

Verifikationsproblem

- Gegeben sei eine Spezifikation (Vor- und Nachbedingungen) und ein Programm S:

$$\{V\} S \{P\}$$

- Beweise: Wenn vor der Ausführung von S die Programmvariablen das Prädikat V erfüllen, so erfüllen sie nach der Ausführung (und Terminierung) von S das Prädikat P.
- Bei Korrektheitsbeweisen werden die **schwächste Vorbedingung** und die **stärkste Nachbedingung** gesucht.

$$\{V1\} \Rightarrow \{V\}$$

{V1} ist stärker als {V}

$$\{P\} \Rightarrow \{P1\}$$

{P1} ist schwächer als {P}

Schwächste/Stärkste Zusicherung

Aufgabe 5-1/1

- Ordnen Sie die Zusicherungen nach der Schwäche/Stärke an:

- $i, j \in \mathbb{Z}$

- $\{(i \geq j) \wedge (i \geq -j)\}, \{T\}, \{i > 0\}, \{i \geq 0\}, \{i < 0\}, \{\perp\}, \{(i \geq j) \wedge (j \geq 0)\}$
 $\{j \geq 0\}, \{(i=i) \vee (j \geq 0)\}$

- $\{(i \geq j) \wedge (i \geq -j)\} \Leftrightarrow \{((i \geq j) \wedge (j \geq 0)) \vee ((i \geq -j) \wedge (j < 0))\}$

- $\{\perp\} \Rightarrow \{(i \geq j) \wedge (j \geq 0)\} \Rightarrow \{(i \geq j) \wedge (i \geq -j)\} \Rightarrow \{T\}$

- $\{\perp\} \Rightarrow \{(i \geq j) \wedge (i \geq -j)\} \Rightarrow \{i \geq 0\} \Rightarrow \{T\}$

- $\{\perp\} \Rightarrow \{(i \geq j) \wedge (j \geq 0)\} \Rightarrow \{i \geq 0\} \Rightarrow \{T\}$

- $\{\perp\} \Rightarrow \{i > 0\} \Rightarrow \{i \geq 0\} \Rightarrow \{T\}$

- $\{\perp\} \Rightarrow \{(i \geq j) \wedge (j \geq 0)\} \Rightarrow \{j \geq 0\} \Rightarrow \{T\}$

- $\{(i=i) \vee (j \geq 0)\} \Leftrightarrow \{T\}$

Schwächste/Stärkste Zusicherung

Aufgabe 5-1/2

- Ordnen Sie die Zusicherungen nach der Schwäche/Stärke an:
- $\{c^*c^n = a^*(c+1) + b^*c\}$, $\{c^2 - c - 1 = 0 \wedge c^n = a^*c + b\}$
- $\{c^2 - c - 1 = 0 \wedge c^n = a^*c + b\} \Rightarrow \{c^*c^n = a^*(c+1) + b^*c\}$
- Beweis:

Wenn $\{c^2 - c - 1 = 0 \wedge c^n = a^*c + b\}$ wahr ist, dann:

$$c^*c^n = a^*(c+1) + b^*c$$

$$c^* (a^*c + b) = a^*(c+1) + b^*c$$

$$a^*c^2 + c^*b = a^*c + a + b^*c$$

$$c^2 = c + 1$$

$$a^*(c+1) = a^*c + a$$

Programmverifikation: Zuweisungsaxiom

- **Beweisregel für Zuweisungen (Zuweisungsaxiom):**
 $\{P[x \leftarrow A]\} x := A \{P(x)\}$
- Angenommen, die Nachbedingung $P(x)$ gilt nach der Ausführung der Zuweisung $x := A$. x hat also den Wert, den A vor der Ausführung der Zuweisung hatte.
- $P(x \leftarrow A)$ ist der Programzustand vor der Zuweisung (jede freie Variable x ist durch A ersetzt).
- Wenn $P(x \leftarrow A)$ gilt, dann $x := A$ korrekt.
- Voraussetzungen:
 - A ist ein wohldefinierter Ausdruck
 - A und x sind vom gleichen Typ

Programmverifikation: Zuweisungen

Aufgabe 5-2/1-5

- $b \in \text{Bool}; x, y, z \in \mathbb{N}_0$ Bestimmen Sie $\{V\}$ bzw. $\{P\}$
- $\{V\} z:=0 \{z=0\}$
$$\{V\} = P[z \leftarrow 0] = \{0=0\} = \{T\}$$
- $\{V\} z:=0 \{z=1\}$
$$\{V\} = P[z \leftarrow 1] = \{1=0\} = \{\perp\}$$
- $\{V\} x:=x+10 \{x=15\}$
$$\{V\} = P[x \leftarrow x+10] = \{x+10=15\} = \{x=5\}$$
- $\{x=3\} y:=x*x \{P\}$
$$\{P\} = \{x=3 \wedge y=x*x\} = \{x=3 \wedge y=9\}$$
- $\{V\} y:= x+z \{y=0\}$
$$\{V\} = P[y \leftarrow x+z] = \{x+z=0\}$$

Programmverifikation: Zuweisungen

Aufgabe 5-2/6-10

- $\{V\} y:= x+z \{z=0\}$
$$\{V\} = P[y \leftarrow x+z] = \{z=0\}$$
- $\{z=0\} y:= x+z \{P\}$
$$\{P\} = \{y=x+z \wedge z=0\} = \{y=x \wedge z=0\}$$
- $\{T\} y:= x+z \{P\}$
$$\{P\} = \{T\}[y \leftarrow x+z] = \{y=x+z\}$$
- $\{x*y=10\} x:=x*y \{P\}$
$$\{P\} = [x_{\text{alt}} * y = 10] \{x_{\text{alt}} \leftarrow x_{\text{neu}} / y \wedge y \neq 0\} =$$

$$\{x_{\text{neu}} / y * y = 10 \wedge y \neq 0\} = \{x=10 \wedge y \neq 0\}$$
- $\{x=5\} x:= x-1 \{P\}$
$$\{P\} = \{x_{\text{alt}}=5\}[x_{\text{alt}} \leftarrow x_{\text{neu}} + 1] = \{x_{\text{neu}} + 1 = 5\} = \{x=4\}$$

Programmverifikation: Zuweisungen

Aufgabe 5-2/11-15

- $\{y \geq x\} y := y+1 \{P\}$
 $\{P\} = \{y_{\text{alt}} \geq x\} [y_{\text{alt}} \leftarrow y_{\text{neu}}-1] = \{y_{\text{neu}}-1 \geq x\} = \{y_{\text{neu}} \geq x+1\} = \{y > x\}$
- $\{x \bmod 2 = 0\} x := x+1 \{P\}$
 $P = \{x_{\text{alt}} \bmod 2 = 0\} [x_{\text{alt}} \leftarrow x_{\text{neu}}-1] =$
 $\{(x_{\text{neu}}-1) \bmod 2 = 0\} = \{x \bmod 2 = 1\}$
- $\{V\} x := x*2 \{x \bmod 2 = 1\}$
 $\{V\} = P[x \leftarrow x*2] = \{(x*2) \bmod 2 = 1\} = \{\perp\}$
- $\{V\} b := x > y \{b \leftrightarrow (x \geq y)\}$
 $\{V\} = P[b \leftarrow (x > y)] = \{(x > y) \leftrightarrow (x \geq y)\} = \{x \neq y\}$
- $\{(x+1) > z\} x := x+2 \{P\}$
 $\{P\} = \{(x_{\text{alt}} + 1) > z\} [x_{\text{alt}} \leftarrow x_{\text{neu}}-2] = \{(x_{\text{neu}}-2+1) > z\} = \{(x-1) > z\}$

Programmverifikation: Zuweisungen

Aufgabe 5-2/16-20

- $\{V\} y := y-z \{x-y=z\}$
 $\{V\} = P[y \leftarrow y-z] = \{x-y+z=z\} = \{x=y\}$
- $\{V\} x := x+1 \{\exists y. x=(y+1)\}$
 $\{V\} = P[x \leftarrow x+1] = \{\exists y. (x+1)=(y+1)\} = \{T\}$
- $\{V\} x := y+1 \{x \geq 0\}$
 $\{V\} = P[x \leftarrow y+1] = \{y+1 \geq 0\}$
- $\{V\} x := x-y \{x \geq 0\}$
 $\{V\} = P[x \leftarrow x-y] = \{x-y \geq 0\} = \{x \geq y\}$
- $\{\forall x Q(x) \rightarrow \exists y Q(y)\} x := y+z \{P\}$
 $\{\forall x Q(x) \rightarrow \exists y Q(y)\} \leftrightarrow \{T\}; \{T\} x := y+z \{P\}; \{P\} = \{x=y+z\}$

Abschwächungsregel

- Falls gilt:

$$\{V1\} S \{P1\}$$

$$\{V\} \Rightarrow \{V1\} S \{P1\} \Rightarrow \{P\}$$

V ist stärker als V1

P ist schwächer als P1

- Dann gilt:

$$\{V\} S \{P\}$$

Programmverifikation: Zuweisungen

Aufgabe 5-3/1

- Beweisen Sie die Korrektheit:

$$V: \{x=(q+1)*y+r-y \wedge r \geq (y-1)\}$$

$$r:=r-y$$

$$P: \{x=(q+1)*y+r \wedge r \geq 0\}$$

$$\{V1\} = \{P[r \leftarrow r-y]\} = \{x=(q+1)*y+r-y \wedge r-y \geq 0\} =$$

$$= \{x=(q+1)*y+r-y \wedge r \geq y\}$$

$$\{V1\} \neq \{V\}$$

Können wir zeigen, daß $\{V\} \Rightarrow \{V1\}$? Nein!

$$\{x=(q+1)*y+r-y \wedge r \geq (y-1)\} \Leftarrow \{x=(q+1)*y+r-y \wedge r \geq y\}$$

Programmverifikation: Zuweisungen

Aufgabe 5-3/2

- Beweisen Sie die Korrektheit:

V: $\{x=a\}$

$x:=x*x+5$

P: $\{x=a^2 + 5 \wedge x \geq 0\}$

$\{V1\} = \{P[x \leftarrow x*x+5]\} = \{(x*x+5 = a^2 + 5 \wedge (x*x+5) \geq 0)\} =$
 $= \{x*x = a^2\} = \{x=a \vee x=-a\}$

Es gilt: $\{V1\} x:=x*x+5 \{P\}$; $\{V1\} \neq \{V\}$

Können wir zeigen, daß $\{V\} \Rightarrow \{V1\}$? Ja!

$\{x=a\} \Rightarrow \{x=a \vee x=-a\}$

Deshalb gilt auch $\{V\} x:=x*x \{P\}$

Programmverifikation: Zuweisungen

Aufgabe 5-3/3

- Beweisen Sie die Korrektheit:

V: $\{x=a \wedge y \neq 0\}$

$x:=x/y$

P: $\{x*y=a\}$

$\{V1\} = \{P[x \leftarrow x/y]\} = \{(x/y)*y=a\} = \{x=a\}$

Es gilt: $\{V1\} x:=x/y \{P\}$

$\{V1\} \neq \{V\}$

Können wir zeigen, daß $\{V\} \Rightarrow \{V1\}$? Ja!

$\{x=a \wedge y \neq 0\} \Rightarrow \{x=a\}$

Deshalb gilt auch $\{V\} x:=x/y \{P\}$