Formale Spezifikation und Verifikation
Schleifeninvarianten, Hoare-Logik

Wintersemester 2024
Übungsblatt 04

Prof. Dr. Gidon Ernst, Marian Lingsch-Rosenfeld, Simon Rossmair, Noah König

26. November 2024

Addieren durch Inkrementieren

$\mathtt{x} = \mathtt{x}_0, \mathtt{y} = \mathtt{y}_0;$

while $\mathtt{y} > 0$ **do**

$\quad \mathtt{x} = \mathtt{x} + 1;$

$\quad \mathtt{y} = \mathtt{y} - 1;$

end

Addieren durch Inkrementieren

$\{y_0 \geq 0 \land x_0 = x_0 \land y_0 = y_0\}$ Vorbedingung

$x = x_0, y = y_0;$

while $y > 0$ **do**

$\quad x = x + 1;$

$\quad y = y - 1;$

end

$\{x = x_0 + y_0\}$ Nachbedingung soll hier gelten

Addieren durch Inkrementieren

$\{y_0 \geq 0 \land x_0 = x_0 \land y_0 = y_0\}$ Vorbedingung

$x = x_0, y = y_0;$
$\{y \geq 0 \land x + y = x_0 + y_0\}$ Invariante initial zu zeigen
while $y > 0$ **do**

$x = x + 1;$

$y = y - 1;$

end
$\{y \leq 0 \land y \geq 0 \land x + y = x_0 + y_0\}$ Annahme: negierter Test & Invariante

$\{x = x_0 + y_0\}$ Nachbedingung soll hier gelten

Addieren durch Inkrementieren

$\{y_0 \geq 0 \land x_0 = x_0 \land y_0 = y_0\}$ Vorbedingung

$\{y_0 \geq 0 \land x_0 + y_0 = x_0 + y_0\}$ (*) Nebenrechnung

$x = x_0, y = y_0;$

$\{y \geq 0 \land x + y = x_0 + y_0\}$ Invariante initial zu zeigen

while $y > 0$ **do**

$\quad x = x + 1;$

$\quad y = y - 1;$

end

$\{y \leq 0 \land y \geq 0 \land x + y = x_0 + y_0\}$ Annahme: negierter Test & Invariante

$\{x + y = x + 0 = x_0 + y_0\}$ (*) Nebenrechnung

$\{x = x_0 + y_0\}$ Nachbedingung soll hier gelten

Addieren durch Inkrementieren

$\{y_0 \geq 0 \wedge x_0 = x_0 \wedge y_0 = y_0\}$ — Vorbedingung

$\{y_0 \geq 0 \wedge x_0 + y_0 = x_0 + y_0\}$ — (*) Nebenrechnung

$x = x_0, y = y_0;$

$\{y \geq 0 \wedge x + y = x_0 + y_0\}$ — Invariante initial zu zeigen

$\textbf{while } y > 0 \textbf{ do}$

$\quad \{y > 0 \wedge y \geq 0 \wedge x + y = x_0 + y_0\}$ — Annahme: Schleifentest & Invariante

$\quad x = x + 1;$

$\quad y = y - 1;$

$\quad \{y \geq 0 \wedge x + y = x_0 + y_0\}$ — Invariante gilt wieder

$\textbf{end}$

$\{y \leq 0 \wedge y \geq 0 \wedge x + y = x_0 + y_0\}$ — Annahme: negierter Test & Invariante

$\{x + y = x + 0 = x_0 + y_0\}$ — (*) Nebenrechnung

$\{x = x_0 + y_0\}$ — Nachbedingung soll hier gelten

Addieren durch Inkrementieren

$\{y_0 \geq 0 \land x_0 = x_0 \land y_0 = y_0\}$ Vorbedingung

$\{y_0 \geq 0 \land x_0 + y_0 = x_0 + y_0\}$ (*) Nebenrechnung

$x = x_0, y = y_0;$

$\{y \geq 0 \land x + y = x_0 + y_0\}$ Invariante initial zu zeigen

while $y > 0$ **do**

$\quad \{y > 0 \land y \geq 0 \land x + y = x_0 + y_0\}$ Annahme: Schleifentest & Invariante

$\quad \{y - 1 \geq 0 \land x + 1 + y - 1 = x_0 + y_0\}$ (*) Nebenrechnung

$\quad x = x + 1;$

$\quad \{y - 1 \geq 0 \land x + y - 1 = x_0 + y_0\}$

$\quad y = y - 1;$

$\quad \{y \geq 0 \land x + y = x_0 + y_0\}$ Invariante gilt wieder

end

$\{y \leq 0 \land y \geq 0 \land x + y = x_0 + y_0\}$ Annahme: negierter Test & Invariante

$\{x + y = x + 0 = x_0 + y_0\}$ (*) Nebenrechnung

$\{x = x_0 + y_0\}$ Nachbedingung soll hier gelten

Addieren durch Inkrementieren

$\{y_0 \geq 0 \land x_0 = x_0 \land y_0 = y_0\}$	Vorbedingung
$\{y_0 \geq 0 \land x_0 + y_0 = x_0 + y_0\}$	(*) Nebenrechnung
$x = x_0, y = y_0;$	
$\{y \geq 0 \land x + y = x_0 + y_0\}$	Invariante initial zu zeigen
$\textbf{while } y > 0 \textbf{ do}$	
$\quad \{y > 0 \land y \geq 0 \land x + y = x_0 + y_0\}$	Annahme: Schleifentest & Invariante
$\quad \{y - 1 \geq 0 \land x + 1 + y - 1 = x_0 + y_0\}$	(*) Nebenrechnung
$\quad x = x + 1;$	
$\quad \{y - 1 \geq 0 \land x + y - 1 = x_0 + y_0\}$	
$\quad y = y - 1;$	
$\quad \{y \geq 0 \land x + y = x_0 + y_0\}$	Invariante gilt wieder
$\textbf{end}$	
$\{y \leq 0 \land y \geq 0 \land x + y = x_0 + y_0\}$	Annahme: negierter Test & Invariante
$\{x + y = x + 0 = x_0 + y_0\}$	(*) Nebenrechnung
$\{x = x_0 + y_0\}$	Nachbedingung soll hier gelten

(*) Nebenrechnungen: alle direkt aufeinander folgenden Zusicherungen im Code sind Anwendungen der Regel CONSEQ und erfordern einen Beweis!

Addition durch Inkrementieren: Nebenrechnungen

Addition durch Inkrementieren: Nebenrechnungen

$$\{\mathtt{y} \geq 0 \land \mathtt{x_0} = \mathtt{x_0} \land \mathtt{y_0} = \mathtt{y_0}\}$$

$$\{\mathtt{y} \geq 0 \land \mathtt{x_0} + \mathtt{y_0} = \mathtt{x_0} + \mathtt{y_0}\}$$

Addition durch Inkrementieren: Nebenrechnungen

$\{\mathtt{y} \geq 0 \wedge \mathtt{x}_0 = \mathtt{x}_0 \wedge \mathtt{y}_0 = \mathtt{y}_0\}$

$\mathtt{x}_0 = \mathtt{x}_0 \wedge \mathtt{y}_0 = \mathtt{y}_0 \Rightarrow \mathtt{x}_0 + \mathtt{y}_0 = \mathtt{x}_0 + \mathtt{y}_0$ Gilt immer für alle $\mathtt{x}_0, \mathtt{y}_0$

$\{\mathtt{y} \geq 0 \wedge \mathtt{x}_0 + \mathtt{y}_0 = \mathtt{x}_0 + \mathtt{y}_0\}$

Addition durch Inkrementieren: Nebenrechnungen

$\{y \geq 0 \land x_0 = x_0 \land y_0 = y_0\}$

$x_0 = x_0 \land y_0 = y_0 \Rightarrow x_0 + y_0 = x_0 + y_0$ Gilt immer für alle x_0, y_0

$\{y \geq 0 \land x_0 + y_0 = x_0 + y_0\}$

$\{y > 0 \land y \geq 0 \land x + y = x_0 + y_0\}$

$\{y - 1 \geq 0 \land x + 1 + y - 1 = x_0 + y_0\}$

Addition durch Inkrementieren: Nebenrechnungen

$\{y \geq 0 \land x_0 = x_0 \land y_0 = y_0\}$

$x_0 = x_0 \land y_0 = y_0 \Rightarrow x_0 + y_0 = x_0 + y_0$ Gilt immer für alle x_0, y_0

$\{y \geq 0 \land x_0 + y_0 = x_0 + y_0\}$

$\{y > 0 \land y \geq 0 \land x + y = x_0 + y_0\}$

$y > 0 \Rightarrow y - 1 \geq 0$ $y \geq 0$ ist als Annahme nicht ausreichend

$x + y = x + 1 + y - 1$ $+1 - 1$ ändert die Gleichung nicht

$\{y - 1 \geq 0 \land x + 1 + y - 1 = x_0 + y_0\}$

Addition durch Inkrementieren: Nebenrechnungen

$\{y \geq 0 \land x_0 = x_0 \land y_0 = y_0\}$

$x_0 = x_0 \land y_0 = y_0 \Rightarrow x_0 + y_0 = x_0 + y_0$ — Gilt immer für alle x_0, y_0

$\{y \geq 0 \land x_0 + y_0 = x_0 + y_0\}$

$\{y > 0 \land y \geq 0 \land x + y = x_0 + y_0\}$

$y > 0 \Rightarrow y - 1 \geq 0$ — $y \geq 0$ ist als Annahme nicht ausreichend

$x + y = x + 1 + y - 1$ — $+1 - 1$ ändert die Gleichung nicht

$\{y - 1 \geq 0 \land x + 1 + y - 1 = x_0 + y_0\}$

$\{y \leq 0 \land y \geq 0 \land x + y = x_0 + y_0\}$

$\{x + y = x + 0 = x_0 + y_0\}$

$\{x = x_0 + y_0\}$

Addition durch Inkrementieren: Nebenrechnungen

$\{y \geq 0 \land x_0 = x_0 \land y_0 = y_0\}$

$x_0 = x_0 \land y_0 = y_0 \Rightarrow x_0 + y_0 = x_0 + y_0$ — Gilt immer für alle x_0, y_0

$\{y \geq 0 \land x_0 + y_0 = x_0 + y_0\}$

$\{y > 0 \land y \geq 0 \land x + y = x_0 + y_0\}$

$y > 0 \Rightarrow y - 1 \geq 0$ — $y \geq 0$ ist als Annahme nicht ausreichend

$x + y = x + 1 + y - 1$ — $+1 - 1$ ändert die Gleichung nicht

$\{y - 1 \geq 0 \land x + 1 + y - 1 = x_0 + y_0\}$

$\{y \leq 0 \land y \geq 0 \land x + y = x_0 + y_0\}$

$y \leq 0 \land y \geq 0 \Rightarrow y = 0$

$\{x + y = x + 0 = x_0 + y_0\}$

$\{x = x_0 + y_0\}$

Addition durch Inkrementieren: Nebenrechnungen

$\{y \geq 0 \wedge x_0 = x_0 \wedge y_0 = y_0\}$

$x_0 = x_0 \wedge y_0 = y_0 \Rightarrow x_0 + y_0 = x_0 + y_0$ Gilt immer für alle x_0, y_0

$\{y \geq 0 \wedge x_0 + y_0 = x_0 + y_0\}$

$\{y > 0 \wedge y \geq 0 \wedge x + y = x_0 + y_0\}$

$y > 0 \Rightarrow y - 1 \geq 0$ $y \geq 0$ ist als Annahme nicht ausreichend
$x + y = x + 1 + y - 1$ $+1 - 1$ ändert die Gleichung nicht

$\{y - 1 \geq 0 \wedge x + 1 + y - 1 = x_0 + y_0\}$

$\{y \leq 0 \wedge y \geq 0 \wedge x + y = x_0 + y_0\}$

$y \leq 0 \wedge y \geq 0 \Rightarrow y = 0$

$\{x + y = x + 0 = x_0 + y_0\}$

$x + 0 = x_0 + y_0 \Rightarrow x = x_0 + y_0$

$\{x = x_0 + y_0\}$

Substraktion durch Dekrementieren

```
y = a;
while b > 0 do
    y = y - 1;
    b = b - 1;
end
z = y;
```

Substraktion durch Dekrementieren

$\{\mathtt{b} \geq 0 \land \mathtt{a} = \mathtt{a} \land \mathtt{b} = \mathtt{b}_{\mathtt{pre}}\}$ Vorbedingung

$\mathtt{y} = \mathtt{a};$

while $\mathtt{b} > 0$ **do**

$\quad \mathtt{y} = \mathtt{y} - 1;$

$\quad \mathtt{b} = \mathtt{b} - 1;$

end

$\mathtt{z} = \mathtt{y};$

$\{\mathtt{z} = \mathtt{a} - \mathtt{b}_{\mathtt{pre}}\}$ Nachbedingung soll hier gelten

Substraktion durch Dekrementieren

$\{b \geq 0 \land a = a \land b = b_{pre}\}$ Vorbedingung

$y = a;$

$\{y = a + b - b_{pre} \land b \geq 0\}$ Invariante initial zu zeigen

while $b > 0$ **do**

$\qquad y = y - 1;$

$\qquad b = b - 1;$

end

$\{b \leq 0 \land y = a + b - b_{pre} \land b \geq 0\}$ Annahme: negierter Test & Invariante

$z = y;$

$\{z = a - b_{pre}\}$ Nachbedingung soll hier gelten

Substraktion durch Dekrementieren

$\{\mathtt{b} \geq 0 \land \mathtt{a} = \mathtt{a} \land \mathtt{b} = \mathtt{b}_{\mathtt{pre}}\}$	Vorbedingung
$\{\mathtt{a} = \mathtt{a} + \mathtt{b} - \mathtt{b}_{\mathtt{pre}} \land \mathtt{b} \geq 0\}$	(*) Nebenrechnung
$\mathtt{y} = \mathtt{a};$	
$\{\mathtt{y} = \mathtt{a} + \mathtt{b} - \mathtt{b}_{\mathtt{pre}} \land \mathtt{b} \geq 0\}$	Invariante initial zu zeigen
while $\mathtt{b} > 0$ **do**	
$\quad \mathtt{y} = \mathtt{y} - 1;$	
$\quad \mathtt{b} = \mathtt{b} - 1;$	
end	
$\{\mathtt{b} \leq 0 \land \mathtt{y} = \mathtt{a} + \mathtt{b} - \mathtt{b}_{\mathtt{pre}} \land \mathtt{b} \geq 0\}$	Annahme: negierter Test & Invariante
$\mathtt{z} = \mathtt{y};$	
$\{\mathtt{b} \leq 0 \land \mathtt{z} = \mathtt{a} + \mathtt{b} - \mathtt{b}_{\mathtt{pre}} \land b \geq 0\}$	(*) Nebenrechnung
$\{\mathtt{z} = \mathtt{a} - \mathtt{b}_{\mathtt{pre}}\}$	Nachbedingung soll hier gelten

Substraktion durch Dekrementieren

$\{\mathtt{b} \geq 0 \wedge \mathtt{a} = \mathtt{a} \wedge \mathtt{b} = \mathtt{b}_{\mathtt{pre}}\}$	Vorbedingung
$\{\mathtt{a} = \mathtt{a} + \mathtt{b} - \mathtt{b}_{\mathtt{pre}} \wedge \mathtt{b} \geq 0\}$	(*) Nebenrechnung
$\mathtt{y} = \mathtt{a};$	
$\{\mathtt{y} = \mathtt{a} + \mathtt{b} - \mathtt{b}_{\mathtt{pre}} \wedge \mathtt{b} \geq 0\}$	Invariante initial zu zeigen
while $\mathtt{b} > 0$ **do**	
$\quad\{\mathtt{b} > 0 \wedge \mathtt{y} = \mathtt{a} + \mathtt{b} - \mathtt{b}_{\mathtt{pre}} \wedge \mathtt{b} \geq 0\}$	Annahme: Schleifentest & Invariante
$\quad\mathtt{y} = \mathtt{y} - 1;$	
$\quad\mathtt{b} = \mathtt{b} - 1;$	
$\quad\{\mathtt{y} = \mathtt{a} + \mathtt{b} - \mathtt{b}_{\mathtt{pre}} \wedge \mathtt{b} \geq 0\}$	Invariante gilt wieder
end	
$\{\mathtt{b} \leq 0 \wedge \mathtt{y} = \mathtt{a} + \mathtt{b} - \mathtt{b}_{\mathtt{pre}} \wedge \mathtt{b} \geq 0\}$	Annahme: negierter Test & Invariante
$\mathtt{z} = \mathtt{y};$	
$\{\mathtt{b} \leq 0 \wedge \mathtt{z} = \mathtt{a} + \mathtt{b} - \mathtt{b}_{\mathtt{pre}} \wedge b \geq 0\}$	(*) Nebenrechnung
$\{\mathtt{z} = \mathtt{a} - \mathtt{b}_{\mathtt{pre}}\}$	Nachbedingung soll hier gelten

Substraktion durch Dekrementieren

$\{b \geq 0 \land a = a \land b = b_{pre}\}$ — Vorbedingung
$\{a = a + b - b_{pre} \land b \geq 0\}$ — (*) Nebenrechnung
$y = a;$
$\{y = a + b - b_{pre} \land b \geq 0\}$ — Invariante initial zu zeigen
while $b > 0$ **do**
$\quad\{b > 0 \land y = a + b - b_{pre} \land b \geq 0\}$ — Annahme: Schleifentest & Invariante
$\quad\{y - 1 = a + b - 1 - b_{pre} \land b - 1 \geq 0\}$ — (*) Nebenrechnung
$\quad y = y - 1;$
$\quad\{y = a + b - 1 - b_{pre} \land b - 1 \geq 0\}$
$\quad b = b - 1;$
$\quad\{y = a + b - b_{pre} \land b \geq 0\}$ — Invariante gilt wieder
end
$\{b \leq 0 \land y = a + b - b_{pre} \land b \geq 0\}$ — Annahme: negierter Test & Invariante
$z = y;$
$\{b \leq 0 \land z = a + b - b_{pre} \land b \geq 0\}$ — (*) Nebenrechnung
$\{z = a - b_{pre}\}$ — Nachbedingung soll hier gelten

Substraktion durch Dekrementieren

$\{b \geq 0 \wedge a = a \wedge b = b_{pre}\}$	Vorbedingung
$\{a = a + b - b_{pre} \wedge b \geq 0\}$	(*) Nebenrechnung
$y = a;$	
$\{y = a + b - b_{pre} \wedge b \geq 0\}$	Invariante initial zu zeigen
while $b > 0$ **do**	
$\quad\{b > 0 \wedge y = a + b - b_{pre} \wedge b \geq 0\}$	Annahme: Schleifentest & Invariante
$\quad\{y - 1 = a + b - 1 - b_{pre} \wedge b - 1 \geq 0\}$	(*) Nebenrechnung
$\quad y = y - 1;$	
$\quad\{y = a + b - 1 - b_{pre} \wedge b - 1 \geq 0\}$	
$\quad b = b - 1;$	
$\quad\{y = a + b - b_{pre} \wedge b \geq 0\}$	Invariante gilt wieder
end	
$\{b \leq 0 \wedge y = a + b - b_{pre} \wedge b \geq 0\}$	Annahme: negierter Test & Invariante
$z = y;$	
$\{b \leq 0 \wedge z = a + b - b_{pre} \wedge b \geq 0\}$	(*) Nebenrechnung
$\{z = a - b_{pre}\}$	Nachbedingung soll hier gelten

(*) Nebenrechnungen: alle direkt aufeinander folgenden Zusicherungen im Code sind Anwendungen der Regel $\textsc{Conseq}$ und erfordern einen Beweis!

Substraktion durch Dekrementieren: Nebenrechnungen

Substraktion durch Dekrementieren: Nebenrechnungen

$$\{\mathtt{b} \geq 0 \land \mathtt{a} = \mathtt{a} \land \mathtt{b} = \mathtt{b}_{\mathtt{pre}}\}$$

$$\{\mathtt{a} = \mathtt{a} + \mathtt{b} - \mathtt{b}_{\mathtt{pre}} \land \mathtt{b} \geq 0\}$$

Substraktion durch Dekrementieren: Nebenrechnungen

$\{\mathtt{b} \geq 0 \land \mathtt{a} = \mathtt{a} \land \mathtt{b} = \mathtt{b}_{\mathtt{pre}}\}$

$\mathtt{b} = \mathtt{b}_{\mathtt{pre}} \Rightarrow \mathtt{b} - \mathtt{b}_{\mathtt{pre}} = 0 \Rightarrow \mathtt{a} = \mathtt{a} + \mathtt{b} - \mathtt{b}_{\mathtt{pre}}$ Gilt immer für alle a, b

$\{\mathtt{a} = \mathtt{a} + \mathtt{b} - \mathtt{b}_{\mathtt{pre}} \land \mathtt{b} \geq 0\}$

Substraktion durch Dekrementieren: Nebenrechnungen

$\{\mathtt{b} \geq 0 \land \mathtt{a} = \mathtt{a} \land \mathtt{b} = \mathtt{b}_{\mathtt{pre}}\}$

$\mathtt{b} = \mathtt{b}_{\mathtt{pre}} \Rightarrow \mathtt{b} - \mathtt{b}_{\mathtt{pre}} = 0 \Rightarrow \mathtt{a} = \mathtt{a} + \mathtt{b} - \mathtt{b}_{\mathtt{pre}}$ Gilt immer für alle $\mathtt{a}$, $\mathtt{b}$

$\{\mathtt{a} = \mathtt{a} + \mathtt{b} - \mathtt{b}_{\mathtt{pre}} \land \mathtt{b} \geq 0\}$

$\{\mathtt{b} > 0 \land \mathtt{y} = \mathtt{a} + \mathtt{b} - \mathtt{b}_{\mathtt{pre}} \land \mathtt{b} \geq 0\}$

$\{\mathtt{y} - 1 = \mathtt{a} + \mathtt{b} - 1 - \mathtt{b}_{\mathtt{pre}} \land b - 1 \geq 0\}$

Substraktion durch Dekrementieren: Nebenrechnungen

$\{\mathtt{b} \geq 0 \wedge \mathtt{a} = \mathtt{a} \wedge \mathtt{b} = \mathtt{b}_{\mathtt{pre}}\}$

$\mathtt{b} = \mathtt{b}_{\mathtt{pre}} \Rightarrow \mathtt{b} - \mathtt{b}_{\mathtt{pre}} = 0 \Rightarrow \mathtt{a} = \mathtt{a} + \mathtt{b} - \mathtt{b}_{\mathtt{pre}}$ — Gilt immer für alle $\mathtt{a}$, $\mathtt{b}$

$\{\mathtt{a} = \mathtt{a} + \mathtt{b} - \mathtt{b}_{\mathtt{pre}} \wedge \mathtt{b} \geq 0\}$

$\{\mathtt{b} > 0 \wedge \mathtt{y} = \mathtt{a} + \mathtt{b} - \mathtt{b}_{\mathtt{pre}} \wedge \mathtt{b} \geq 0\}$

$\mathtt{y} = \mathtt{a} + \mathtt{b} - \mathtt{b}_{\mathtt{pre}} \Rightarrow \mathtt{y} - 1 = \mathtt{a} + \mathtt{b} - 1 - \mathtt{b}_{\mathtt{pre}}$ — $-1, -1$ ändert die Gleichung nicht

$\mathtt{b} > 0 \Rightarrow \mathtt{b} - 1 \geq 0$ — $\mathtt{b} \geq 0$ ist als Annahme nicht ausreichend

$\{\mathtt{y} - 1 = \mathtt{a} + \mathtt{b} - 1 - \mathtt{b}_{\mathtt{pre}} \wedge b - 1 \geq 0\}$

Substraktion durch Dekrementieren: Nebenrechnungen

$\{\mathtt{b} \geq 0 \land \mathtt{a} = \mathtt{a} \land \mathtt{b} = \mathtt{b}_{\mathtt{pre}}\}$

$\mathtt{b} = \mathtt{b}_{\mathtt{pre}} \Rightarrow \mathtt{b} - \mathtt{b}_{\mathtt{pre}} = 0 \Rightarrow \mathtt{a} = \mathtt{a} + \mathtt{b} - \mathtt{b}_{\mathtt{pre}}$ Gilt immer für alle a, b

$\{\mathtt{a} = \mathtt{a} + \mathtt{b} - \mathtt{b}_{\mathtt{pre}} \land \mathtt{b} \geq 0\}$

$\{\mathtt{b} > 0 \land \mathtt{y} = \mathtt{a} + \mathtt{b} - \mathtt{b}_{\mathtt{pre}} \land \mathtt{b} \geq 0\}$

$\mathtt{y} = \mathtt{a} + \mathtt{b} - \mathtt{b}_{\mathtt{pre}} \Rightarrow \mathtt{y} - 1 = \mathtt{a} + \mathtt{b} - 1 - \mathtt{b}_{\mathtt{pre}}$ $-1, -1$ ändert die Gleichung nicht
$\mathtt{b} > 0 \Rightarrow \mathtt{b} - 1 \geq 0$ $\mathtt{b} \geq 0$ ist als Annahme nicht ausreichend

$\{\mathtt{y} - 1 = \mathtt{a} + \mathtt{b} - 1 - \mathtt{b}_{\mathtt{pre}} \land b - 1 \geq 0\}$

$\{\mathtt{b} \leq 0 \land \mathtt{z} = \mathtt{a} + \mathtt{b} - \mathtt{b}_{\mathtt{pre}} \land \mathtt{b} \geq 0\}$

$\{\mathtt{z} = \mathtt{a} - \mathtt{b}_{\mathtt{pre}}\}$

Substraktion durch Dekrementieren: Nebenrechnungen

$\{\mathtt{b} \geq 0 \land \mathtt{a} = \mathtt{a} \land \mathtt{b} = \mathtt{b}_{\mathtt{pre}}\}$

$\mathtt{b} = \mathtt{b}_{\mathtt{pre}} \Rightarrow \mathtt{b} - \mathtt{b}_{\mathtt{pre}} = 0 \Rightarrow \mathtt{a} = \mathtt{a} + \mathtt{b} - \mathtt{b}_{\mathtt{pre}}$ — Gilt immer für alle a, b

$\{\mathtt{a} = \mathtt{a} + \mathtt{b} - \mathtt{b}_{\mathtt{pre}} \land \mathtt{b} \geq 0\}$

$\{\mathtt{b} > 0 \land \mathtt{y} = \mathtt{a} + \mathtt{b} - \mathtt{b}_{\mathtt{pre}} \land \mathtt{b} \geq 0\}$

$\mathtt{y} = \mathtt{a} + \mathtt{b} - \mathtt{b}_{\mathtt{pre}} \Rightarrow \mathtt{y} - 1 = \mathtt{a} + \mathtt{b} - 1 - \mathtt{b}_{\mathtt{pre}}$ — $-1, -1$ ändert die Gleichung nicht

$\mathtt{b} > 0 \Rightarrow \mathtt{b} - 1 \geq 0$ — $\mathtt{b} \geq 0$ ist als Annahme nicht ausreichend

$\{\mathtt{y} - 1 = \mathtt{a} + \mathtt{b} - 1 - \mathtt{b}_{\mathtt{pre}} \land b - 1 \geq 0\}$

$\{\mathtt{b} \leq 0 \land \mathtt{z} = \mathtt{a} + \mathtt{b} - \mathtt{b}_{\mathtt{pre}} \land \mathtt{b} \geq 0\}$

$\mathtt{b} \leq 0 \land \mathtt{b} \geq 0 \Rightarrow \mathtt{b} = 0$

$\mathtt{z} = \mathtt{a} + 0 - \mathtt{b}_{\mathtt{pre}} = \mathtt{a} - \mathtt{b}_{\mathtt{pre}}$

$\{\mathtt{z} = \mathtt{a} - \mathtt{b}_{\mathtt{pre}}\}$

Laufzeitkomplexitäten

- Addition durch Inkrementieren: $\mathcal{O}(y_0)$
- Subtraktion durch Dekrementieren: $\mathcal{O}(b)$

Hoare-Triple

Begründen Sie für jedes Hoare-Tripel an, ob dieses wahr oder falsch ist. Die Rechenoperationen agieren auf der Menge der ganzen Zahlen ohne Ganzzahlüberläufe.

1. $\{\ \mathit{false}\ \}$ `j = i + 1;` $\{\ \mathtt{i} > 7\ \}$

2. $\{\ \mathtt{x} < \mathtt{y}\ \}$ `x = x + y;` $\{\ \mathtt{x} \geq \mathtt{y}\ \}$

3. $\{\ \mathtt{j} = 0\ \}$ `j = i * i;` $\{\ \mathtt{j} \geq \mathtt{i}\ \}$

Hoare-Triple

Begründen Sie für jedes Hoare-Tripel an, ob dieses wahr oder falsch ist. Die Rechenoperationen agieren auf der Menge der ganzen Zahlen ohne Ganzzahlüberläufe.

1. $\{ \mathit{false} \}$ `j = i + 1;` $\{ \mathtt{i} > 7 \}$

   ✓ wahr, jedes Tripel mit Vorbedingung false ist gültig
   (keine Startzustände müssen geprüft werden)

2. $\{ \mathtt{x} < \mathtt{y} \}$ `x = x + y;` $\{ \mathtt{x} \geq \mathtt{y} \}$

3. $\{ \mathtt{j} = 0 \}$ `j = i * i;` $\{ \mathtt{j} \geq \mathtt{i} \}$

Hoare-Triple

Begründen Sie für jedes Hoare-Tripel an, ob dieses wahr oder falsch ist. Die Rechenoperationen agieren auf der Menge der ganzen Zahlen ohne Ganzzahlüberläufe.

1. $\{ \mathit{false} \}$ `j = i + 1;` $\{ \mathtt{i} > 7 \}$

   ✓ wahr, jedes Tripel mit Vorbedingung false ist gültig
   (<u>keine</u> Startzustände müssen geprüft werden)

2. $\{ \mathtt{x} < \mathtt{y} \}$ `x = x + y;` $\{ \mathtt{x} \geq \mathtt{y} \}$

   ✗ falsch Rückwärtsrechnen: $(\mathtt{x} \geq \mathtt{y})[\mathtt{x} \mapsto \mathtt{x + y}] = \mathtt{x + y} \geq \mathtt{y} \equiv \mathtt{x} \geq 0$
   Es gilt nicht: $\mathtt{x} < \mathtt{y} \Longrightarrow \mathtt{x} \geq 0$

3. $\{ \mathtt{j} = 0 \}$ `j = i * i;` $\{ \mathtt{j} \geq \mathtt{i} \}$

Hoare-Triple

Begründen Sie für jedes Hoare-Tripel an, ob dieses wahr oder falsch ist. Die Rechenoperationen agieren auf der Menge der ganzen Zahlen ohne Ganzzahlüberläufe.

1. $\{ \mathit{false} \}$ `j = i + 1;` $\{ \mathtt{i} > 7 \}$

   ✓ wahr, jedes Tripel mit Vorbedingung false ist gültig
   (<u>keine</u> Startzustände müssen geprüft werden)

2. $\{ \mathtt{x} < \mathtt{y} \}$ `x = x + y;` $\{ \mathtt{x} \geq \mathtt{y} \}$

   ✗ falsch Rückwärtsrechnen: $(\mathtt{x} \geq \mathtt{y})[\mathtt{x} \mapsto \mathtt{x + y}] = \mathtt{x + y} \geq \mathtt{y} \equiv \mathtt{x} \geq 0$
   Es gilt nicht: $\mathtt{x} < \mathtt{y} \implies \mathtt{x} \geq 0$

3. $\{ \mathtt{j} = 0 \}$ `j = i * i;` $\{ \mathtt{j} \geq \mathtt{i} \}$

   ✓ wahr, Vorbedingung irrelevant, aber $\mathtt{i}^2 \geq \mathtt{i}$ für alle $\mathtt{i} \in \mathbb{Z}$.

Hoare-Triple

Begründen Sie für jedes Hoare-Tripel an, ob dieses wahr oder falsch ist. Die Rechenoperationen agieren auf der Menge der ganzen Zahlen ohne Ganzzahlüberläufe.

4. $\{\, \mathtt{i} < \mathtt{n} \,\}$ `while i<n do i=i+1; end` $\{\, \mathtt{i} = \mathtt{n} \,\}$

5. $\{\, \mathtt{a} = 2 \cdot \mathtt{b} \,\}$ `if a < b then m=-b; else m=a; end` $\{\, \mathtt{m} \geq 0 \,\}$

6. $\{\, \mathtt{a} = \mathtt{d} \,\}$ `b = a + c;  a = b - c;` $\{\, \mathtt{a} = \mathtt{d} \,\}$

Hoare-Triple

Begründen Sie für jedes Hoare-Tripel an, ob dieses wahr oder falsch ist. Die Rechenoperationen agieren auf der Menge der ganzen Zahlen ohne Ganzzahlüberläufe.

4. $\{\, \mathtt{i} < \mathtt{n} \,\}$ `while i<n do i=i+1; end` $\{\, \mathtt{i} = \mathtt{n} \,\}$

   ✓ wahr, Beispiel aus der Vorlesung (mit Invariante $\mathtt{i} \leq \mathtt{n}$)

5. $\{\, \mathtt{a} = 2 \cdot \mathtt{b} \,\}$ `if a < b then m=-b; else m=a; end` $\{\, \mathtt{m} \geq 0 \,\}$

6. $\{\, \mathtt{a} = \mathtt{d} \,\}$ `b = a + c;  a = b - c;` $\{\, \mathtt{a} = \mathtt{d} \,\}$

Hoare-Triple

Begründen Sie für jedes Hoare-Tripel an, ob dieses wahr oder falsch ist. Die Rechenoperationen agieren auf der Menge der ganzen Zahlen ohne Ganzzahlüberläufe.

4. $\{\ \mathtt{i} < \mathtt{n}\ \}$ `while i<n do i=i+1; end` $\{\ \mathtt{i} = \mathtt{n}\ \}$

   ✓ wahr, Beispiel aus der Vorlesung (mit Invariante $\mathtt{i} \leq \mathtt{n}$)

5. $\{\ \mathsf{a} = 2 \cdot \mathsf{b}\ \}$ `if a < b then m=-b; else m=a; end` $\{\ \mathtt{m} \geq 0\ \}$

   ✓ if-Fall: $\{\ \mathsf{a} = 2 \cdot \mathsf{b} \land \mathsf{a} < \mathsf{b}\ \}$ $\{\ -\mathsf{b} \geq 0\ \}$ `m=-b` $\{\ \mathtt{m} \geq 0\ \}$

   ✓ then-Fall: $\{\ \mathsf{a} = 2 \cdot \mathsf{b} \land \mathsf{a} \geq \mathsf{b}\ \}$ $\{\ \mathsf{a} \geq 0\ \}$ `m= a` $\{\ \mathtt{m} \geq 0\ \}$

   Nebenrechnungen! z.B. für `if`-Fall: $\mathsf{a} = 2 \cdot \mathsf{b} \land \mathsf{a} < \mathsf{b} \Longrightarrow -\mathsf{b} \geq 0$

6. $\{\ \mathsf{a} = \mathsf{d}\ \}$ `b = a + c;  a = b - c;` $\{\ \mathsf{a} = \mathsf{d}\ \}$

Hoare-Triple

Begründen Sie für jedes Hoare-Tripel an, ob dieses wahr oder falsch ist. Die Rechenoperationen agieren auf der Menge der ganzen Zahlen ohne Ganzzahlüberläufe.

4. $\{ \mathtt{i} < \mathtt{n} \}$ `while i<n do i=i+1; end` $\{ \mathtt{i} = \mathtt{n} \}$

   ✓ wahr, Beispiel aus der Vorlesung (mit Invariante $\mathtt{i} \leq \mathtt{n}$)

5. $\{ \mathsf{a} = 2 \cdot \mathsf{b} \}$ `if a < b then m=-b; else m=a; end` $\{ \mathtt{m} \geq 0 \}$

   ✓ if-Fall: $\{ \mathsf{a} = 2 \cdot \mathsf{b} \land \mathsf{a} < \mathsf{b} \}$ $\{ -\mathsf{b} \geq 0 \}$ `m=-b` $\{ \mathtt{m} \geq 0 \}$
   ✓ then-Fall: $\{ \mathsf{a} = 2 \cdot \mathsf{b} \land \mathsf{a} \geq \mathsf{b} \}$ $\{ \mathsf{a} \geq 0 \}$ `m= a` $\{ \mathtt{m} \geq 0 \}$

   Nebenrechnungen! z.B. für if-Fall: $\mathsf{a} = 2 \cdot \mathsf{b} \land \mathsf{a} < \mathsf{b} \implies -\mathsf{b} \geq 0$

6. $\{ \mathsf{a} = \mathsf{d} \}$ `b = a + c;` `a = b - c;` $\{ \mathsf{a} = \mathsf{d} \}$

   ✓ wahr $\{ (\mathsf{a} + \mathsf{c}) - \mathsf{c} = \mathsf{d} \}$ `b = a + c;` $\{ \mathsf{b} - \mathsf{c} = \mathsf{d} \}$ `a = b - c;` $\{ \mathsf{a} = \mathsf{d} \}$