b = y\}$
(G)	$\Rightarrow \{x, y \in \mathbf{N}$ *und* $a = x$ *und* $b + a = a + y\}$
(4)	$b := b + a;$
(H)	$\{x, y \in \mathbf{N}$ *und* $a = x$ *und* $b = a + y\}$
(5)	`end`
(I)	
(J)	

Hoare-Regeln und partielle Korrektheit

Beispiel zur Verifikation eines Programmes

Spezifikation:

Vorbedingung: $\{x, y \in \mathbf{N}\}$
Nachbedingung: $\{b = x + y\}$

(A)	$\{x, y \in \mathbf{N}\}$
(1)	`begin`
(B)	$\{x, y \in \mathbf{N}\}$
(C)	$\Rightarrow \{x, y \in \mathbf{N}$ *und* $x = x\}$
(2)	$a := x;$
(D)	$\{x, y \in \mathbf{N}$ *und* $a = x\}$
(E)	$\Rightarrow \{x, y \in \mathbf{N}$ *und* $a = x$ *und* $y = y\}$
(3)	$b := y;$
(F)	$\{x, y \in \mathbf{N}$ *und* $a = x$ *und* $b = y\}$
(G)	$\Rightarrow \{x, y \in \mathbf{N}$ *und* $a = x$ *und* $b + a = a + y\}$
(4)	$b := b + a;$
(H)	$\{x, y \in \mathbf{N}$ *und* $a = x$ *und* $b = a + y\}$
(5)	`end`
(I)	$\{x, y \in \mathbf{N}$ *und* $a = x$ *und* $b = a + y\}$
(J)	$\Rightarrow \{b = x + y\}$

Bemerkungen:

- Beim Aufschreiben eines Programmes wird jede Anweisung in einer neuen Zeile begonnen.
- Die Zeilen im Programm werden so eingerückt, dass die Schachtelung der Anweisungen erkennbar ist.
- Die Zusicherungen werden in das Programm eingefügt.
- Die Einrückung der Zusicherungen erfolgt so, dass sie auf gleicher Höhe mit den zugehörigen Anweisungen stehen.

Hoare-Regeln und partielle Korrektheit

Beispiel zur Verifikation eines Programmes (Fortsetzung)

Herleitung im Hoare-Kalkül

Nr.	Hoare-Formel	Regel
a.	(C)(2)(D)	nach Zuweisungsregel A
b.	(B)(2)(D)	nach Abschwächungsregel C1 für a
c.	(E)(3)(F)	nach Zuweisungsregel A
d.	(D)(3)(F)	nach Abschwächungsregel C1 für c
e.	(B)(2)(3)(F)	nach Sequenzenregel S für b,d
f.	(G)(4)(H)	nach Zuweisungsregel A
g.	(F)(4)(H)	nach Abschwächungsregel C1 für f
h.	(B)(2)(3)(4)(H)	nach Sequenzenregel S für e,g
i.	(A)(1)(2)(3)(4)(5)(I)	nach Blockregel B für h
i.	(A)(1)(2)(3)(4)(5)(J)	nach Abschwächungsregel C2 für i

Dieser Beweis zeigt nur die partielle Korrektheit, d.h. es muss zusätzlich gezeigt werden, dass das Programm terminiert.

Bemerkungen zum Lesen der Tabelle:

- Die Elemente der Herleitung sind in Spalte 1 durchnummeriert (a-z).
- Die Liste der Hoare-Formeln wird untereinander in Spalte 2 der Tabelle angegeben.
- Die Hoare-Formeln werden durch Referenz auf die Zeilennummern in dem durch Zusicherungen ergänzten Programm angegeben ((1) - (9999)).
- Es wird in Spalte 3 die angewendete Regel angegeben und eine die Referenzen auf die Hoare-Formeln, die ihre Voraussetzung bilden.

Hoare-Regeln und partielle Korrektheit

Hoare-Regeln für bedingte Anweisungen

$$I1: \quad \frac{\{B \textit{ und } P\}\ S_1\ \{Q\} \qquad \{(\textit{nicht } B) \textit{ und } P\} \Rightarrow \{Q\}}{\{P\}\ \texttt{if}\ (B)\ \texttt{then}\ S_1\ \{Q\}}$$

$$I2: \quad \frac{\{B \textit{ und } P\}\ S_1\ \{Q\} \qquad \{(\textit{nicht } B) \textit{ und } P\}\ S_2\ \{Q\}}{\{P\}\ \texttt{if}\ (B)\ \texttt{then}\ S_1\ \texttt{else}\ S_2\ \{Q\}}$$

- In der Regel für bedingte Anweisungen wird die Bedingung der Anweisung für zusätzliche Bedingungen in den Zusicherungen verwendet.
- Da die Handlungsfäden des Programmes wieder zusammenlaufen, muss in beiden Alternativen dieselbe Nachbedingung erreicht werden.
- Eine gemeinsame Nachbedingung kann durch Abschwächungsregeln erreicht werden:
  - durch Abstraktion wie im Beispiel oder
  - durch disjunktive Verknüpfung der einzelnen Nachbedingungen.

Hoare-Regeln und partielle Korrektheit

Beispiele zur Anwendung der Regeln für bedingte Anweisungen

$\{a \in \mathbf{Z}\}$

`if` $(a > 0)$ `then`

$b := a;$

`else`

$b := -a;$

Hoare-Regeln und partielle Korrektheit

Beispiele zur Anwendung der Regeln für bedingte Anweisungen

$\{a \in \mathbf{Z}\}$

`if` $(a > 0)$ `then`

$\{a \in \mathbf{Z}$ *und* $a > 0\}$

$b := a;$

`else`

$\{a \in \mathbf{Z}$ *und* $(\textit{nicht } a > 0)\}$

$b := -a;$

Hoare-Regeln und partielle Korrektheit

Beispiele zur Anwendung der Regeln für bedingte Anweisungen

$\{a \in \mathbf{Z}\}$

`if` $(a > 0)$ `then`

$\{a \in \mathbf{Z}$ *und* $a > 0\}$

$\Rightarrow \{a \in \mathbf{Z}$ *und* $a > 0$ *und* $a = a\}$

$b := a;$

`else`

$\{a \in \mathbf{Z}$ *und* $($*nicht* $a > 0)\}$

$\Rightarrow \{a \in \mathbf{Z}$ *und* $a \leq 0$ *und* $-a = -a\}$

$b := -a;$

Hoare-Regeln und partielle Korrektheit

Beispiele zur Anwendung der Regeln für bedingte Anweisungen

$\{a \in \mathbf{Z}\}$

`if` $(a > 0)$ `then`

$\{a \in \mathbf{Z}$ *und* $a > 0\}$

$\Rightarrow \{a \in \mathbf{Z}$ *und* $a > 0$ *und* $a = a\}$

$b := a;$

$\{a \in \mathbf{Z}$ *und* $a > 0$ *und* $b = a\}$

`else`

$\{a \in \mathbf{Z}$ *und* $(\textit{nicht } a > 0)\}$

$\Rightarrow \{a \in \mathbf{Z}$ *und* $a \leq 0$ *und* $-a = -a\}$

$b := -a;$

$\{a \in \mathbf{Z}$ *und* $a \leq 0$ *und* $b = -a\}$

Hoare-Regeln und partielle Korrektheit

Beispiele zur Anwendung der Regeln für bedingte Anweisungen

$\{a \in \mathbf{Z}\}$

`if` $(a > 0)$ `then`

$\{a \in \mathbf{Z}$ *und* $a > 0\}$

$\Rightarrow \{a \in \mathbf{Z}$ *und* $a > 0$ *und* $a = a\}$

$b := a;$

$\{a \in \mathbf{Z}$ *und* $a > 0$ *und* $b = a\}$

$\Rightarrow \{a \in \mathbf{Z}$ *und* $b = |a|\}$

`else`

$\{a \in \mathbf{Z}$ *und* $(\textit{nicht } a > 0)\}$

$\Rightarrow \{a \in \mathbf{Z}$ *und* $a \leq 0$ *und* $-a = -a\}$

$b := -a;$

$\{a \in \mathbf{Z}$ *und* $a \leq 0$ *und* $b = -a\}$

$\Rightarrow \{a \in \mathbf{Z}$ *und* $b = |a|\}$

$\{a \in \mathbf{Z}$ *und* $b = |a|\}$

Hoare-Regeln und partielle Korrektheit

Anwendung der Regeln für bedingte Anweisungen

Vorgehensweise bei bekannter Vorbedingung $\{P\}$

- Vorbedingung zu den Vorbedingungen $\{P$ *und* $B\}$ im *then*-Teil und $\{P$ *und* $(\textit{nicht}\ B)\}$ im *else*-Teil ergänzen.
- *then*-Teil und *else*-Teil verifizieren mit Nachbedingungen $\{Q_1\}$ bzw. $\{Q_2\}$.
- Nachbedinungen zu gemeinsamer Nachbedingung $\{Q\}$ abschwächen (z.B. $(Q_1$ *oder* $Q_2)$ für Q wählen).
- Nachbedingung $\{Q\}$ der bedingten Anweisung einfügen.

Hoare-Regeln und partielle Korrektheit

Beispiele zur Anwendung der Regeln für bedingte Anweisungen (Fortsetzung)

$\{a > 0$ *und* $b > 0$ *und* $a \neq b\}$

`if` $(a > b)$ `then`

$a := a - b;$

`else`

$b := b - a;$

Hoare-Regeln und partielle Korrektheit

Beispiele zur Anwendung der Regeln für bedingte Anweisungen (Fortsetzung)

$\{a > 0$ *und* $b > 0$ *und* $a \neq b\}$

`if` $(a > b)$ `then`

$\{a > 0$ *und* $b > 0$ *und* $a \neq b$ *und* $a > b\}$

$a := a - b;$

`else`

$\{a > 0$ *und* $b > 0$ *und* $a \neq b$ *und* $a \leq b\}$

$b := b - a;$

Hoare-Regeln und partielle Korrektheit

Beispiele zur Anwendung der Regeln für bedingte Anweisungen (Fortsetzung)

$\{a > 0$ *und* $b > 0$ *und* $a \neq b\}$

`if` $(a > b)$ `then`

$\{a > 0$ *und* $b > 0$ *und* $a \neq b$ *und* $a > b\}$

$\Rightarrow \{a - b + b > 0$ *und* $b > 0$ *und* $a - b + b \neq b$ *und* $a - b + b > b\}$

$a := a - b;$

`else`

$\{a > 0$ *und* $b > 0$ *und* $a \neq b$ *und* $a \leq b\}$

$\Rightarrow \{a > 0$ *und* $b - a + a > 0$ *und* $a \neq b - a + a$ *und* $a \leq b - a + a\}$

$b := b - a;$

Hoare-Regeln und partielle Korrektheit

Beispiele zur Anwendung der Regeln für bedingte Anweisungen (Fortsetzung)

$\{a > 0$ *und* $b > 0$ *und* $a \neq b\}$

`if` $(a > b)$ `then`

$\{a > 0$ *und* $b > 0$ *und* $a \neq b$ *und* $a > b\}$

$\Rightarrow \{a - b + b > 0$ *und* $b > 0$ *und* $a - b + b \neq b$ *und* $a - b + b > b\}$

$a := a - b;$

$\{a + b > 0$ *und* $b > 0$ *und* $a + b \neq b$ *und* $a + b > b\}$

`else`

$\{a > 0$ *und* $b > 0$ *und* $a \neq b$ *und* $a \leq b\}$

$\Rightarrow \{a > 0$ *und* $b - a + a > 0$ *und* $a \neq b - a + a$ *und* $a \leq b - a + a\}$

$b := b - a;$

$\{a > 0$ *und* $b + a > 0$ *und* $a \neq b + a$ *und* $a \leq b + a\}$

Hoare-Regeln und partielle Korrektheit

Beispiele zur Anwendung der Regeln für bedingte Anweisungen (Fortsetzung)

$\{a > 0$ *und* $b > 0$ *und* $a \neq b\}$

`if` $(a > b)$ `then`

$\{a > 0$ *und* $b > 0$ *und* $a \neq b$ *und* $a > b\}$

$\Rightarrow \{a - b + b > 0$ *und* $b > 0$ *und* $a - b + b \neq b$ *und* $a - b + b > b\}$

$a := a - b;$

$\{a + b > 0$ *und* $b > 0$ *und* $a + b \neq b$ *und* $a + b > b\}$

$\Rightarrow \{b > 0$ *und* $a > 0\}$

`else`

$\{a > 0$ *und* $b > 0$ *und* $a \neq b$ *und* $a \leq b\}$

$\Rightarrow \{a > 0$ *und* $b - a + a > 0$ *und* $a \neq b - a + a$ *und* $a \leq b - a + a\}$

$b := b - a;$

$\{a > 0$ *und* $b + a > 0$ *und* $a \neq b + a$ *und* $a \leq b + a\}$

$\Rightarrow \{a > 0$ *und* $a + b > 0$ *und* $0 \neq b$ *und* $0 \leq b\}$

$\Rightarrow \{a > 0$ *und* $b > 0\}$

$\{a > 0$ *und* $b > 0\}$

Hoare-Regeln und partielle Korrektheit

Beispiel zur Verifikation von bedingten Anweisungen

$\{a \in \mathbf{Z}$ *und* $a \geq 0\}$

`if` $(a$ ungerade$)$ `then`

$a := a - 1;$

// `empty else branch`

Hoare-Regeln und partielle Korrektheit

Beispiel zur Verifikation von bedingten Anweisungen

$\{a \in \mathbf{Z}$ *und* $a \geq 0\}$

`if` $(a$ ungerade$)$ `then`

$\{a \in \mathbf{Z}$ *und* $a \geq 0$ *und* a ungerade$\}$

$a := a - 1;$

`// empty else branch`

$\{a \in \mathbf{Z}$ *und* $a \geq 0$ *und* a gerade$\}$

Hoare-Regeln und partielle Korrektheit

Beispiel zur Verifikation von bedingten Anweisungen

$\{a \in \mathbf{Z}$ *und* $a \geq 0\}$

`if` $(a$ ungerade$)$ `then`

$\{a \in \mathbf{Z}$ *und* $a \geq 0$ *und* a ungerade$\}$

$\Rightarrow \{a - 1 \in \mathbf{Z}$ *und* $a - 1 \geq 0$ *und* $a - 1$ gerade$\}$

$a := a - 1;$

$\{a \in \mathbf{Z}$ *und* $a \geq 0$ *und* a gerade$\}$

// `empty else branch`

$\{a \in \mathbf{Z}$ *und* $a \geq 0$ *und* a gerade$\}$

Hoare-Regeln und partielle Korrektheit

Beispiel zur Verifikation von bedingten Anweisungen

$\{a \in \mathbf{Z}$ *und* $a \geq 0\}$

`if` $(a$ ungerade$)$ `then`

$\{a \in \mathbf{Z}$ *und* $a \geq 0$ *und* a ungerade$\}$

$\Rightarrow \{a - 1 \in \mathbf{Z}$ *und* $a - 1 \geq 0$ *und* $a - 1$ gerade$\}$

$a := a - 1;$

$\{a \in \mathbf{Z}$ *und* $a \geq 0$ *und* a gerade$\}$

// `empty else branch`

$\{a \in \mathbf{Z}$ *und* $a \geq 0$ *und* a gerade$\}$

$\{a \in \mathbf{Z}$ *und* $a \geq 0$ *und* a gerade$\}$

Hoare-Regeln und partielle Korrektheit

Beispiel zur Verifikation von bedingten Anweisungen (Fortsetzung)

$\{a, b \in \mathbf{Z}$ *und* $a \geq 0$ *und* $b \geq 0\}$

`if` $(a > b)$ `then`

$a := a - b;$

// `empty else branch`

Hoare-Regeln und partielle Korrektheit

Beispiel zur Verifikation von bedingten Anweisungen (Fortsetzung)

$\{a, b \in \mathbf{Z}$ *und* $a \geq 0$ *und* $b \geq 0\}$

`if` $(a > b)$ `then`

$\{a, b \in \mathbf{Z}$ *und* $a \geq 0$ *und* $b \geq 0$ *und* $a > b\}$

$a := a - b;$

`// empty else branch`

$\{a, b \in \mathbf{Z}$ *und* $a \geq 0$ *und* $b \geq 0$ *und* $($*nicht* $a > b)\}$

Hoare-Regeln und partielle Korrektheit

Beispiel zur Verifikation von bedingten Anweisungen (Fortsetzung)

$\{a, b \in \mathbf{Z}$ *und* $a \geq 0$ *und* $b \geq 0\}$

`if` $(a > b)$ `then`

$\{a, b \in \mathbf{Z}$ *und* $a \geq 0$ *und* $b \geq 0$ *und* $a > b\}$

$\Rightarrow \{a - b, b \in \mathbf{Z}$ *und* $a - b \geq 0$ *und* $b \geq 0\}$

$a := a - b;$

$\{a, b \in \mathbf{Z}$ *und* $a \geq 0$ *und* $b \geq 0\}$

// `empty else branch`

$\{a, b \in \mathbf{Z}$ *und* $a \geq 0$ *und* $b \geq 0$ *und* $($*nicht* $a > b)\}$

$\Rightarrow \{a, b \in \mathbf{Z}$ *und* $a \geq 0$ *und* $b \geq 0\}$

Hoare-Regeln und partielle Korrektheit

Beispiel zur Verifikation von bedingten Anweisungen (Fortsetzung)

$\{a, b \in \mathbf{Z}$ *und* $a \geq 0$ *und* $b \geq 0\}$

`if` $(a > b)$ `then`

$\{a, b \in \mathbf{Z}$ *und* $a \geq 0$ *und* $b \geq 0$ *und* $a > b\}$

$\Rightarrow \{a - b, b \in \mathbf{Z}$ *und* $a - b \geq 0$ *und* $b \geq 0\}$

$a := a - b;$

$\{a, b \in \mathbf{Z}$ *und* $a \geq 0$ *und* $b \geq 0\}$

// `empty else branch`

$\{a, b \in \mathbf{Z}$ *und* $a \geq 0$ *und* $b \geq 0$ *und* $($*nicht* $a > b)\}$

$\Rightarrow \{a, b \in \mathbf{Z}$ *und* $a \geq 0$ *und* $b \geq 0\}$

$\{a, b \in \mathbf{Z}$ *und* $a \geq 0$ *und* $b \geq 0\}$

Hoare-Regeln und partielle Korrektheit

Beispiel zur Verifikation von bedingten Anweisungen (Fortsetzung)

$\{a \neq 0\}$

`if` $(a > 0)$ `then`

$b := 1;$

`else`

$b := -1;$

$\{a \cdot b > 0$ *und* $a \neq 0\}$

Hoare-Regeln und partielle Korrektheit

Beispiel zur Verifikation von bedingten Anweisungen (Fortsetzung)

$\{a \neq 0\}$

`if` $(a > 0)$ `then`

$\{a \neq 0$ *und* $a > 0\}$

$b := 1;$

`else`

$\{a \neq 0$ *und* $a \leq 0\}$

$b := -1;$

$\{a \cdot b > 0$ *und* $a \neq 0\}$

Hoare-Regeln und partielle Korrektheit

Beispiel zur Verifikation von bedingten Anweisungen (Fortsetzung)

$\{a \neq 0\}$

`if` $(a > 0)$ `then`

$\{a \neq 0$ *und* $a > 0\}$

$\Rightarrow \{a > 0$ *und* $1 = 1\}$

$b := 1;$

$\{a > 0$ *und* $b = 1\}$

`else`

$\{a \neq 0$ *und* $a \leq 0\}$

$\Rightarrow \{a < 0$ *und* $-1 = -1\}$

$b := -1;$

$\{a < 0$ *und* $b = -1\}$

$\{a \cdot b > 0$ *und* $a \neq 0\}$

Hoare-Regeln und partielle Korrektheit

Beispiel zur Verifikation von bedingten Anweisungen (Fortsetzung)

$\{a \neq 0\}$

`if` $(a > 0)$ `then`

$\{a \neq 0$ *und* $a > 0\}$

$\Rightarrow \{a > 0$ *und* $1 = 1\}$

$b := 1;$

$\{a > 0$ *und* $b = 1\}$

$\Rightarrow \{a \cdot b > 0$ *und* $a \neq 0\}$

`else`

$\{a \neq 0$ *und* $a \leq 0\}$

$\Rightarrow \{a < 0$ *und* $-1 = -1\}$

$b := -1;$

$\{a < 0$ *und* $b = -1\}$

$\Rightarrow \{a \cdot b > 0$ *und* $a \neq 0\}$

$\{a \cdot b > 0$ *und* $a \neq 0\}$

Hoare-Regeln und partielle Korrektheit

Beispiel zur Verifikation von bedingten Anweisungen (Fortsetzung)

```
if (a > b) then
   begin
      x := a − b;
      b := b − a;
      a := x;
   end
else
   a := b;
```

Hoare-Regeln und partielle Korrektheit

Beispiel zur Verifikation von bedingten Anweisungen (Fortsetzung)

$\{a \cdot b \geq 0\}$

`if` $(a > b)$ `then`

`begin`

$x := a - b;$

$b := b - a;$

$a := x;$

`end`

`else`

$a := b;$

$\{a \cdot b < 0\}$

Ist die Nachbedingung gültig bei dieser Vorbedingung?

Hoare-Regeln und partielle Korrektheit

Beispiel zur Verifikation von bedingten Anweisungen (Fortsetzung)

$\{a \cdot b \geq 0\}$

`if` $(a > b)$ `then`

  $\{a \cdot b \geq 0$ *und* $a > b\}$

  `begin`

    $x := a - b;$

    $b := b - a;$

    $a := x;$

  `end`

  $\{\ ???\ \}$

`else`

  $\{a \cdot b \geq 0$ *und* $a \leq b\}$

  $a := b;$

  $\{\ ???\ \}$

$\{a \cdot b < 0\}$

Ist die Nachbedingung gültig bei dieser Vorbedingung?

Hoare-Regeln und partielle Korrektheit

Beispiele zur Verifikation von bedingten Anweisungen (Fortsetzung)

Then-Zweig

$\{a \cdot b \geq 0\}$

`if` $(a > b)$ `then`

`begin`

$x := a - b;$

$b := b - a;$

$a := x;$

`end`

Hoare-Regeln und partielle Korrektheit

Beispiele zur Verifikation von bedingten Anweisungen (Fortsetzung)

Then-Zweig

$\{a \cdot b \geq 0\}$

`if` $(a > b)$ `then`

  $\{a \cdot b \geq 0$ *und* $a > b\}$

  `begin`

    $\{a \cdot b \geq 0$ *und* $a > b\}$

    $x := a - b;$

    $b := b - a;$

    $a := x;$

  `end`

Hoare-Regeln und partielle Korrektheit

Beispiele zur Verifikation von bedingten Anweisungen (Fortsetzung)

Then-Zweig

$\{a \cdot b \geq 0\}$

`if` $(a > b)$ `then`

$\{a \cdot b \geq 0$ *und* $a > b\}$

`begin`

$\{a \cdot b \geq 0$ *und* $a > b\}$

$\Rightarrow \{a \cdot b \geq 0$ *und* $a > b$ *und* $a - b = a - b\}$

$x := a - b;$

$\{a \cdot b \geq 0$ *und* $a > b$ *und* $x = a - b\}$

$\Rightarrow \{a \cdot (b - a + a) \geq 0$ *und* $0 > b - a$ *und* $-x = b - a\}$

$b := b - a;$

$\{a \cdot (b + a) \geq 0$ *und* $0 > b$ *und* $-x = b\}$

$\Rightarrow \{0 > b$ *und* $-x = b$ *und* $x = x\}$

$a := x;$

$\{0 > b$ *und* $-x = b$ *und* $a = x\}$

`end`

Hoare-Regeln und partielle Korrektheit

Beispiele zur Verifikation von bedingten Anweisungen (Fortsetzung)

Then-Zweig

$\{a \cdot b \geq 0\}$

`if` $(a > b)$ `then`

$\{a \cdot b \geq 0$ *und* $a > b\}$

`begin`

$\{a \cdot b \geq 0$ *und* $a > b\}$

$\Rightarrow \{a \cdot b \geq 0$ *und* $a > b$ *und* $a - b = a - b\}$

$x := a - b;$

$\{a \cdot b \geq 0$ *und* $a > b$ *und* $x = a - b\}$

$\Rightarrow \{a \cdot (b - a + a) \geq 0$ *und* $0 > b - a$ *und* $-x = b - a\}$

$b := b - a;$

$\{a \cdot (b + a) \geq 0$ *und* $0 > b$ *und* $-x = b\}$

$\Rightarrow \{0 > b$ *und* $-x = b$ *und* $x = x\}$

$a := x;$

$\{0 > b$ *und* $-x = b$ *und* $a = x\}$

$\Rightarrow \{0 > b$ *und* $a > 0\}$

$\Rightarrow \{a \cdot b < 0\}$

`end`

$\{a \cdot b < 0\}$

Hoare-Regeln und partielle Korrektheit

Beispiel zur Verifikation von bedingten Anweisungen (Fortsetzung)

Else-Zweig

$\{a \cdot b \geq 0\}$

`if` $(a > b)$ `then`

...

`else`

$a := b;$

$\{a \cdot b < 0\}$

Hoare-Regeln und partielle Korrektheit

Beispiel zur Verifikation von bedingten Anweisungen (Fortsetzung)

Else-Zweig

$\{a \cdot b \geq 0\}$

`if` $(a > b)$ `then`

...

`else`

$\{a \cdot b \geq 0$ *und* $a \leq b\}$

$a := b;$

$\{a \cdot b < 0\}$

Hoare-Regeln und partielle Korrektheit

Beispiel zur Verifikation von bedingten Anweisungen (Fortsetzung)

Else-Zweig

$\{a \cdot b \geq 0\}$

`if` $(a > b)$ `then`

...

`else`

$\{a \cdot b \geq 0$ *und* $a \leq b\}$

$\Rightarrow \{b = b\}$

$a := b;$

$\{a = b\}$

$\{a \cdot b < 0\}$

Hoare-Regeln und partielle Korrektheit

Beispiel zur Verifikation von bedingten Anweisungen (Fortsetzung)

Else-Zweig

$\{a \cdot b \geq 0\}$

`if` $(a > b)$ `then`

...

$\{a \cdot b < 0\}$

`else`

$\{a \cdot b \geq 0$ *und* $a \leq b\}$

$\Rightarrow \{b = b\}$

$a := b;$

$\{a = b\}$

$\Rightarrow \{a \cdot b = a^2\}$

$\Rightarrow \{a \cdot b \geq 0\}$

$\not\Rightarrow \{a \cdot b < 0\}$

$\{a \cdot b < 0\}$

Nachbedingung nicht gültig.

Hoare-Regeln und partielle Korrektheit

Hoare-Regel für Schleifen

$$L: \quad \frac{\{I \textit{ und } B\}\ S\ \{I\}}{\{I\}\ \texttt{while}\ (B)\ \texttt{do}\ S\ \{I \textit{ und } (\textit{nicht } B)\}}$$

- Die Zusicherung I heißt *Invariante* der Schleife.
- Nach Voraussetzung gilt nach dem Schleifenrumpf S die Zusicherung I, wenn $(I \textit{ und } B)$ vor dem Schleifenrumpf galt. Wenn I vor Ausführung der Schleife gilt, dann gilt I in jedem Zustand nach einer Ausführung des Schleifenrumpfes S.
- Da I nach jeder Ausführung des Schleifenrumpfes gilt, so gilt I nach der Schleife, sofern diese terminiert.
- Die Schleife wird beendet, wenn die Schleifenbedingung nicht mehr gilt. Also ist $(I \textit{ und nicht } B)$ in diesem Fall die Nachbedingung der Schleife.
- Wenn die Schleifenbedingung von Anfang an nicht gilt, so wird die Schleife nicht durchlaufen. Da I vor der Schleife gilt, so gilt nach der Schleife $(I \textit{ und nicht } B)$.

Bemerkungen:

- Die Verifikation mit der Schleifenregel zeigt nicht das Terminieren der Schleife.
- Das Finden der Invarianten stellt in der Programmverifikation i.d.R. den schwierigsten Schritt dar.
- Die Verifikation einer Schleife entspricht einem induktiven Beweis. Die Invariante entspricht der Induktionsbehauptung.

Hoare-Regeln und partielle Korrektheit

Beispiel zur Anwendung der Schleifenregel

$\{x = a$ *und* $y = b$ *und* $x \geq 0\}$

```
while (x > 0) do
  begin
    x := x - 1;
    y := y + 1;
  end
```

Hoare-Regeln und partielle Korrektheit

Beispiel zur Anwendung der Schleifenregel

$\{x = a$ *und* $y = b$ *und* $x \geq 0\}$

$\Rightarrow \{x + y = a + b$ *und* $x \geq 0\}$ Invariante

`while` $(x > 0)$ `do`

`begin`

$x := x - 1;$

$y := y + 1;$

`end`

Hoare-Regeln und partielle Korrektheit

Beispiel zur Anwendung der Schleifenregel

$\{x = a$ *und* $y = b$ *und* $x \geq 0\}$

$\Rightarrow \{x + y = a + b$ *und* $x \geq 0\}$ Invariante

`while` $(x > 0)$ `do`

$\{x + y = a + b$ *und* $x \geq 0$ *und* $x > 0\}$

`begin`

$\{x + y = a + b$ *und* $x \geq 0$ *und* $x > 0\}$

$x := x - 1;$

$y := y + 1;$

$\{x + y = a + b$ *und* $x \geq 0\}$

`end`

$\{x + y = a + b$ *und* $x \geq 0\}$

$\{x + y = a + b$ *und* $x \geq 0$ *und* $(\textit{nicht } x > 0)\}$

Hoare-Regeln und partielle Korrektheit

Beispiel zur Anwendung der Schleifenregel

$\{x = a$ *und* $y = b$ *und* $x \geq 0\}$

$\Rightarrow \{x + y = a + b$ *und* $x \geq 0\}$ Invariante

`while` $(x > 0)$ `do`

$\{x + y = a + b$ *und* $x \geq 0$ *und* $x > 0\}$

`begin`

$\{x + y = a + b$ *und* $x \geq 0$ *und* $x > 0\}$

$\Rightarrow \{x - 1 + y + 1 = a + b$ *und* $x - 1 \geq 0\}$

$x := x - 1;$

$\{x + y + 1 = a + b$ *und* $x \geq 0\}$

$y := y + 1;$

$\{x + y = a + b$ *und* $x \geq 0\}$

`end`

$\{x + y = a + b$ *und* $x \geq 0\}$

$\{x + y = a + b$ *und* $x \geq 0$ *und* $(\textit{nicht } x > 0)\}$

Hoare-Regeln und partielle Korrektheit

Beispiel zur Anwendung der Schleifenregel

$\{x = a$ *und* $y = b$ *und* $x \geq 0\}$

$\Rightarrow \{x + y = a + b$ *und* $x \geq 0\}$ Invariante

`while` $(x > 0)$ `do`

$\{x + y = a + b$ *und* $x \geq 0$ *und* $x > 0\}$

`begin`

$\{x + y = a + b$ *und* $x \geq 0$ *und* $x > 0\}$

$\Rightarrow \{x - 1 + y + 1 = a + b$ *und* $x - 1 \geq 0\}$

$x := x - 1;$

$\{x + y + 1 = a + b$ *und* $x \geq 0\}$

$y := y + 1;$

$\{x + y = a + b$ *und* $x \geq 0\}$

`end`

$\{x + y = a + b$ *und* $x \geq 0\}$

$\{x + y = a + b$ *und* $x \geq 0$ *und* $(\textit{nicht } x > 0)\}$

$\Rightarrow \{x + y = a + b$ *und* $x = 0\}$

$\Rightarrow \{y = a + b\}$

Hoare-Regeln und partielle Korrektheit

Anwendung der Regeln für bedingte Anweisungen

- Wie entdeckt man eine Invariante?
  - Bei der Programmerstellung kann eine Invariante zur Verifikation vorgegeben und als Kommentar in den Programmtext eingefügt werden.
  - Ansonsten ist die einzige Möglichkeit,
    - die Implementation vollständig zu begreifen,
    - aus Durchläufen durch den Schleifenrumpf mit Beispielwerten ein Verständnis für die Veränderung der Zustände zu entwickeln und
    - dieses Verständnis als eine Invariante zu formulieren.
- Invarianten sind nicht eindeutig.
- Invarianten sind häufig konjunktiv verknüpften Aussagen.

Hoare-Regeln und partielle Korrektheit

Beispiel zur Anwendung der Schleifenregel: Abrollen der Schleife

```
while (x > 0) do
   begin
      x := x − 1;
      y := y + 1;
   end
```

```
if (x > 0) then
   begin
      x := x − 1;
      y := y + 1;
   end

if (x > 0) then
   begin
      x := x − 1;
      y := y + 1;
   end

if (x > 0) then
   begin
      x := x − 1;
      y := y + 1;
   end

      ...
```

Hoare-Regeln und partielle Korrektheit

Beispiel zur Anwendung der Schleifenregel: Abrollen der Schleife (Fortsetzung)

Suche nach einer Invarianten

- Betrachte Werteverlauf in der Schleife für beteiligte Variablen.
- Suche invariante Zusammenhänge zwischen Variablen.

$\{x = a$ *und* $y = b$ *und* $x \geq 0\}$

```
while (x > 0) do
   begin
      x := x − 1;
      y := y + 1;
   end
```

Variablenwerte bei Test der Bedingung in `while`

	a	b	x	y
0	a	b	a	b
1	a	b	$a-1$	$b+1$
2	a	b	$a-2$	$b+2$
3	a	b	$a-3$	$b+3$
4	a	b	$a-4$	$b+4$

➜ Invariante: $\{x + y = a + b$ *und* $x \geq 0\}$

Hoare-Regeln und partielle Korrektheit

Beispiel zur Anwendung der Schleifenregel: Abrollen der Schleife (Fortsetzung)

$\{x + y = a$ *und* $x \geq 0\}$ Invariante

```
if (x > 0) then

  begin



    x := x − 1;

    y := y + 1;

  end

  // empty else branch


if (x > 0) then

    x := x − 1;
    y := y + 1;
  end

    ...
```

Hoare-Regeln und partielle Korrektheit

Beispiel zur Anwendung der Schleifenregel: Abrollen der Schleife (Fortsetzung)

$\{x + y = a$ *und* $x \geq 0\}$ Invariante

`if` $(x > 0)$ `then`

  $\{x + y = a$ *und* $x \geq 0$ *und* $x > 0\}$

  `begin`

    $\{x + y = a$ *und* $x \geq 0$ *und* $x > 0\}$

    $\Rightarrow \{x - 1 + y + 1 = a$ *und* $x - 1 \geq 0\}$

    $x := x - 1;$

    $\{x + y + 1 = a$ *und* $x \geq 0\}$

    $y := y + 1;$

    $\{x + y = a$ *und* $x \geq 0\}$

  `end`

  $\{x + y = a$ *und* $x \geq 0\}$

  `// empty else branch`

  $\{x + y = a$ *und* $x \geq 0$ *und* $(\textit{nicht}\ x > 0)\} \Rightarrow \{x + y = a$ *und* $x \geq 0\}$

$\{x + y = a$ *und* $x \geq 0\}$ Invariante

`if` $(x > 0)$ `then`

  `begin`

    $x := x - 1;$

    $y := y + 1;$

  `end`

$\{x + y = a$ *und* $x \geq 0\}$ Invariante

$\ldots$

➜ Beachte Ähnlichkeit zur Verifikation der Schleife!

Hoare-Regeln und partielle Korrektheit

Beispiel zu Schleifeninvarianten

Programmfragment mit Vor- und Nachbedingungen:

$\{n \in \mathbf{N}_0\}$

```
begin
    i := 0;
    x := 0;
    while (i < n) do
        begin
            i := i + 1;
            x := x + i;
        end
end
```

$\{n \in \mathbf{N}_0$ *und* $x = \sum_{i=0}^{n} i\}$

Ist eine Kombination aus drei der folgenden Teilausdrücke als Invariante möglich?

$$I_0 = (n, i \in \mathbf{N}_0), I_1 = (n \geq i), I_2 = (2x = i^2), I_3 = (x = \frac{i(i+1)}{2}), I_4 = (i \geq n)$$

Hoare-Regeln und partielle Korrektheit

Beispiel zu Schleifeninvarianten (Fortsetzung)

Verifikation des Anfangsstückes

$\{n \in \mathbf{N}_0\}$

```
begin
```

$i := 0;$

$x := 0;$

```
while (i < n) do
   begin
      i := i + 1;
      x := x + i;
   end
end
```

$\{n \in \mathbf{N}_0$ *und* $x = \sum_{i=0}^{n} i\}$

Hoare-Regeln und partielle Korrektheit

Beispiel zu Schleifeninvarianten (Fortsetzung)

Verifikation des Anfangsstückes

$\{n \in \mathbf{N}_0\}$

```
begin
```

$\{n \in \mathbf{N}_0\}$

$\Rightarrow \{n \in \mathbf{N}_0 \textit{ und } 0 = 0\}$

$i := 0;$

$\{n \in \mathbf{N}_0 \textit{ und } i = 0\}$

$\Rightarrow \{n \in \mathbf{N}_0 \textit{ und } i = 0 \textit{ und } 0 = 0\}$

$x := 0;$

$\{n \in \mathbf{N}_0 \textit{ und } i = 0 \textit{ und } x = 0\}$

```
while (i < n) do
   begin
      i := i + 1;
      x := x + i;
   end
end
```

$\{n \in \mathbf{N}_0 \textit{ und } x = \sum_{i=0}^{n} i\}$

Hoare-Regeln und partielle Korrektheit

Beispiel zu Schleifeninvarianten (Fortsetzung)

Test der Invarianten $n, i \in \mathbf{N}_0$ ✓

Test der Invarianten $n \geq i$

$\{n \in \mathbf{N}_0$ *und* $i = 0$ *und* $x = 0\}$

```
while (i < n) do
  begin
    i := i + 1;
    x := x + i;
  end
end
```

Hoare-Regeln und partielle Korrektheit

Beispiel zu Schleifeninvarianten (Fortsetzung)

Test der Invarianten $n, i \in \mathbf{N}_0$ ✓

Test der Invarianten $n \geq i$

$\{n \in \mathbf{N}_0$ *und* $i = 0$ *und* $x = 0\}$

$\Rightarrow \{n, i \in \mathbf{N}_0$ *und* $n \geq i$ *und* ...$\}$

```
while (i < n) do
    {n, i ∈ N_0 und n ≥ i und ... und n > i}
    begin
        {n, i ∈ N_0 und n ≥ i und ... und n > i}

        i := i + 1;

        x := x + i;

    end

end
```

Hoare-Regeln und partielle Korrektheit

Beispiel zu Schleifeninvarianten (Fortsetzung)

Test der Invarianten $n, i \in \mathbf{N}_0$ ✓

Test der Invarianten $n \geq i$

$\{n \in \mathbf{N}_0$ *und* $i = 0$ *und* $x = 0\}$

$\Rightarrow \{n, i \in \mathbf{N}_0$ *und* $n \geq i$ *und* ...$\}$

`while` $(i < n)$ `do`

  $\{n, i \in \mathbf{N}_0$ *und* $n \geq i$ *und* ... *und* $n > i\}$

  `begin`

    $\{n, i \in \mathbf{N}_0$ *und* $n \geq i$ *und* ... *und* $n > i\}$

    $\Rightarrow \{n, i \in \mathbf{N}_0$ *und* $n > i$ *und* ...$\} \Rightarrow \{n, (i+1) \in \mathbf{N}_0$ *und* $n \geq i+1$ *und* ...$\}$

    $i := i + 1;$

    $\{n, i \in \mathbf{N}_0$ *und* $n \geq i$ *und* ...$\}$

    $x := x + i;$

    $\{n, i \in \mathbf{N}_0$ *und* $n \geq i$ *und* ...$\}$

  `end`

  $\{n, i \in \mathbf{N}_0$ *und* $n \geq i$ *und* ...$\}$

`end`

Also ist Zusicherung $n \geq i$ als Invariante geeignet.

Hoare-Regeln und partielle Korrektheit

Beispiel zu Schleifeninvarianten (Fortsetzung)

Test der Invarianten $2x = i^2$

$\{n \in \mathbf{N}_0$ *und* $i = 0$ *und* $x = 0\}$

`while` $(i < n)$ `do`

`begin`

$i := i + 1;$

$x := x + i;$

`end`

`end`

Hoare-Regeln und partielle Korrektheit

Beispiel zu Schleifeninvarianten (Fortsetzung)

Test der Invarianten $2x = i^2$

$\{n \in \mathbf{N}_0$ *und* $i = 0$ *und* $x = 0\} \Rightarrow \{n, i \in \mathbf{N}_0$ *und* $2x = i^2$ *und* ...$\}$

```
while (i < n) do
```

$\{n, i \in \mathbf{N}_0$ *und* $2x = i^2$ *und* ... *und* $n > i\}$

```
begin
```

$\{n, i \in \mathbf{N}_0$ *und* $2x = i^2$ *und* ... *und* $n > i\}$

$i := i + 1;$

$x := x + i;$

```
end
end
```

Hoare-Regeln und partielle Korrektheit

Beispiel zu Schleifeninvarianten (Fortsetzung)

Test der Invarianten $2x = i^2$

$\{n \in \mathbf{N}_0$ *und* $i = 0$ *und* $x = 0\} \Rightarrow \{n, i \in \mathbf{N}_0$ *und* $2x = i^2$ *und* ...$\}$

`while` $(i < n)$ `do`

$\{n, i \in \mathbf{N}_0$ *und* $2x = i^2$ *und* ... *und* $n > i\}$

`begin`

$\{n, i \in \mathbf{N}_0$ *und* $2x = i^2$ *und* ... *und* $n > i\}$

$\Rightarrow \{n, (i+1) \in \mathbf{N}_0$ *und* $2x = (i+1-1)^2$ *und* $n \geq i+1$ *und* ...$\}$

$i := i + 1;$

$\{n, i \in \mathbf{N}_0$ *und* $2x = (i-1)^2$ *und* $n \geq i$ *und* ...$\}$

$\Rightarrow \{n \in \mathbf{N}_0$ *und* $2(x + i - i) = (i-1)^2$ *und* $n \geq i$ *und* ...$\}$

$x := x + i;$

$\{n, i \in \mathbf{N}_0$ *und* $2(x - i) = (i-1)^2$ *und* $n \geq i$ *und* ...$\}$

$\Rightarrow \{n, i \in \mathbf{N}_0$ *und* $2x - 2i = i^2 - 2i + 1$ *und* $n \geq i$ *und* ...$\}$

`end`

`end`

Hoare-Regeln und partielle Korrektheit

Beispiel zu Schleifeninvarianten (Fortsetzung)

Test der Invarianten $2x = i^2$

$\{n \in \mathbf{N}_0$ *und* $i = 0$ *und* $x = 0\} \Rightarrow \{n, i \in \mathbf{N}_0$ *und* $2x = i^2$ *und* ...$\}$

`while` $(i < n)$ `do`

$\{n, i \in \mathbf{N}_0$ *und* $2x = i^2$ *und* ... *und* $n > i\}$

`begin`

$\{n, i \in \mathbf{N}_0$ *und* $2x = i^2$ *und* ... *und* $n > i\}$

$\Rightarrow \{n, (i+1) \in \mathbf{N}_0$ *und* $2x = (i+1-1)^2$ *und* $n \geq i+1$ *und* ...$\}$

$i := i + 1;$

$\{n, i \in \mathbf{N}_0$ *und* $2x = (i-1)^2$ *und* $n \geq i$ *und* ...$\}$

$\Rightarrow \{n \in \mathbf{N}_0$ *und* $2(x + i - i) = (i-1)^2$ *und* $n \geq i$ *und* ...$\}$

$x := x + i;$

$\{n, i \in \mathbf{N}_0$ *und* $2(x - i) = (i-1)^2$ *und* $n \geq i$ *und* ...$\}$

$\Rightarrow \{n, i \in \mathbf{N}_0$ *und* $2x - 2i = i^2 - 2i + 1$ *und* $n \geq i$ *und* ...$\}$

$\not\Rightarrow \{n, i \in \mathbf{N}_0$ *und* $2x = i^2$ *und* ...$\}$

`end`

`end`

Also ist Zusicherung $2x = i^2$ als Invariante nicht geeignet.

Hoare-Regeln und partielle Korrektheit

Beispiel zu Schleifeninvarianten (Fortsetzung)

Test der Invarianten $x = \frac{1}{2}i(i+1)$

$\{n \in \mathbf{N}_0$ *und* $i = 0$ *und* $x = 0\}$

```
while (i < n) do

  begin


    i := i + 1;


    x := x + i;


  end
end
```

Hoare-Regeln und partielle Korrektheit

Beispiel zu Schleifeninvarianten (Fortsetzung)

Test der Invarianten $x = \frac{1}{2}i(i+1)$

$\{n \in \mathbf{N}_0$ *und* $i = 0$ *und* $x = 0\} \Rightarrow \{n, i \in \mathbf{N}_0$ *und* $x = \frac{1}{2}i(i+1)$ *und* ...$\}$

```
while (i < n) do
```

$\{n, i \in \mathbf{N}_0$ *und* $x = \frac{1}{2}i(i+1)$ *und* ... *und* $n > i\}$

```
begin
```

$\{n, i \in \mathbf{N}_0$ *und* $x = \frac{1}{2}i(i+1)$ *und* ... *und* $n > i\}$

$i := i + 1;$

$x := x + i;$

```
end
end
```

Hoare-Regeln und partielle Korrektheit

Beispiel zu Schleifeninvarianten (Fortsetzung)

Test der Invarianten $x = \frac{1}{2}i(i+1)$

$\{n \in \mathbf{N}_0$ *und* $i = 0$ *und* $x = 0\} \Rightarrow \{n, i \in \mathbf{N}_0$ *und* $x = \frac{1}{2}i(i+1)$ *und* ...$\}$

`while` $(i < n)$ `do`

$\{n, i \in \mathbf{N}_0$ *und* $x = \frac{1}{2}i(i+1)$ *und* ... *und* $n > i\}$

`begin`

$\{n, i \in \mathbf{N}_0$ *und* $x = \frac{1}{2}i(i+1)$ *und* ... *und* $n > i\}$

$\Rightarrow \{n, (i+1) \in \mathbf{N}_0$ *und* $x = \frac{1}{2}(i+1-1)(i+1)$ *und* $n \geq i+1$ *und* ...$\}$

$i := i + 1;$

$\{n, i \in \mathbf{N}_0$ *und* $x = \frac{1}{2}(i-1)i, n \geq i$ *und* ...$\}$

$\Rightarrow \{n, i \in \mathbf{N}_0$ *und* $x + i - i = \frac{1}{2}(i-1)i$ *und* $n \geq i$ *und* ...$\}$

$x := x + i;$

$\{n, i \in \mathbf{N}_0$ *und* $x - i = \frac{1}{2}(i-1)i$ *und* $n \geq i$ *und* ...$\}$

`end`

`end`

Hoare-Regeln und partielle Korrektheit

Beispiel zu Schleifeninvarianten (Fortsetzung)

Test der Invarianten $x = \frac{1}{2}i(i+1)$

$\{n \in \mathbf{N}_0$ *und* $i = 0$ *und* $x = 0\} \Rightarrow \{n, i \in \mathbf{N}_0$ *und* $x = \frac{1}{2}i(i+1)$ *und* ...$\}$

`while` $(i < n)$ `do`

$\{n, i \in \mathbf{N}_0$ *und* $x = \frac{1}{2}i(i+1)$ *und* ... *und* $n > i\}$

`begin`

$\{n, i \in \mathbf{N}_0$ *und* $x = \frac{1}{2}i(i+1)$ *und* ... *und* $n > i\}$

$\Rightarrow \{n, (i+1) \in \mathbf{N}_0$ *und* $x = \frac{1}{2}(i+1-1)(i+1)$ *und* $n \geq i+1$ *und* ...$\}$

$i := i + 1;$

$\{n, i \in \mathbf{N}_0$ *und* $x = \frac{1}{2}(i-1)i, n \geq i$ *und* ...$\}$

$\Rightarrow \{n, i \in \mathbf{N}_0$ *und* $x + i - i = \frac{1}{2}(i-1)i$ *und* $n \geq i$ *und* ...$\}$

$x := x + i;$

$\{n, i \in \mathbf{N}_0$ *und* $x - i = \frac{1}{2}(i-1)i$ *und* $n \geq i$ *und* ...$\}$

$\Rightarrow \{n, i \in \mathbf{N}_0$ *und* $x = \frac{1}{2}((i-1)i + 2i)$ *und* $n \geq i$ *und* ...$\}$

$\Rightarrow \{n, i \in \mathbf{N}_0$ *und* $x = \frac{1}{2}i(i+1)$ *und* $n \geq i$ *und* ...$\}$

`end`

`end`

Also ist Zusicherung $x = \frac{1}{2}i(i+1)$ als Invariante geeignet.

Hoare-Regeln und partielle Korrektheit

Beispiel zu Schleifeninvarianten (Fortsetzung)

Test der Invarianten $i \geq n$

$\{n \in \mathbf{N}_0$ *und* $i = 0$ *und* $x = 0\}$

```
    while (i < n) do
      begin
        i := i + 1;
        x := x + i;
      end
end
```

Hoare-Regeln und partielle Korrektheit

Beispiel zu Schleifeninvarianten (Fortsetzung)

Test der Invarianten $i \geq n$

$\{n \in \mathbf{N}_0$ *und* $i = 0$ *und* $x = 0\}$

$\not\Rightarrow \{n \in \mathbf{N}_0$ *und* $i \geq n$ *und* ...$\}$

```
while (i < n) do
   begin
      i := i + 1;
      x := x + i;
   end
end
```

Also ist Zusicherung $i \geq n$ als Invariante nicht geeignet.

Hoare-Regeln und partielle Korrektheit

Beispiel zu Schleifeninvarianten (Fortsetzung)

Partielle Korrektheit: Verifikation mit Invariante $\{n, i \in \mathbf{N}_0 \textit{ und } n \geq i \textit{ und } x = \frac{1}{2}i(i+1)\}$

$\{n \in \mathbf{N}_0 \textit{ und } i = 0 \textit{ und } x = 0\} \Rightarrow \{n, i \in \mathbf{N}_0 \textit{ und } n \geq i \textit{ und } x = \frac{1}{2}i(i+1)\}$

`while` $(i < n)$ `do`

$\{n, i \in \mathbf{N}_0 \textit{ und } n \geq i \textit{ und } x = \frac{1}{2}i(i+1) \textit{ und } n > i\}$

`begin`

$\{n, i \in \mathbf{N}_0 \textit{ und } n \geq i \textit{ und } x = \frac{1}{2}i(i+1) \textit{ und } n > i\}$

$\Rightarrow \{n, (i+1) \in \mathbf{N}_0 \textit{ und } x = \frac{1}{2}(i+1-1)(i+1) \textit{ und } n \geq i+1\}$

$i := i + 1;$

$\{n, i \in \mathbf{N}_0 \textit{ und } x = \frac{1}{2}(i-1)i \textit{ und } n \geq i\}$

$\Rightarrow \{n, i \in \mathbf{N}_0 \textit{ und } x + i - i = \frac{1}{2}(i-1)i \textit{ und } n \geq i\}$

$x := x + i;$

$\{n, i \in \mathbf{N}_0 \textit{ und } x - i = \frac{1}{2}(i-1)i \textit{ und } n \geq i\}$

$\Rightarrow \{n, i \in \mathbf{N}_0 \textit{ und } x = \frac{1}{2}((i-1)i + 2i) \textit{ und } n \geq i\} \Rightarrow \{n, i \in \mathbf{N}_0 \textit{ und } x = \frac{1}{2}i(i+1) \textit{ und } n \geq i\}$

`end`

$\{n, i \in \mathbf{N}_0 \textit{ und } x = \frac{1}{2}i(i+1) \textit{ und } n \geq i\}$

$\{n, i \in \mathbf{N}_0 \textit{ und } x = \frac{1}{2}i(i+1) \textit{ und } n \geq i \textit{ und } i \geq n\}$

$\Rightarrow \{n, i \in \mathbf{N}_0 \textit{ und } x = \frac{1}{2}i(i+1) \textit{ und } n = i\} \Rightarrow \{n, i \in \mathbf{N}_0 \textit{ und } x = \frac{1}{2}n(n+1)\}$

`end`

$\{n \in \mathbf{N}_0 \textit{ und } x = \frac{1}{2}n(n+1)\} \Rightarrow \{n \in \mathbf{N}_0 \textit{ und } x = \sum_{i=0}^{n} i\}$

Hoare-Regeln und partielle Korrektheit

Beispiel Einfaches Potenzieren

Idee des Algorithmus: Rückführung auf die iterierte Multiplikation

Spezifikation: Vorbedingung: $\{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0\}$
Nachbedingung: $\{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0$ *und* $b = x^n\}$

```
begin
    a := x;
    b := 1;
    i := n;
    while (i > 0) do
        begin
            b := b * a;
            i := i - 1;
        end
end
```

Variable x und n sind Eingabewerte, Variable b speichert das Ergebnis.

Hoare-Regeln und partielle Korrektheit

Beispiel Einfaches Potenzieren (Fortsetzung)

Spezifikation: Vorbedingung: $\{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0\}$
Nachbedingung: $\{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0$ *und* $b = x^n\}$

$\{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0\}$

```
begin
    a := x;
    b := 1;
    i := n;
    while (i > 0) do
        begin
            b := b * a;
            i := i - 1;
        end
end
```

$\{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0$ *und* $b = x^n\}$

Hoare-Regeln und partielle Korrektheit

Beispiel Einfaches Potenzieren (Fortsetzung)

Spezifikation: Vorbedingung: $\{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0\}$
Nachbedingung: $\{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0$ *und* $b = x^n\}$

$\{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0\}$

```
begin
    a := x;
    b := 1;
    i := n;
    while (i > 0) do
      begin
        b := b * a;
        i := i - 1;
      end
end
```

Hoare-Regeln und partielle Korrektheit

Beispiel Einfaches Potenzieren (Fortsetzung)

Spezifikation: Vorbedingung: $\{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0\}$
Nachbedingung: $\{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0$ *und* $b = x^n\}$

$\{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0\}$

```
begin
```

$\{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0\}$

$\Rightarrow \{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0$ *und* $x = x\}$

$a := x;$

$\{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0$ *und* $a = x\}$

$\Rightarrow \{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0$ *und* $a = x$ *und* $1 = 1\}$

$b := 1;$

$\{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0$ *und* $a = x$ *und* $b = 1\}$

$\Rightarrow \{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0$ *und* $a = x$ *und* $b = 1$ *und* $n = n\}$

$i := n;$

$\{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0$ *und* $a = x$ *und* $b = 1$ *und* $i = n\}$

```
while (i > 0) do
   begin
      b := b * a;
      i := i - 1;
   end
end
```

Hoare-Regeln und partielle Korrektheit

Beispiel Einfaches Potenzieren (Fortsetzung)

Suche nach einer Invarianten

- Tautologische Aussagen sind immer invariant, aber sie helfen nicht.
- Betrachte Werteverlauf in der Schleife für beteiligte Variablen.

```
begin
    a := x; b := 1; i := n;
    while (i > 0) do
        begin
            b := b * a;
            i := i - 1;
        end
end
```

Variablenwerte bei Test der Bedingung in `while`

	x	n	a	b	i
0	x	n	x	x^0	n
1	x	n	x	x^1	$n-1$
2	x	n	x	x^2	$n-2$
3	x	n	x	x^3	$n-3$
4	x	n	x	x^4	$n-4$

Invariante I: $\{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i \geq 0\}$

Hoare-Regeln und partielle Korrektheit

Beispiel Einfaches Potenzieren (Fortsetzung)

...

$\{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0$ *und* $a = x$ *und* $b = 1$ *und* $i = n\}$

`while` $(i > 0)$ `do`

`begin`

$b := b * a;$

$i := i - 1;$

`end`

`end`

$\{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0$ *und* $b = x^n\}$

Hoare-Regeln und partielle Korrektheit

Beispiel Einfaches Potenzieren (Fortsetzung)

...

$\{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0$ *und* $a = x$ *und* $b = 1$ *und* $i = n\}$

$\Rightarrow \{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i \geq 0\}$ Invariante

`while` $(i > 0)$ `do`

$\{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i \geq 0$ *und* $i > 0\}$

`begin`

$\{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i \geq 0$ *und* $i > 0\}$

$b := b * a;$

$i := i - 1;$

$\{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i \geq 0\}$

`end`

$\{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i \geq 0\}$

$\{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i \geq 0$ *und* $i \leq 0\}$

`end`

$\{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0$ *und* $b = x^n\}$

Hoare-Regeln und partielle Korrektheit

Beispiel Einfaches Potenzieren (Fortsetzung)

...

$\{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0$ *und* $a = x$ *und* $b = 1$ *und* $i = n\}$

$\Rightarrow \{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i \geq 0\}$ Invariante

`while` $(i > 0)$ `do`

$\{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i \geq 0$ *und* $i > 0\}$

`begin`

$\{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i \geq 0$ *und* $i > 0\}$

$\Rightarrow \{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i > 0\}$

$\Rightarrow \{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a * a^{i-1}$ *und* $i > 0\}$

$b := b * a;$

$\{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^{i-1}$ *und* $i > 0\}$

$\Rightarrow \{x \in \mathbf{R}$ *und* $n, (i-1) \in \mathbf{N}_0$ *und* $x^n = b * a^{i-1}$ *und* $i - 1 \geq 0\}$

$i := i - 1;$

$\{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i \geq 0\}$

`end`

$\{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i \geq 0\}$

$\{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i \geq 0$ *und* $i \leq 0\}$

`end`

$\{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0$ *und* $b = x^n\}$

Hoare-Regeln und partielle Korrektheit

Beispiel Einfaches Potenzieren (Fortsetzung)

...

$\{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0$ *und* $a = x$ *und* $b = 1$ *und* $i = n\}$

$\Rightarrow \{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i \geq 0\}$ Invariante

`while` $(i > 0)$ `do`

$\{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i \geq 0$ *und* $i > 0\}$

`begin`

$\{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i \geq 0$ *und* $i > 0\}$

$\Rightarrow \{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i > 0\}$

$\Rightarrow \{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a * a^{i-1}$ *und* $i > 0\}$

$b := b * a;$

$\{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^{i-1}$ *und* $i > 0\}$

$\Rightarrow \{x \in \mathbf{R}$ *und* $n, (i-1) \in \mathbf{N}_0$ *und* $x^n = b * a^{i-1}$ *und* $i - 1 \geq 0\}$

$i := i - 1;$

$\{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i \geq 0\}$

`end`

$\{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i \geq 0\}$

$\{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i \geq 0$ *und* $i \leq 0\}$

$\Rightarrow \{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i = 0\} \Rightarrow \{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0$ *und* $b = x^n\}$

`end`

$\{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0$ *und* $b = x^n\}$

Hoare-Regeln und partielle Korrektheit

Beispiel Effizientes Potenzieren

Idee des Algorithmus:

Quadrieren von Teilergebnissen spart mehr als die Hälfte der Multiplikationen.

Sei $n_k n_{k-1} \ldots n_2 n_1 n_0$ die Dualdarstellung von n, also

$$n = \sum_{i=0}^{k} n_i 2^i \qquad \text{mit } n_i = \begin{cases} 1 & \text{falls } n/2^i \text{ ungerade} \\ 0 & \text{sonst} \end{cases}$$

Dann gilt

$$x^n = x^{\sum_{i=0}^{k} n_i 2^i} = \prod_{i=0}^{k} (x^{2^i})^{n_i}$$

Hoare-Regeln und partielle Korrektheit

Beispiel Effizientes Potenzieren (Fortsetzung)

Spezifikation: Vorbedingung: $\{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0\}$
Nachbedingung: $\{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0$ *und* $b = x^n\}$

```
begin
    a := x;
    b := 1;
    i := n;
    while (i > 0) do
        begin
            if (i ungerade) then
                b := b * a;
            a := a^2;
            i := i/2;
        end
end
```

Hoare-Regeln und partielle Korrektheit

Beispiel Effizientes Potenzieren (Fortsetzung)

Spezifikation: Vorbedingung: $\{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0\}$
Nachbedingung: $\{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0$ *und* $b = x^n\}$

$\{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0\}$

```
begin
```

$a := x;$

$b := 1;$

$i := n;$

$\ldots$

Hoare-Regeln und partielle Korrektheit

Beispiel Effizientes Potenzieren (Fortsetzung)

Spezifikation: Vorbedingung: $\{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0\}$
Nachbedingung: $\{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0$ *und* $b = x^n\}$

$\{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0\}$

`begin`

$\{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0\}$

$\Rightarrow \{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0$ *und* $x = x\}$

$a := x;$

$\{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0$ *und* $a = x\}$

$\Rightarrow \{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0$ *und* $a = x$ *und* $1 = 1\}$

$b := 1;$

$\{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0$ *und* $a = x$ *und* $b = 1\}$

$\Rightarrow \{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0$ *und* $a = x$ *und* $b = 1$ *und* $n = n\}$

$i := n;$

$\{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0$ *und* $a = x$ *und* $b = 1$ *und* $i = n\}$

$\ldots$

Hoare-Regeln und partielle Korrektheit

Beispiel Effizientes Potenzieren (Fortsetzung)

Suche nach einer Invarianten

- Betrachte Werteverlauf in der Schleife für beteiligte Variablen.
- $n_k n_{k-1} ... n_2 n_1 n_0$ sei Dualzahldarstellung von n.

$a := x;\ b := 1;\ i := n;$
`while` $(i > 0)$ `do`
  `begin`
    `if` (i ungerade) `then`
      $b := b * a;$
    $a := a^2;$
    $i := i/2;$
  `end`

Variablenwerte bei Test der Bedingung in `while`

	x	n	a	b	i
0	x	n	x^1	1	$n_k n_{k-1} ... n_2 n_1 n_0$
1	x	n	x^2	x^{n_0}	$n_k n_{k-1} ... n_2 n_1$
2	x	n	x^4	$x^{n_1 n_0}$	$n_k n_{k-1} ... n_2$
3	x	n	x^8	$x^{n_2 n_1 n_0}$	$n_k n_{k-1} ... n_3$
4	x	n	x^{16}	$x^{n_3 n_2 n_1 n_0}$	$n_k n_{k-1} ... n_4$

Invariante: $\{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i \geq 0\}$

Hoare-Regeln und partielle Korrektheit

Beispiel Effizientes Potenzieren (Fortsetzung)

...

$\{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0$ *und* $a = x$ *und* $b = 1$ *und* $i = n\}$

`while` $(i > 0)$ `do`

`begin`

`if` $(i$ ungerade$)$ `then`

$b := b * a;$

$a := a^2;$

$i := i/2;$

`end`

...

Hoare-Regeln und partielle Korrektheit

Beispiel Effizientes Potenzieren (Fortsetzung)

...

$\{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0$ *und* $a = x$ *und* $b = 1$ *und* $i = n\} \Rightarrow \{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i \geq 0\}$ Inv.

`while` $(i > 0)$ `do`

`begin`

$\{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i \geq 0$ *und* $i > 0\}$

`if` $(i$ ungerade$)$ `then`

$b := b * a;$

$a := a^2;$

$i := i/2;$

$\{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i \geq 0\}$

`end`

$\{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i \geq 0$ *und* $i \leq 0\}$

...

Hoare-Regeln und partielle Korrektheit

Beispiel Effizientes Potenzieren (Fortsetzung)

...

$\{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0$ *und* $a = x$ *und* $b = 1$ *und* $i = n\} \Rightarrow \{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i \geq 0\}$ Inv.

`while` $(i > 0)$ `do`

`begin`

$\{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i \geq 0$ *und* $i > 0\} \Rightarrow \{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i > 0\}$

`if` (i ungerade) `then`

$\{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i > 0$ *und* i ungerade$\}$

$b := b * a;$

$\{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i > 0$ *und* i gerade$\}$ // leere Alternative

$a := a^2;$

$i := i/2;$

$\{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i \geq 0\}$

`end`

$\{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i \geq 0$ *und* $i \leq 0\}$

...

Hoare-Regeln und partielle Korrektheit

Beispiel Effizientes Potenzieren (Fortsetzung)

...

$\{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0$ *und* $a = x$ *und* $b = 1$ *und* $i = n\} \Rightarrow \{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i \geq 0\}$ Inv.

`while` $(i > 0)$ `do`

`begin`

$\{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i \geq 0$ *und* $i > 0\} \Rightarrow \{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i > 0\}$

`if` (i ungerade) `then`

$\{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i > 0$ *und* i ungerade$\}$

$\Rightarrow \{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a * (a^2)^{[i/2]}$ *und* $i > 0$ *und* i ungerade$\}$

$b := b * a;$

$\{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * (a^2)^{[i/2]}$ *und* $i > 0$ *und* i ungerade$\}$

$\Rightarrow \{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * (a^2)^{[i/2]}$ *und* $i > 0\}$

$\{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i > 0$ *und* i gerade$\}$ // leere Alternative

$\Rightarrow \{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * (a^2)^{[i/2]}$ *und* $i > 0$ *und* i gerade$\}$

$\Rightarrow \{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * (a^2)^{[i/2]}$ *und* $i > 0\}$

$a := a^2;$

$i := i/2;$

$\{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i \geq 0\}$

`end`

$\{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i \geq 0$ *und* $i \leq 0\}$

...

Hoare-Regeln und partielle Korrektheit

Beispiel Effizientes Potenzieren (Fortsetzung)

...

$\{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0$ *und* $a = x$ *und* $b = 1$ *und* $i = n\} \Rightarrow \{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i \geq 0\}$ Inv.

`while` $(i > 0)$ `do`

`begin`

$\{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i \geq 0$ *und* $i > 0\} \Rightarrow \{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i > 0\}$

`if` (i ungerade) `then`

$\{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i > 0$ *und* i ungerade$\}$

$\Rightarrow \{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a * (a^2)^{[i/2]}$ *und* $i > 0$ *und* i ungerade$\}$

$b := b * a;$

$\{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * (a^2)^{[i/2]}$ *und* $i > 0$ *und* i ungerade$\}$

$\Rightarrow \{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * (a^2)^{[i/2]}$ *und* $i > 0\}$

$\{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i > 0$ *und* i gerade$\}$ // leere Alternative

$\Rightarrow \{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * (a^2)^{[i/2]}$ *und* $i > 0$ *und* i gerade$\}$

$\Rightarrow \{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * (a^2)^{[i/2]}$ *und* $i > 0\}$

$\{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * (a^2)^{[i/2]}$ *und* $i > 0\}$

$a := a^2;$

$\{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^{[i/2]}$ *und* $i > 0\} \Rightarrow \{x \in \mathbf{R}$ *und* $n, [i/2] \in \mathbf{N}_0$ *und* $x^n = b * a^{[i/2]}$ *und* $[i/2] \geq 0\}$

$i := i/2;$

$\{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i \geq 0\}$

`end`

$\{x \in \mathbf{R}$ *und* $n, i \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i \geq 0$ *und* $i \leq 0\}$

...

Hoare-Regeln und partielle Korrektheit

Beispiel Effizientes Potenzieren (Fortsetzung)

...

$\{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i \geq 0$ *und* $i \leq 0\}$

end

$\{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0$ *und* $b = x^n\}$

Hoare-Regeln und partielle Korrektheit

Beispiel Effizientes Potenzieren (Fortsetzung)

...

$\{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i \geq 0$ *und* $i \leq 0\}$

$\Rightarrow \{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0$ *und* $x^n = b * a^i$ *und* $i = 0\}$

$\Rightarrow \{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0$ *und* $x^n = b\}$

`end`

$\{x \in \mathbf{R}$ *und* $n \in \mathbf{N}_0$ *und* $b = x^n\}$

Bemerkungen:

- Schleifeninvarianten sind Zusicherungen, d.h. sie beschreiben Zusammenhänge von Programmgrößen.
- Eine Invariante muss vor der Schleife gültig sein.
- Eine Invariante muss nach Durchlauf durch den Schleifenrumpf gültig sein, wenn sie vor dem Schleifenrumpf gültig war (zusammen mit der Schleifenbedingung).
- Invarianten sind zum Zeitpunkt der Implementierung leichter zu bestimmen.

Hoare-Regeln und partielle Korrektheit

Möglichkeiten zum Einsparen von Schreibarbeit

- Festlegungen des Grundbereiches wie $x \in \mathbf{R}$ oder $n \in \mathbf{N}$ werden in der Spezifikation für die Eingabevariablen benötigt. Da nach Vereinbarung die Eingabevariablen im Programm nicht verändert werden, können diese Festlegungen in alle Zusicherungen aufgenommen werden, ohne deren Gültigkeit zu verändern. Da sie aber nur sehr selten wirklich benötigt werden, kann man auf sie in kleinen Beispielen aus Gründen der Übersichtlichkeit verzichten.

  ➜ Festlegungen der Grundbereiche für Eingabevariablen könnte man in den Zusicherungen als bekannt voraussetzen.

- Alle einzelnen Bedingungen in den Zusicherungen sind konjunktiv verknüpft. Nur selten muss man Disjunktionen oder Negationen verwenden.

  ➜ Als Kurzform für die konjunktive Verknüpfung von Bedingungen könnte man ein Komma verwenden.

  Beispiel: $\{x^n = b * (a^2)^{[i/2]}, i > 0\}$